UNIVERSITE PARIS 8

U.F.R. LANGAGE, INFORMATIQUE, TECHNOLOGIE

N° attribué par la bibliothèque

THESE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE PARIS 8

Discipline : science de l'information et de la communication

présentée et soutenue publiquement

par

Antoine CASANOVA

le 19 mars 1999

Titre : méthodes d'analyse du langage crypté : Une contribution à l'étude du manuscrit de Voynich

---

Directeur de thèse : M. LEPERS Jean-Marc

JURY

Professeur émérite	**M. Paul CAMION**
Professeur	**M. Maxime CROCHEMORE**
Directeur	**M. Jean-Marc LEPERS**
Adjoint au Délégué Interministériel de la DISSI	**M. André CATTIEUW**
Inspecteur du SCSSI	**M. Michel MITTON**
Enseignant	**M. Paul LOUBIÈRE**
Enseignant	**M. Patrick DESHAYES**

14 novembre 1998 —Première édition

UNIVERSITE PARIS 8

Discipline : science de l'information et de la communication

Résumé

<u>Titre</u> : méthodes d'analyse du langage crypté : Une contribution à l'étude du manuscrit de Voynich

par

Antoine CASANOVA

Directeur de thèse : M. LEPERS Jean-Marc

1-§ L'énigme du manuscrit de Voynich semble être née d'une génération spontanée. Le manuscrit fut découvert une première fois à la fin du XVI^{ème} siècle et l'idée s'imposait déjà, comme une évidence, que ce fût là un manuscrit de Roger BACON. Le manuscrit semblait d'un décryptage aisé, les dessins, pensait-on, devaient contribuer à sa résolution, et pourtant aucun n'a pu aboutir à une solution acceptable. Quel paradoxe, que des cryptanalystes du vingtième siècle, de renom et entraînés par l'activité cryptographique des deux guerres mondiales, n'arrivaient pas à vaincre ce problème issu d'une cryptographie balbutiante.

2-§ En fait, le problème du non-aboutissement prend sa source dans un dysfonctionnement de l'*artefact* cryptanalytique qui fait trop tôt appel à l'analogie de langages avant même d'extraire les structures de symboles indépendantes de l'idée de référence. Notre méthodologie s'en trouve affectée. Nous replaçons les méthodes traditionnelles de la cryptanalyse dans les limites de ce qu'elles enseignent sur la nature de l'information étudiée ; leur connaissance nous incite à développer de nouvelles façons de faire.

3-§ Nous découvrons que le manuscrit revêt les qualités d'un langage synthétique dont l'alphabet, servant à sa rédaction, subirait des mutations. En fait, deux langages apparaissent distincts, bien qu'entre eux deux, il existe d'autres —au plus quatre— langages déclinés et pourvus de termes communs ce qui privilégient la thèse de la substitution à représentations multiples. La forme particulière de cette énonciation procède d'une condensation de l'information que l'on peut comparer à celle subie par un texte consonantique. Assurément, d'une à quatre lettres de Voynich s'assimilent à la nature de la lettre nulle selon que nous considérons le manuscrit comme un unique texte ou comme un conglomérat de cryptogrammes pourvus de six alphabets distincts.

UNIVERSITE PARIS 8

Discipline : communication and information science

Abstract

<u>Title</u> : methods of analysis of the coded language : a contribution to the study of the Voynich's manuscript

by

Antoine CASANOVA

Director of thesis : M. LEPERS Jean-Marc

———————

4-§ The enigma of Voynich's manuscript seems to have come out of a spontaneous generation. The manuscript was first discovered at the close of the 16th century and the idea that it was a manuscript by Roger BACON already established itself as being obvious. The manuscript seemed easy to decipher ; and it was believed that the drawings on it were to contribute to solve its enigma, and yet none could lead to a satisfactory solution. Isn't it paradoxical that in the 20th century, renowned cryptanalysts trained for and having gained by a cryptographic activity which had boomed during the two world wars failed to solve this problem arising from an infant cryptography.

5-§ Indeed, the problem of failure is due to a dysfunction of the cryptanalytic *artefact* whose use of the analogy of languages comes at too early a stage, even before extracting the structures of symbols independently of the idea of reference. And this happens to have affected our own methodology. We put the traditional methods of cryptanalysis back within the limits of what they inform us about the nature of the studied information ;our knowing them prompts us to evolve new modes of approach.

6-§ We discover that the manuscript takes on the qualities of a synthetic language whose alphabet —used for its writing— would be subject to transformations. In fact, two languages appear distinct although between the two of them, there exists other declined languages —four at the most— which contain the same terms that give greater importance to the thesis of the substitution by multiple representation. The particular form of this enunciation stems from a reduction of the information which the one undergone by a consonantal text. Most certainly, several letters —between one and four— in Voynich's manuscript show analogies with the nature of the null letter depending on whether we regard the manuscript as one single text or as a conglomerate of cryptograms endowed with six separate alphabets.

DEDICACES

A mes parents,

A Yves LECERF,

REMERCIEMENTS

Nous voudrions avant tout remercier M. DESHAYES Patrick et M. CROCHEMORE Maxime.

Nous remercions M. MITTON Michel et M. CATTIEUW André pour leur contribution à l'aboutissement de notre travail et par-delà nous remercions l'ensemble des intervenants du SCSSI.

Nous adressons nos remerciements aux membres du jury.

Nous remercions M. LEPERS Jean-Marc, pour sa gentillesse, sa capacité d'écoute, son ouverture vers d'autres mondes, notre monde, et qui nous a accompagné pendant ces trois années de recherches comme directeur de thèse.

Nous adressons particulièrement nos remerciements à M. BAFFOY Thierry, directeur de l'Institut Universitaire de Technologie du site de Montreuil (93) qui nous a accueilli pendant deux années en tant qu'ATER et nous a nourri de savants conseils, ainsi qu'à M. LOUBIÈRE Paul qui fut le directeur de nos recherches en 1995 et devenait notre collègue l'année suivante, et nous n'oublions pas les professeurs et les enseignants avec qui nous avons eu le plaisir de travailler. Nous remercions aussi Mme. BELGODÈRE Jeanine de l'université du Havre pour sa contribution anglophile. Nous remercions M. Андрей Могутов de l'université de Saint-Pétersbourg pour ses précieux conseils et sa participation à l'étude du manuscrit de Voynich. Enfin, nous remercions les membres ethnologues de l'institut Charles V.

Nous ne pourrions conclure sans citer et remercier les membres de notre groupe de recherche pour la résolution de l'énigme du manuscrit de Voynich.

Par ordre alphabétique des pays concernés, nous commençons par l'Australie qui accueille notre linguiste M. Jacques GUY, Docteur de l'université de Canberra, issu de l'Institut des Langues Orientales à Paris et spécialiste du décryptage des tablettes de l'île de Pâques ; au Brésil, M. Jorge STOLFI, Professeur à l'université de Campinas ; en Grande-Bretagne, M. Gabriel LANDINI, Maître de conférence en Pathologie Analytique à l'université de Birmingham ; aux Pays-Bas, M. René ZANDBERGEN, préposé aux calculs des orbites satellitaires à l'Agence Spatiale Européenne et aux questions des langues synthétiques, pour qui —et pour nous— « le manuscrit doit être traité comme une réelle énigme —et pas seulement comme une pièce bizarre de musée— dont l'étude doit nous amener à comprendre des traits de l'histoire moyenâgeuse » ; aux USA, Bâton Rouge, M. Dennis STALLINGS, diplômé en biologie à l'université du Kansas, travaille au département de la Louisiane au service de la qualité de l'air et de l'environnement et qui adresse un encouragement aux « institutions » pour qu'elles s'engagent dans l'étude de ce manuscrit, et il exprime le souhait « qu'il serait

spécialement bienvenue que l'université de Yale —New York— accorde plus aisément les accès au manuscrit MS408 » ; toujours aux USA, M. Jim REEDS, Docteur en Statistiques de l'université de Harvard, travaille chez AT&T au laboratoire de recherche SHANNON sur les questions de mathématiques et de cryptographie. Surtout, nous n'oublions pas nos « pairs » qui depuis le XVII^{ème} siècle se sont successivement employés à cette énigme.

Avertissements

•

Discipline. Sujet. Origines des membres. Sujets transversaux. Outils.

Introduction

•

Partie I

Le manuscrit de Voynich

•

14 novembre 1998 —Première édition

Partie II

Quel cheminement emprunter ?

•

Partie III

Les structures de motifs

•

Conclusion

•

L'ensemble des propositions hypothétiques, des faits observés et des conclusions intermédiaires que nous avons établies au cours de la thèse sont à la page 283. La conclusion que nous formulons repose sur cet ensemble. Il nous permet de répondre aux trois questions essentielles de « *La nature du texte »,* de la *« Nature de la substitution »* et des *« Autres natures »* probables du texte manuscrit. Notre contribution à l'étude du manuscrit de Voynich se poursuivra sur de nouveaux axes de recherche que nous proposons dans la partie intitulée *Perspectives.*

—page 299—

Bibliographie

•

Pour conduire l'étude du manuscrit de Voynich nous avons défini trois catégories de documents qui décrivent notre *Artefact*, *Les mots du langage* et les *Structures de motifs.*

—page 319—

ANNEXE

•

Les informations annexes se décomposent en deux parties. La première partie rassemble les données permettant d'accéder directement au cœur du travail (page 309). La deuxième partie détaille les résultats obtenus (page 341).

Index

—page 329—

Figures

—page 311—

Equations

—page 309—

Tableaux

—page 315—

LEXIQUE

Anagrammatique. Se dit d'une séquence d 'éléments ayant été transposés les uns avec les autres, exemple : « NEIGE » et « GENIE ».

Consonantique. Texte dont on a supprimé les voyelles ou « TXT DNT N SPPRM LS VLLS ».

Cryptage. Opération qui consiste à transcrire un texte clair en écriture secrète.

Cryptanalyse. Vocable d'origine américaine —cryptanalysis— précise que l'étude faite sur le cryptogramme repose sur une méthodologie d'analyse propre à résoudre l'énigme soulevée par ce cryptogramme.

Cryptogramme. Séquence de symboles ayant subi une modification — normalement— méthodique pour que le sens intelligible du message soit imperceptible. On en reconnaît un quand on ne peut le comprendre ce qui induit que tous les cryptogrammes ne sont pas égaux.

Cryptographie. Ensemble des techniques utilisées pour transcrire en écriture secrète un texte qui est en clair, et inversement.

Cryptologie. Etude savante des moyens de cryptage et de décryptage de l'information.

Décryptage. Opération inverse du cryptage, transcrire un texte secret en un texte clair. La notion de « secret » étant basé sur l 'état de connaissance relative à l'information qu'il contient.

Familles. Ensemble de lettres remplaçables qui obéissent à un même *modus operandi*, exemple : la ponctuation, le point, la virgule, le point-virgule.

Lettre. Chacun des signes graphiques, des caractères imprimés de l'alphabet.

Manuscrit de Voynich. Nous ne savons pas qui a écrit le manuscrit, le nom de ce manuscrit est donc devenu celui qui le découvrit en 1912 ; ce point est d'ailleurs étrange puisqu'il avait déjà eu des « propriétaires » au XVII^{ème} siècle dont le premier est assurément Marcus MARCI, nous pourrions tout aussi bien appeler ce manuscrit : « le manuscrit de MARCI ».

MS408. Diminutif attribué au manuscrit de Voynich. A l'origine, c'est la référence que la bibliothèque de Yale lui a attribuée, le manuscrit est donc le manuscrit numéro 408.

Sémitique. Nous employons cette terminologie pour indiquer qu'un texte est consonantique mais l'hypothèse que la langue soit sémite n'est pas exclue.

Stéganographie. Technique qui consiste à dissimuler un message sans pour autant le crypter.

Sténographie. Ecriture serrée qui procède de la condensation de l'information.

Symbole. (grec : *symbolos*, signe) Ce qui représente une entité abstraite. Nous employons le terme « symbole » avec une définition proche de celle de « lettre ». Cependant, il nous arrivera d'opposer l'étude d'un texte en parallèle à l'étude du manuscrit : nous dirons, « une lettre du texte est similaire à un symbole du manuscrit », nous marquons ainsi la différence entre « texte clair » et « texte crypté ».

Symboles de Voynich. Référence au symboles du manuscrit de Voynich et non au « redécouvreur » Wilfrid Voynich.

Pasilalie. Ensemble des règles d'exécution verbale des signes d'un langage écrit.

Pasigraphie. Langue écrite —peut être synthétique— qui n'est pas prévue pour une exécution verbale.

ILBHJ HZVYJ FZNLU VBRCS SDUEB TQVHL CGTHS IJQXK KFIPP

EWQVJ QXGGJ YFPSH NTCRT ZNIMY PMEIH BZAKJ DLLOS OSNFX

SYWZX RJKUJ RFLGG XXJAG ZVOXO VRGPD ZGYEY NDPES MMUDN

KPNJY NPKAM IZOVN IJ

michiton oladabas multos te tccr cerc portas

tix quarix morix ahca maria

Res, non verba

14 novembre 1998 —Première édition

14 novembre 1998 —Première édition

Avertissements

•

LE SUJET que nous allons traiter doit être présenté avec précaution. La rareté des thèses doctorales traitant d'analyse du langage crypté ne nous permet pas d'introduire directement sur les problématiques soulevées par notre travail de recherche et d'analyse. Nous présentons donc trois aspects de notre discipline pour que le lecteur puisse prendre appui sur des repères entre lesquels, et au-delà desquels, notre exposé se construit; ces trois références placent l'acteur dans son parcours, son sujet, et ses outils.

Discipline

7-§ La discipline dans laquelle s'insère notre étude est la cryptologie. Elle consiste simplement à étudier des documents qui apparaissent inintelligibles. Nous appellerons souvent cette discipline par le synonyme d'origine américaine *cryptanalyse*.

Sujet

8-§ Le sujet que nous discutons est celui des méthodes d'analyse du langage crypté que nous utilisons pour l'étude du manuscrit de Voynich. Or, quand nous évoquons le vocable « méthode » il nous vient à l'esprit le *Discours de la méthode* de René DESCARTES. Il nous dit dans son livre que

> *le bon sens est la chose du monde la mieux partagée : car chacun pense en être si bien pourvu que ceux même qui sont les plus difficiles à contenter en toute autre chose n'ont point coutume d'en désirer plus qu'ils en ont. En quoi il n'est pas vraisemblable que tous se trompent ; mais plutôt cela témoigne que la puissance de bien juger, et distinguer le vrai d'avec le faux, qui est proprement ce qu'on nomme le bon sens, ou la raison, est naturellement égale en tous les hommes ; et ainsi que la diversité de nos opinions ne vient pas de ce que les uns sont plus raisonnables que les autres, mais seulement de ce que nous conduisons nos pensées par diverses voies, et ne considérons pas les mêmes choses.*

9-§ et en ce sens vous devez vous attendre à trouver dans notre document une multitude de méthodes[1] qui empruntent *diverses voies*. Toutefois, si il existe une discipline où rien n'est moins sûr, où aucun résultat n'est jamais certain, mais reste probable, il s'agit bien de cryptanalyse.

---

[1] Jusqu'au seizième siècle, les méthodes n'étaient pas classées selon leurs caractéristiques. Il faut attendre Giovanni Battista PORTA pour qu'en 1563, dans *« De furtivis literarum notis »,* la cryptologie commence à s'organiser méthodiquement et que les premières critiques sur la solidité et le bon emploi des procédés soient expliqués. Il cataloguait les procédés en transposition, substitution par symboles et en substitution par alphabet cryptographique.

Origines des membres

10-§ Des ethnologues et linguistes ont pratiqué cette discipline sans pour autant penser être cryptanalystes. Antoine Rossignol, fondateur du service du Chiffre français, n'avait reçu aucun enseignement spécifique pour exercer cet art. De l'autre coté de l'Atlantique, trois cents ans après, William F. FRIEDMAN se consacrait avant tout à la génétique avant d'emprunter le chemin de la cryptanalyse. Ceci pourtant ne l'empêcha pas de devenir un des grands spécialistes du domaine et d'être le fondateur du mythique NSA. Il semble que la cryptanalyse « s'impose d'elle-même » à des individus qui n'aspiraient apparemment pas à ce sacerdoce. Il apparaît que plusieurs chemins mènent à cet Art. Les parcours de ces hommes[2] sont souvent hors du commun. Nous pensons par exemple au Capitaine KASISKI qui après avoir apporté la solution[3] au problème majeur des polysubstitutions[4] se consacra à l'anthropologie.

11-§ Alan TURING vint aussi à la cryptanalyse[5] mais d'une façon occasionnelle[6]; il élabora la formalisation et la construction du premier ordinateur (*la bombe*[7]) dédié à la cryptanalyse de machine chiffrante. Après la deuxième Guerre Mondiale, TURING poursuivit ses travaux sur la programmabilité des ordinateurs et il s'intéressa à la croissance des organismes biologiques avant de connaître une fin tragique.

Sujets transversaux

12-§ Il serait faux de croire que la cryptanalyse n'est que militaire ; bien qu'elle aida à disculper le Capitaine DREYFUS des accusations de trahisons qui lui étaient reprochées et qu'elle contribua aussi à confondre l'agent H-21 plus connu sous le nom de MATA-

---

[2] Nous ne savons pas pour quelle raison ce milieu est exclusivement masculin; il faut attendre le vingtième siècle pour qu'une femme pratique la cryptanalyse militaire ; bien entendu, elle était la femme de W. F. FRIEDMAN.

[3] Ses travaux, un peu comme ceux de Mendel, furent oubliés puis redécouverts par la suite. Certains spécialistes de la cryptographie affirmaient encore, quarante ans après KASISKI, que les polysubstitutions étaient des moyens sûrs de cryptage.

[4] La polysubstitution est antérieure à la méthode PLAYFAIR mais est postérieure au carré de POLYBE. Elle connut longtemps une gestation sous la forme d'un assemblage entre procédés à représentations multiples et procédés par groupes codiques auxquels on y ajoutait des signes nuls. Il y avait alors constitution d'un dictionnaire de codes mettant en relation des lettres et des mots avec des signes. Il faudra attendre la fin du seizième siècle pour qu'une méthode alphabétique de polysubstitution soit proposée, et point remarquable, il faudra attendre la fin du dix-neuvième siècle pour qu'elle soit décryptée.

[5] Il travaillait au G. C. C. S. Government Code and Cypher School.

[6] Deuxième Guerre Mondiale.

[7] La « bombe » n'est pas originaire du G. C. C. S mais du B. S. 4 polonais. En effet, les polonais avaient réussi le décryptage de la première version de la machine Enigma avant le début de la deuxième guerre mondiale.

HARI[8] ; la cryptanalyse est transversale aux disciplines et elle s'intéresse à une multitude de types de problématiques.

13-§ La plus connue est l'étude faite des hiéroglyphes égyptiens par Jean-François CHAMPOLLION dont la résolution reposait sur la compréhension du Monde Antique Egyptien et de son imprégnation dans son écriture plutôt que sur une analyse algébrique[9] si chère aux cryptologues de cette deuxième moitié de vingtième siècle. CHAMPOLLION constat la forte relation entre les glyphes et leur capacité à décrire un naturel vivant ou inerte. La relation entre l'environnement naturel et l'écriture était sans équivoque, le dessin d'un oiseau se rapportait à l'oiseau[10] lui-même [CHAM1841].

Ainsi, comprendre la nature et son contexte était un premier pas indispensable dans l'apprentissage des hiéroglyphes.

14-§ CHAMPOLLION faisait remarquer qu'il suffisait, pour distinguer les hiéroglyphes du chacal et du chien, de regarder ces animaux vivre dans la nature : le chien a pour habitude de se promener la queue dressée en trompette tandis que le chacal usa de la coutume de tenir sa queue non dressée ; voici comment on distingue ces deux animaux aux postures différentes lorsqu'ils sont sculptés dans la pierre [CHAM1989].

Le contexte naturel est la source informative indispensable à l'analyse des hiéroglyphes ; il usa de la méthode analogique, entre nature et écriture, comme expression du lien logique entre le contexte social et le contexte hiéroglyphique.

15-§ Toujours à partir de la nature et de sa représentation, CHAMPOLLION tira un ensemble de constatations normatives sur la représentation des glyphes : la lune était représentée par un disque de couleur jaune, le soleil par un disque de couleur rouge, et symétriquement, l'homme est de chair rouge plus ou moins foncée, la femme est de chair jaune [CHAM1841] et [CHAM1823].

L'homme s'inscrit dans la nature, l'écriture de l'homme dévoile sa nature. Les connexions décrivent les contextes et contribuent à la compréhension de l'écrit.

[8] Une des rares collaborations entre services de décryptage permit aux français d'arrêter « l'espionne » qui avait reçu l'ordre de se rendre à Paris par un message crypté allemand.

[9] La comparaison entre le texte hiéroglyphique et le texte grec de la pierre de Rosette montrait une grande différence entre les nombres de symboles nécessaires à l'un et à l'autre. Il fallait près de trois fois plus de symboles égyptiens pour transcrire le même texte en grec.

[10] Chouette, petite caille, vautour.

16-§ Le deuxième point fondamental est l'utilisation de la méthode analogique entre écritures. La découverte de la pierre de Rosette est l'élément fondamental[11] qui mettait en présence trois textes en langue grecque, copte et hiéroglyphique. Cette pierre montrait les mutations de l'écriture hiéroglyphique en écriture égyptienne cursive, alors plus récente, ainsi que leurs traductions en grec. Cette pierre démonstratrice de l'évolution scripturale permit de résoudre un mystère si longuement préservé.

La recherche d'analogies entre textes est nécessaire voire incontournable. Cependant, il reste à définir les limites de cette recherche et à partir de quand elle passe de l'état utilitaire à l'état indispensable.

17-§ Le décryptement du Cunéiforme de Babylone, par NIEBUHR et ses successeurs TYCHSEN et GROTEFEND, procède de la même méthodologie : –Recherches des différents types d'écritures, du sens de la lecture[12], de la séparation des vocables et de l'analogie du texte analysé avec d'autres langages qui lui sont liés de quelques façons et enfin mise en exergue de structures équivalentes.

Mais alors, que se passe-t-il lorsque nous perdons les contextes culturels et naturels dans lesquels l'écrit de l'homme se circonscrit ?

18-§ Contrairement aux hiéroglyphes égyptiens et au cunéiforme de Babylone, les signes étranges de l'île de Pâques sont « isolés » culturellement du reste du monde et ne sont en aucune relation de traduction avec d'autres langues parlés ou écrites. Peut-on résoudre la signification de ce langage écrit sans l'étude de son contexte, et combien même, peut-on comprendre ces écritures sans liens avec les quelques langages que nous connaissons ?

19-§ Les tablettes d'Aruku Kurenga[13] sont sculptées avec une écriture balbutiante dans laquelle nous retrouvons les formes naturelles de l 'étoile de mer, du crabe, de plantes de la flore locale, d'objets usuels, de parties du corps humain ou bien des formes

[11] La recherche d'analogie entre le texte grec et le texte hiéroglyphique mettait en exergue la structure particulière de l'écriture des noms des rois et reines circonscrits dans des cartouches. La seule méthode algébrique utilisée fut celle du calcul de la surabondance des hiéroglyphes par rapport aux lettres grecques (trois fois plus) ce qui laissa penser que les glyphes des cartouches représentaient autre « chose » que des lettres. L'idée de CHAMPOLLION fut d'attribuer des valeurs phonétiques aux hiéroglyphes et que dans le texte de la pierre de Rosette, orienté en un sens, les êtres vivants indiquaient en les regardant droit dans les yeux le nom de Cléopatre et de Thoutmosis.

[12] Déterminé par la technique d 'écriture du cunéiforme avec le roseau taillé que l'on appelle calame.

[13] Tablette gravée de 1135 signes à l'aide de dents de requin ou d 'éclats d'obsidienne. L'écriture est dite *boustrophédon à inversion alternée*. En tout, les tablettes de Kohau Rongo Rongo sont au nombre de vingt et un ; elles contiennent cinq insignes royaux, 14021 signes dont 595 signes de base.

géométriques [ORL1988] ; mais nous y trouvons aussi le signe du dieu Make Make[14] dont l'extrême représentation[15] nous rappelle encore une fois la relation entre l'écrit et l'homme dans sa nature et que même si nous ne comprenons pas cette écriture nous comprenons que la valeur culturelle de l'incarnation du dieu Make Make des pascuans se trouve si fréquemment appelée dans l'écriture et tout autant gravée sur les roches basaltiques de cette île volcanique.

20-§ Pouvons-nous comprendre ces messages écrits indépendamment des références culturelles auxquelles les signes sont liés ? Retournons la question et demandons-nous :

Comment rédigerions-nous un message devant être compris par quiconque et quelque soit le siècle ?

21-§ La conquête spatiale des années 1970 a accompagné le programme de recherche d'intelligence extraterrestre SETI[16]. En 1972, les vaisseaux, Pioneer 10, 11 et Voyager 1, 2, abritaient des plaques gravées d'informations[17] nous concernant. Cependant, mises à part les représentations humaines de la femme et de l'homme, les autres représentations nécessitaient une symétrie de la communication [RUES&BATE1988] pour en comprendre la signification ; or, cet équilibre entre communiquants n'est pas systématiquement vrai entre terriens, que peut-il en être entre terrestres et extraterrestres ?

En 1984, Thomas A. SEBEOK se pencha sur une question[18] analogue :

> *comment signaler le danger d'intrusion sur un site radioactif pendant une période de 10000 ans ?*

22-§ Ce message devait protéger les individus de toutes les civilisations, connues et

---

[14] Il semble tout droit sorti de l'œuf originel de Tangaroa, dieu à l'origine de toute chose en Polynésie. Les représentations qui le figurent sous forme d'un être humain à tête d'oiseau évoquent le mythe de la création du monde par Tangaroa

> *Pendant des millions d'années Tangaroa resta dans les ténèbres. Préexistant au monde, il s'était crée et nommé lui-même. Sa coquille était comme un œuf qui tournait dans l'espace infini, sans ciel ni terre, sans mer, sans lune, sans soleil et sans étoiles. Lorsqu'il cassa sa coquille, il se débarrassa des plumes qui couvraient son corps, celles-ci en tombant sur la terre, donnèrent naissance à la végétation [JAUS1893].*

[15] 183 fois sur 1135 signes, soit 16% du texte.

[16] Search for ExtraTerrestrial Intelligence : MC DONOUGH'S Thomas, édition WILEY Science, 1987. Le but de SETI était de détecter des émissions radios et d'émettre des signaux pour signaler notre présence. Un des messages reconstituait la silhouette humaine par l'impulsions d'ondes courtes et longues.

[17] Les dessins devaient préciser, la position de la terre, des informations sur notre système solaire,..., les atomes de carbone et d'oxygène.

[18] Formulée par l'Office of Nuclear Waste Isolation et de U.S. Nuclear Regulatory Commission.

inconnues, quelque soit leur degré d'évolution. SEBEOK ne conserva[19] que trois façons possibles de transmission de cette information. La première consiste à transmettre le message écrit en le formulant à nouveau toutes les trois générations : grand-parents, parents, enfants ; la sémiotique du message évolue dans une continuité sociale, elle n'est donc pas adaptée en cas de ruptures sociales. Alors SEBEOK imagina que la pluralité des messages écrits dans diverses traductions favorisait le décryptage d'au moins un message comme la pierre de Rosette en avait fait office. Seulement, même si la redondance des messages formulés sous diverses formes rend probable la compréhension d'au moins un message, il demeure vrai qu'il doit exister un semblant de reste de continuité sociale, semblant que les extraterrestres n'ont probablement pas. Finalement, SEBEOK conclut que seule la création de mythes, de légendes ou de superstitions liées aux dangers du site, permettait la survivance du message originel et même dans le cas ou la civilisation retournerait à l'état de civilisation barbare. Toutefois, et encore une fois, mythes, légendes et superstitions sont de nature narrative et en ce cas, l'extinction des civilisations humaines ne permettrait pas à l'extraterrestre d'être averti du danger.

Pour conclure, les expériences cryptanalytiques transversales aux disciplines montrent que, la connaissance du contexte naturel, la recherche d'analogies entre écrits, et la continuité sociale, sont nécessaires voire incontournables pour l'étude de messages cryptés.

23-§ Le manuscrit que nous allons étudier est dans une situation critique d'étude et contient à lui seul l'ensemble des cas défavorables pour réussir son analyse ; en ce sens, le contexte locatif et datif est approximatif, il n'existe aucun autre manuscrit qui revêt des apparences similaires, seule un semblant de continuité sociale existe dans sa possession mais non dans son langage. Autant dire qu'il prend la forme d'un problème avec information très minimale.

24-§ Cependant, nous disposons d'*Artefact* utiles pour conduire l'étude de messages cryptés. Nous allons en faire usage et nous manierons nos outils dans des méthodes qui, même si elles ne nous permettent pas de décrypter pleinement ce manuscrit, nous mèneront vers une réduction des hypothèses et elles nous conforteront pour des études ultérieures.

Outils

25-§ Il nous faut vous indiquer qu'il n'existe pas d'école où l'on enseigne la cryptanalyse. Certes, il en existe où la cryptologie et la cryptographie sont dispensées mais il n'en est point où la façon de faire, de conduire une analyse et de détecter la corde sensible d'un cryptogramme, soit enseignée. Il est remarquable, et l'histoire en témoigne, que

[19] Il rejeta : les signaux électriques et sonores parce qu'ils nécessitaient une source d'énergie, les signaux olfactifs car ils ne perdurent pas et les idéogrammes car ils nécessitent des conventions précises.

le cryptanalyste doit ses connaissances à son autoformation[20] et de ce fait il est enclin à emprunter des chemins pluridisciplinaires aux risques d'être exposé aux foudres des sciences compartimentées[21] pour mener à bien son travail. Synthétiquement, nous décrivons trois d'entre elles : les langues, les mathématiques et l'informatique.

26-§ Les mathématiques constituent un ensemble d'outils fondamentaux dans l'énumération, la combinatoire et la permutation, des symboles ; mais aussi dans leurs capacités à montrer des périodicités variables quand les textes de symboles sont différemment ordonnés.

27-§ Les langues en cryptanalyse appartiennent à une sphère d'étude où l'on s'intéresse à leurs signes caractéristiques et à leurs modifications en fonction des contextes de communication.

28-§ Entre ces deux connaissances, mathématiques et linguistiques, s'intercale l'informatique comme, précieux outil réducteur de temps de traitement, et, système de formalisation de méthodes rationnelles qui puisent dans les cryptogrammes des données comparables ou opposables à des caractères linguistiques référencés.

---

[20] Alfred EWING, alors directeur de l'Enseignement maritime de l'armée Anglaise engagée dans cette première Guerre Mondiale, ne savait que faire de tous ces messages cryptés et captés par les stations de radio navales et commerciales. L'Amirauté n'était pas dotée de service de traitement des cryptogrammes ennemis. EWING s'intéressa à ces énigmes mais n'avait aucune idée des méthodologies cryptanalytiques. Il créa sa propre formation selon trois axes : il étudia, les questions cryptographiques dans les livres de la bibliothèque du British Museum, les structures des codes commerciaux, et recruta des instructeurs qui connaissaient l'allemand. La synthèse des trois formait un bon début bien que la pratique se montrait laborieuse dans les premiers temps.

[21] « Restreindre une problématique à un domaine qui en interdirait le dénouement est une faute de méthode ». VAUDENE Didier, Thèse de Doctorat d'état, Une contribution à l'étude des fondements de l'informatique, Université PARIS VI, 1992.

Introduction

•

LE MANUSCRIT de Voynich est une énigme et notre intention est de la résoudre. Nous n'avons pas la prétention d 'apporter sa solution dans notre présente étude mais nous désirons contribuer à son étude.

29-§ Jusqu'alors, la seule étude universitaire du manuscrit de Voynich fut faite, en 1969 par Jeffrey KRISCHER, lors de son *graduate study* à l'université de *Harvard*. Il l'intitula « The Voynich manuscript » et constitua principalement[22] une étude des différentes perceptions holistiques des analystes qui étudièrent le manuscrit. La thèse de Jeffrey KRISCHER a l'honneur de la primauté mais elle ne constitue pas une nouvelle approche cryptanalytique.

30-§ Notre problématique est différente, l'intitulé de notre étude en témoigne. Nous plaçons notre *artefact* au service du décryptage de cet ouvrage, nous n'avons pas d'autres buts que celui-ci. Nous, qui nous inscrivons dans le projet EVMT[23], proposons de poursuivre et de propager son étude en espérant créer de nouvelles motivations de recherches.

31-§ Pour cela, nous commençons par mettre en exergue les trois problématiques essentielles incontournables. Nous nous demandons si, il existe un message sous-jacent au texte ou si, il est simplement dans sa forme naturelle. La deuxième et la troisième question reposent sur la nature, du chiffrement, du codage, du système d'écriture, employé : existe-t-il une substitution cryptographique ?, quelle est sa nature ?, et, est-ce que le manuscrit révèle une nature d'encryptage autre que ces substitutions ?

32-§ La diversité et la combinatoire des hypothèses fournies par ces trois problématiques mettent en évidence la difficulté de l'élaboration d'un cheminement déductif. Nous comprenons que la comparaison d'événements par le simple système binaire *concordance-différence* est insuffisant pour la *réfutation* et la *validation* des hypothèses.

---

[22] Il proposa une méthode de discrétisation des symboles du manuscrit en codes informatiques par un procédé de lecture optique devant être utilisé pour la lecture des idéogrammes chinois. Bien que pourvus de méthodes de calculs —statistiques, probabilistes, informationnels— son étude n'était pas orientée pour mener une cryptanalyse du manuscrit.

[23] Nous ne faisons pas de distinction, entre le premier et le second groupe, et nous considérons que la dynamique de rassemblement autour du même intérêt sera la condition *sine qua non* pour aboutir un jour à la solution. EVMT — Project européen— : *Electronic Voynich Manuscrit Transcription.*

33-§ Il est primordial d'introduire une troisième valeur indispensable à la méthodologie cryptanalytique; la *contrariété* dont l'objet est d'apporter un élément de réflexion supplémentaire sur notre propre *artefact*. La conséquence directe se ressent dans notre capacité à réemprunter, rejeter et interpréter à nouveau les expériences, et en cela, elle nous montre que notre attachement à la comparaison analytique *objet-référence* empêche une cryptanalyse dépourvue d'induction.

La lettre de MARCI

34-§ Nous sommes en 1912, Wilfrid Voynich est un commerçant de livre ancien. Au cours d'une investigation en Italie, il découvre la Villa Mandragone dans laquelle une bibliothèque recèle de nombreux ouvrages de valeur. Un manuscrit sans couverture s'arrête entre ses mains. Une lettre[24] écrite en latin l'accompagne

Révérend et distingué monsieur,

Père en Christ,

35-§ *Ce livre, légué à moi par un ami intime, je vous le destine, mon très cher Athanasius, comme il venait en ma possession, j'ai été convaincu qu'il ne pouvait être lu par personne d'autre que vous.*

36-§ *Le précédent propriétaire de ce livre demanda une fois votre opinion par lettre, copiant et vous envoyant une partie du livre, lequel croyait que vous étiez capable de lire le reste, mais il refusa, jusqu'à présent, d'envoyer l'original. Il se voua à un déchiffrement pénible et courageux, comme vous-mêmes avez fait cette tentative je vous le transmets, et il abandonna toute espérance en même temps que la vie le quitta. Mais son dur travail demeura sans solution, tels les Sphinx qui n'obéissent qu'à leur maître, KIRCHER. Acceptez maintenant ce présent, tel qu'il est et bien qu'il soit en souffrance, en témoignage de mon affection pour vous, et pulvérisez son armure, si il y en a une, avec votre habituel succès*[25].

37-§ *Docteur Raphaël*[26]*, tuteur en langue Bohémienne de Ferdinand III, alors roi de Bohème, me raconta que ce livre avait été cédé à l'empereur Rudolph*[27] *par un inconnu et pour la somme de six cents ducats. Il pensa que l'auteur était Roger BACON, l'anglais. Sur ce point, je suis sans avis ; c'est à vous de nous dire quelle*

[24] Traduction à partir de la lettre de TILTMAN (1968) que nous plaçons dans l'esprit *traduttore, traditore.*

[25] MARCI faisait référence au décryptage des hiéroglyphes Egyptiens par KIRCHER bien que par la suite ils s'avéraient faux.

[26] Raphaël MISSOWSKY (1580-1644).

[27] Rodolphe II de Hongrie et de Bohème (1552–1612).

opinion nous pourrions avoir.

A la faveur et à la bonté de qui je me confie sans réserve.

A la disposition de votre Révérence.

Prague, 19 août 1665 ? 1666.

38-§ étrange lettre pensa Voynich, étrange manuscrit. Lorsque nous avions découvert son existence au cours d'un travail de recherche concernant *la cryptanalyse de textes chiffrés* : il apparaissait, comme aujourd'hui, être l'objet le plus résistant à dévoiler ses secrets. Depuis que Voynich l'avait sorti de son sommeil séculaire, les analyses avaient échouées dans des conclusions aussi hâtives qu'incroyables, et fait étonnant, les cryptanalystes professionnels ne s'intéressèrent que tardivement à cette énigme et n'eurent pas plus de succès. Cette accumulation de non-aboutissements faisait accroître le caractère énigmatique de ce manuscrit ; mais à la fois, elle montrait une limite de la méthode analytique : toutes deux contribuaient au découragement de son étude.

Etait-il raisonnable d'aborder une problématique qui usa et rejeta l'ambition de décrypteurs pourtant reconnus comme experts ?

39-§ Nous savons que le cryptanalyste doit son *artefact* à l'autoformation ; aussi à chaque cryptanalyste correspond une *façon de faire* propre aux connaissances et au savoir qu'il a engrangés et organisés sous formes de méthodes. De ce fait, la question, que nous avons soulevée à propos de la « rationalité » de l'acte, d'étudier cette problématique, doit être reformulée en :

est-il raisonnable de ne pas aborder l'étude du manuscrit de Voynich sous prétexte que d'autres cryptanalystes, aux compétences particulières, n'ont pas abouti ?

40-§ Chacun répondra comme il l'entend ; nous avons pris l'initiative de ne pas ignorer cette énigme et de tenter d'apporter des éléments de réponse par le biais de nos compétences particulières issues de notre autoformation à la cryptanalyse.

Les éléments du doute et les problématiques essentielles

41-§ Les hypothèses sont nombreuses car nous ne connaissons pas les méthodes cryptographiques utilisées pour crypter l'écriture du manuscrit. En fait, rien ne dit que ce manuscrit soit crypté, ou codé, si ce n'est notre incapacité à le comprendre. Autant, quand un service du chiffre intercepte un message « Ennemi », il présume que le message transmis possède une solution, dans le cas du manuscrit de Voynich, nous ne sommes pas certains de cette évidence. Nous ne connaissons pas le langage utilisé. Nous ne connaissons pas le système d'encryptage. Nous ne savons pas en quel endroit, à quel époque et par quelle personne, ce manuscrit a été écrit. Et finalement,

nous ne sommes pas certains du sujet discuté [IMPE1980]. Ce manuscrit décrit l'ensemble des problématiques qu'un cryptanalyste rencontre dans un cas extrême d'analyse.

42-§ Les différentes hypothèses occupent trois axes de recherche. La première orientation concerne la nature du texte clair. La deuxième concerne la nature de la substitution : est-elle simple ou multiple ? Et la troisième orientation étudie les méthodes de transformations autre que les substitutions.

La nature sous-jacente du texte

43-§ Quatre hypothèses concernent la nature du texte clair. La première idée est que le manuscrit est crypté à partir d'un texte latin **(P1)**[28] ; toutefois, l'hypothèse n'est pas exclue que le texte clair soit d'une autre langue naturelle **(P2)**. Le manuscrit pourrait être aussi le produit d'une codification ou d'un langage synthétique **(P3)** avec association d'idéographies et de caractéristiques de langue naturelle [IMPE1980]. La quatrième hypothèse s'inspire de l'hypothèse précédente : le système de représentation serait purement idéographique sans conservation des caractéristiques de la langue naturelle **(P4)**.

L'hypothèse de la substitution

44-§ Les orientations d 'analyses sont au nombre de huit. La substitution monoalphabétique était la méthode d'encryptage la plus probable car la plus courante et la plus facile à mettre en œuvre, puisque, chaque caractère du texte clair est remplacé par un symbole de Voynich **(E1)**. La deuxième méthode hypothétique consiste à remplacer chaque lettre par deux ou trois symboles de Voynich **(E2)**. A l'opposé de ces deux hypothèses, il est envisageable que deux ou trois lettres du texte clair soient substituées par : un seul symbole **(E3)**, deux symboles ou trois symboles de Voynich **(E4)**. D'une façon plus générale, nous pensons que la dimension des groupes substitués de lettres évolue dans les deux textes **(E5)** ; en ce sens que l'alphabet de substitution change en fonction des parties du texte clair **(E6)**.

45-§ Parfois, un groupe de lettres forme un mot ou un concept[29] ; ce groupe est alors remplaçable par un symbole ou une chaîne de symboles de Voynich comme il est d'usage dans la sténographie **(E7)**. La dernière hypothèse est que la substitution soit polyalphabétique **(E8)**.

Les autres transformations

46-§ Six points différents détaillent ce dernier axe d'hypothèses. Il est probable que le texte clair n'a pas subi de suppression ou d'ajout de lettres **(T1)**. La deuxième

[28] Référence introduite par Maria d'Império [IMPE1980].

[29] Entités Lulliennes.

hypothèse contredit la première : les voyelles sont absentes **(T2)** du texte et d'une façon globale les mots sont arbitrairement abrégés et représentés par certaines lettres **(T3)**. Des caractères inutiles sont probablement insérés au texte de façon à dérouter la cryptanalyse **(T4)**. La cinquième et la sixième hypothèses reposent sur le principe de transposition, de lettres ou de syllabes, interne aux mots **(T5)** ou tout au long du texte **(T6)**.

Implications fondamentales des trois problématiques

47-§ L'analyse des cryptogrammes nécessite trois connaissances particulières qui se conjuguent selon l'état de connaissance que nous avons de chacune d'entre elles. Avoir idée de la nature de la langue utilisée pour rédiger le message *démarqué*[30] est un sérieux atout pour mener à bien la cryptanalyse du message à présent crypté ; cependant, l'encryptage est un second langage qui dénature l'information précédemment claire ; il est de juste que si il est connu[31], en partie ou intégralement, il représente un danger pour l'intégrité du message. Enfin, la troisième connaissance est commune aux deux précédentes ; la structure d'énonciation de ces deux langages est réductible en un nombre de règles[32] qui guident le cryptanalyste dans sa quête d'analogies.

48-§ La conséquence immédiate du manque de connaissances sur l'ensemble des procédés intervenants dans l'encryptage de l'information est un accroissement géométrique du nombre des hypothèses émises pour résoudre le cryptogramme. L'origine de cette progression multiplicatrice est double.

L'émergence de l'hypothèse cryptanalytique se lie au monde de l'intuition en étroite interaction avec le monde rationnel de la méthode scientifique.

49-§ Les différents *artefact,* propre à chaque analyste, génèrent des solutions qui parfois s'éloignent de la démarche scientifique, au sens où l'expérience est reproductible et admet la réciprocité entre méthodes d'encryptage et méthodes de décryptage, et conduit inexorablement l'analyste dans son unique perception de la réalité cryptanalytique : la solution proposée n'a alors plus de *sens partagé* et pose le problème de la démarcation entre la validation et la réfutation d'une hypothèse.

---

[30] Neutralisation des caractères reconnaissables et ambigus pouvant constituer une menace pour l'intégrité du système d'encryptage.

[31] Ceci pose le problème de la normalisation. Un algorithme d'encryptage reconnu par les différents intervenants de la communication sécurisée a pour conséquence une fragilisation du secret (cas des échanges bancaires —norme ETEBAC5).

[32] La connaissance de la syntaxe d'une langue naturelle, ainsi que la connaissance de la syntaxe d'écriture des codes commerciaux et militaires sont des indicateurs forts pour l'analyse des messages cryptés.

50-§ L'expérience des tentatives de cryptanalyses du manuscrit de Voynich montre qu'on tend à rechercher inconsciemment ou consciemment des éléments propre à étayer[33] une hypothèse plutôt qu'à la réfuter ; en ce sens, l'*a priori* est nécessaire pour, conduire, réduire et conjuguer des hypothèses en solutions ; mais en même temps, il est dangereux du fait même qu'il induit une réduction des hypothèses parmi lesquelles se trouvent probablement la solution.

La seconde cause de la multiplicité du nombre des hypothèses et de la raison du non-aboutissement à la solution est la dépendance de l'analyse vis-à-vis des hypothèses linguistiques.

51-§ Le passage entre la constatation de structures particulières vers la formulation d'hypothèses linguistiques, remarquées analogues, est démonstratif de la précaution méthodologique qui caractérise l'*artefact* du cryptanalyste ; le glissement le plus adéquat possible retarde le recours aux références linguistiques pour prolonger l'étude de l'objet dans ses structures ; la méthode recherchée et pratiquée doit être indépendante du langage hypothétique par l'*évitement* de l'*induction* entre le cryptogramme (objet) et les références linguistiques. Or, la problématique se trouve précisément dans la prise de décision de passer d'un état de connaissance de la structure du cryptogramme vers son équivalent intelligible.

52-§ Pour cela, la cryptanalyse se fie naturellement à trois principes qui accordent, à des faits, des *concordances*, des *contrariétés* et des *différences*. Ces trois noms définissent la comparaison dans l'analogie des faits. Ils contribuent à la réduction du champ des hypothèses dont l'enrichissement de la valeur informative grandit dans le sens *concordance-différence-contrariété*.

Il est notable que la *contrariété*[34] est la comparaison qui apporte le plus d'intérêt pour la simple raison qu'elle montre un manque de connaissance ou un dysfonctionnement dans l'*artefact*, et , elle rappelle le problème de la validation et de la réfutation des hypothèses.

53-§ La *contrariété* est obtenue quand la conjoncture d'hypothèses aboutit à une conclusion non observable dans le cryptogramme. Il existe en ce cas un cheminement de penser dont au moins une des idées s'articule difficilement dans le raisonnement. Or, puisque cette méthodologie puise dans une compétence unique de formalisation, il existe une incohérence que cette *contrariété* révèle et renvoie le cryptanalyste dans un état de recherche de nouvelles méthodes ou de modifications de méthodes préexistantes.

---

[33] Cette attitude n'est point anormale puisque le manque de connaissances relatif à ce manuscrit montre qu'il est plus aisé de trouver des éléments défavorables à toutes hypothèses.

[34] *Concordance* et *différence* étant les références habituelles du système de parité *Vrai-Faux*..

54-§ Le manuscrit de Voynich est l'objet[35] idéal pour mettre en évidence les limites de l'étude par analogies et pour remettre en question des cheminements méthodologiques entre les effets constatés dans un cryptogramme et les causes liées à ces effets.

Thématiques de l'exposé

55-§ Le non-aboutissement à une solution acceptable, est le résultat d'une conjugaison de connaissances non adéquate à la problématique soulevée. Le choix des méthodes conditionne l'élaboration du chemin déductif. Les expériences passées, constituent des parcours de pensée, que nous devons considérer dans leurs inspirations en déterminant l'élément causal de l'égarement de l'analyste pour une solution non méthodique. Ainsi, les idées constitutives de ces inspirations doivent être à nouveau visitées dans leur valeur d'hypothèse ; certaines d'entre elles ne pourront être que rejetées mais d'autres demeureront suffisamment probables pour être intégrées dans notre cheminement déductif :

réemprunter, rejeter et interpréter à nouveau les expériences passées seront les actions constitutives du nouveau sédiment à partir duquel une nouvelle approche pourra se développer.

56-§ Les statistiques et les probabilités seront incontournables. Les indices qu'elles mettent en évidences sont précieux dans l'exercice de réfutation et de validation d'hypothèses. Cependant, il ne pourra pas être envisagé de conforter une hypothèse par la seule valeur informative d'une unique mesure. Il est évident que l'interprétation de calculs est sensible à la personnalité de l'analyste. Seul le recoupement d'informations sera estimable dans ses implications. La conséquence directe, dans notre méthodologie, sera que nous irons à la conclusion en opposant les différentes hypothèses d'une même thématique ; mais aussi en testant leurs valeurs à travers l'ensemble des thématiques abordées.

57-§ Les statistiques et probabilités sont insuffisantes pour analyser le manuscrit indépendamment de la référence linguistique bien qu'elles soient nécessaires pour quantifier une attitude et qualifier une règle comportementale. Nous savons que la pluralité des langages nous oblige à délaisser la comparaison analogique entre cryptogrammes et langages ; et fait remarquable qui en découle, nous n'avons que peu de connaissances sur la structure du manuscrit, de ses mots et de ses symboles.

Comment se détacher de cette idée de référence, qui nous oblige à rechercher des structures particulières parce que l'hypothèse implique leur nécessaire existence ?

[35] Ceci est une incidence mais pas un but qui nous le rappelons est la résolution de l'énigme.

58-§ Cet aspect n'a pas été perçu dans les cryptanalyses précédentes. Les études menées n'ont donc pas rendu les traits du cryptogramme mais, seulement, un aperçu déformé par l'hypothèse de ce qu'il devrait être. Nous recherchons la méthode, devant nous éviter de reproduire cette même erreur, en étudiant la structure du manuscrit sous trois aspects.

59-§ Nous nous intéressons à la structure globale du manuscrit et à la recherche de sous parties distinctes ; nous essayons de répondre à la question

Est-ce que ce manuscrit est un unique cryptogramme ou est-il un agrégat de textes différemment encryptés ?

60-§ Prolongeons cette suggestion interrogative aux mots du manuscrit, en recherchant leurs structures et processus de création, et nous nous questionnons sur leur réalité en remettant en cause que le mot est bien l'entité qui se reconnaît selon nos mêmes critères de distinctions ; de toute évidence, nous devons en douter. C'est en cela que la présente étude se doit de *dépasser* la simple recherche d'analogies linguistiques pour une recherche structurelle indépendante du mot.

61-§ La voie que nous explorons s'inspire des faits observés dans la nature à laquelle nous attribuons des aptitudes aux jeux d'imbrications de motifs répétitifs, asymétriques et symétriques. Ces constats si clairement montrés en cristallographie ne le sont pas en cryptographie qui pourtant, elle-même, se confronte à la problématique de l'ordre et du désordre.

Cheminement de l'exposé

62-§ Nous n'avons pas la prétention d'apporter la solution à une énigme vieille de plus de quatre cents ans. La tentation d'aboutir est grande et compréhensible ; toutefois, nous ne devons pas être enclins à la précipitation de risque d'être trop inductif. Notre précipitation serait néfaste pour la cryptanalyse qui se doit de résoudre, en partie ou en totalité, la problématique du *sphinx*. Nous connaissons les difficultés ; il nous faut conjuguer des connaissances, dont la combinatoire trop importante d'hypothèses nous pousseraient vers la tentation de la simplification de l'analyse, en évitant de réduire le champ de ces conjugaisons en convictions propres et indépendantes de cheminements méthodiques.

63-§ Notre exposé reprend les hypothèses et les constats de travaux précédents ; puis, nous poursuivons nos analyses, en nous détachant progressivement de la dépendance linguistique, en étudiant la combinatoire des lettres du manuscrit et en recherchant les jeux de construction de motifs.

64-§ La *première partie* [39–90] est une prospection dans l'état de l'art actuel. Nous y découvrons, ce à quoi ressemble le manuscrit et, quelle est son histoire. Surtout, nous racontons les expériences passées, leurs dérives, et la progression de leurs hypothèses

et de leurs constats.

La diversité des cheminements d'idées nous contraint à réétudier, interpréter à nouveau les statistiques, les probabilités et la combinatoire des symboles de Voynich.

65-§ La *deuxième partie* [93–200] récupère les travaux de transcription du manuscrit. Elle utilise les procédés statistiques, probabilistes, pour une mesure du comportement des lettres et des groupes de lettres de Voynich. Dès lors, bien que nous montrons que la combinatoire de ces symboles tend à ressembler à un système de *langue synthétique*, nous ne pouvons pas encore écarter les autres possibilités.

Plutôt que de rechercher les indices qui confirmeraient l'hypothèse de la langue synthétique, nous prospectons de nouvelles structures de motifs dont la finalité est de contribuer aux recoupements des possibilités.

66-§ La *troisième partie* [201–282] apporte des éléments de réponse sur l'interrogation : qu'entendons-nous par *motif* dans une cryptanalyse ? Les réponses que nous formulons contribuent à définir notre propre système de recherche en motifs, adéquats à leur nécessaire indépendance, vis-à-vis d'un langage hypothétique de référence. La solution puise dans des constats naturels de symétries et de redondances qui mettent en valeur le degré de construction textuel ; mais aussi d'en faire la représentation structurelle dont celle du manuscrit de Voynich montre des singularités utiles pour la compréhension des méthodes probablement utilisées dans sa rédaction.

I

Le manuscrit de Voynich

14 novembre 1998 —Première édition

14 novembre 1998 —Première édition

Partie I

Le manuscrit de Voynich

•

Sommaire

67-§ Le manuscrit de Voynich est une énigme totale qui cache non seulement le sujet discuté mais aussi sa provenance. Il apparaît comme une *génération spontanée,* dans un siècle tourmenté par les Saintes Inquisitions dont des savants comme Giordano BRUNO payeront de leur vie leurs propos érudits. Nous ne pouvons pas être sûr de la période à laquelle le manuscrit a été écrit mais quelques indices nous permettent de spéculer sur son origine. Le manuscrit est orné de représentations graphiques étranges auxquelles certains s'accordent à dire qu'elles sont les preuves datives et circonstancielles du sujet manuscrit. Seulement, tous ne sont pas d'accord, la datation est sujette à des fluctuations de plusieurs siècles qui ne permettent pas de déterminer l'auteur et la nature des informations contenues dans le manuscrit.

•

LA PREMIÈRE description succincte mais exhaustive du manuscrit de Voynich fut faite par Hans P. KRAUS[36]. Dans son catalogue de vente paru en 1962, KRAUS décrit[37] le manuscrit comme : *Le manuscrit le plus mystérieux au monde. Le manuscrit chiffré*[38] *de Roger BACON.*

Images, figures et textes

68-§ En fait, le manuscrit de Voynich est de petites dimensions. Il fait un peu plus de 15 cm de large pour 23 cm de long. Il est composé de deux cent trente-quatre pages[39] manuscrites[40] et dessinées. Ces dessins sont parfois reconnus comme les signes du zodiaque, les signes de la cosmographie et de l'alchimie mais beaucoup d'autres restent mystérieux et plus particulièrement les dessins de *baignoires* reliées par des *tubes* où une *dame nature* semble avoir un rôle actif dans la signification de ces dessins ; elle prend d'une main ce qu'elle donne de l'autre main.

69-§ Le manuscrit se compose de cinq parties fondamentales. La première partie comporte cent douze pages. Les dessins qui ornent les folios sont des fleurs et des plantes. Cette section est appelée « *Herbier* ». La section suivante est un ensemble de trente-quatre pages qui traitent d'astrologie, si bien sûr, nous posons le principe que le texte est lié

---

[36] Libraire de livres anciens à New York, 1960.

[37]

> *(Bacon, Roger ?) Manuscrit chiffré sur vellum texte écrit dans un script secret, apparemment basé sur des caractéres Roman écrits en minuscules, irrégulièrement disposés sur les pages. 102 feuilles (sur 116 ; manque 14 feuilles) incluant 7 feuilles pliées quadruple-folio ; 3 feuilles pliées triple-folio. Avec des marques de signature ajoutée (du 15ème au 16ème siècle) 1–11, 13–58, 65–73, 75–90, 93–96, 99–108, 111–116. Avec à peu près 400 dessins de sujets botaniques dont plusieurs occupent la page entière ; 33 dessins d'astrologie ou astronomie, contiennent environ 350 figures d'étoile ; et 42 (biologie ?) dessins, la plupart composés de figurines humaines. Les dessins sont colorés avec une multitude de nuances de verts, marrons, jaunes clairs, bleus, et de rouges foncés. De dimension 160 mm de longueur par 230 mm de hauteur. Détenu par Rudolph II (Règne de 1576–1611) ; Jacobus Horcicky (Sinapius) de Tepenecz ; Joanus Marcus Marci de Cronland (1666) ; Athanasius KIRCHER, S.J. ; et Wilfrid M. Voynich. Accompagné par une lettre signée par Joanes Marcus Marci, présentant le livre à Athanasius KIRCHER. Pas d'indication de lieu ni de date (15ème siècle, ou avant).*

[38] Traduit de l'anglais « *Cipher* ».

[39] Parmi les deux cent trente-quatre pages, quarante-deux sont manquantes.

[40] Les dessins sont parfois en couleurs (Figure 2 Folio 33v des Tournesols (Herbier). Page 48). Le manuscrit est formé de cinq sections principales.

aux dessins. La biologie est présente dans la troisième partie du manuscrit. Nous y trouvons ces femmes rondes comme celles des nus de RUBENS. Mais celles-ci sont liées par des tubes aux apparences organiques qui enlèvent quelque attirance esthétique. Cet ensemble constitue dix-neuf pages. La quatrième section est appelée « *Pharmacie* » ou « Pharmaceutique », elle commence à la page cent soixante-sept et finit à la page deux cent onze. Finalement, la cinquième et dernière partie est essentiellement une succession de « formules » ou de *Recettes*.

70-§ Le manuscrit est actuellement dans la bibliothèque Beinecke Rare Book Room de l'Université de Yale. Il est enregistré sous le numéro d'accès MS408.

Figure 1 Folio 77v des Dames avec des « tubes » (Biologie).

Figure 2 Folio 33v des Tournesols (Herbier).

Figure 3 Folio Les dames, la mare et les animaux 79v (Biologie).

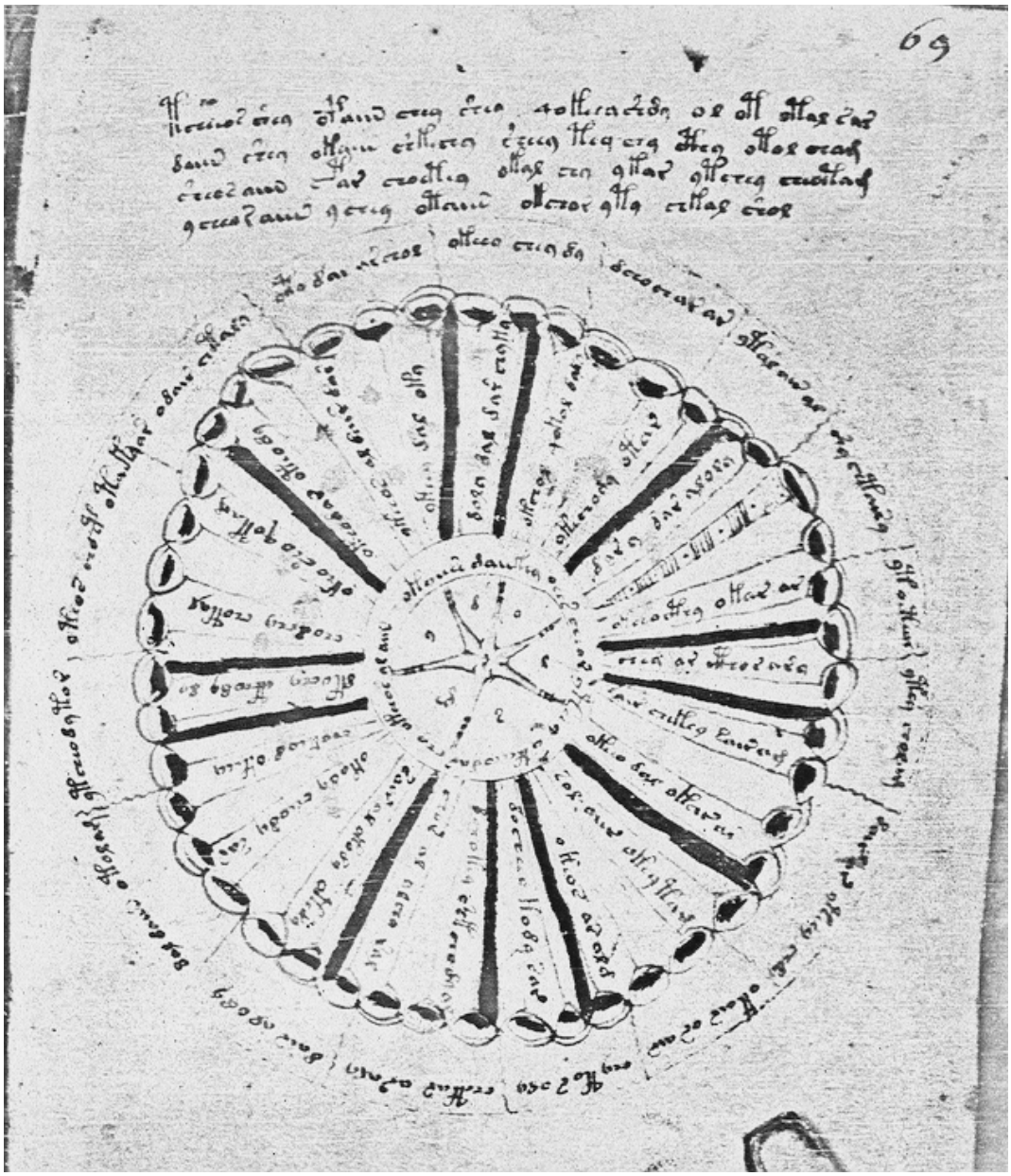


Figure 4 Le folio 69r est une rosette dont le cœur est un hexagramme (Astrologie).

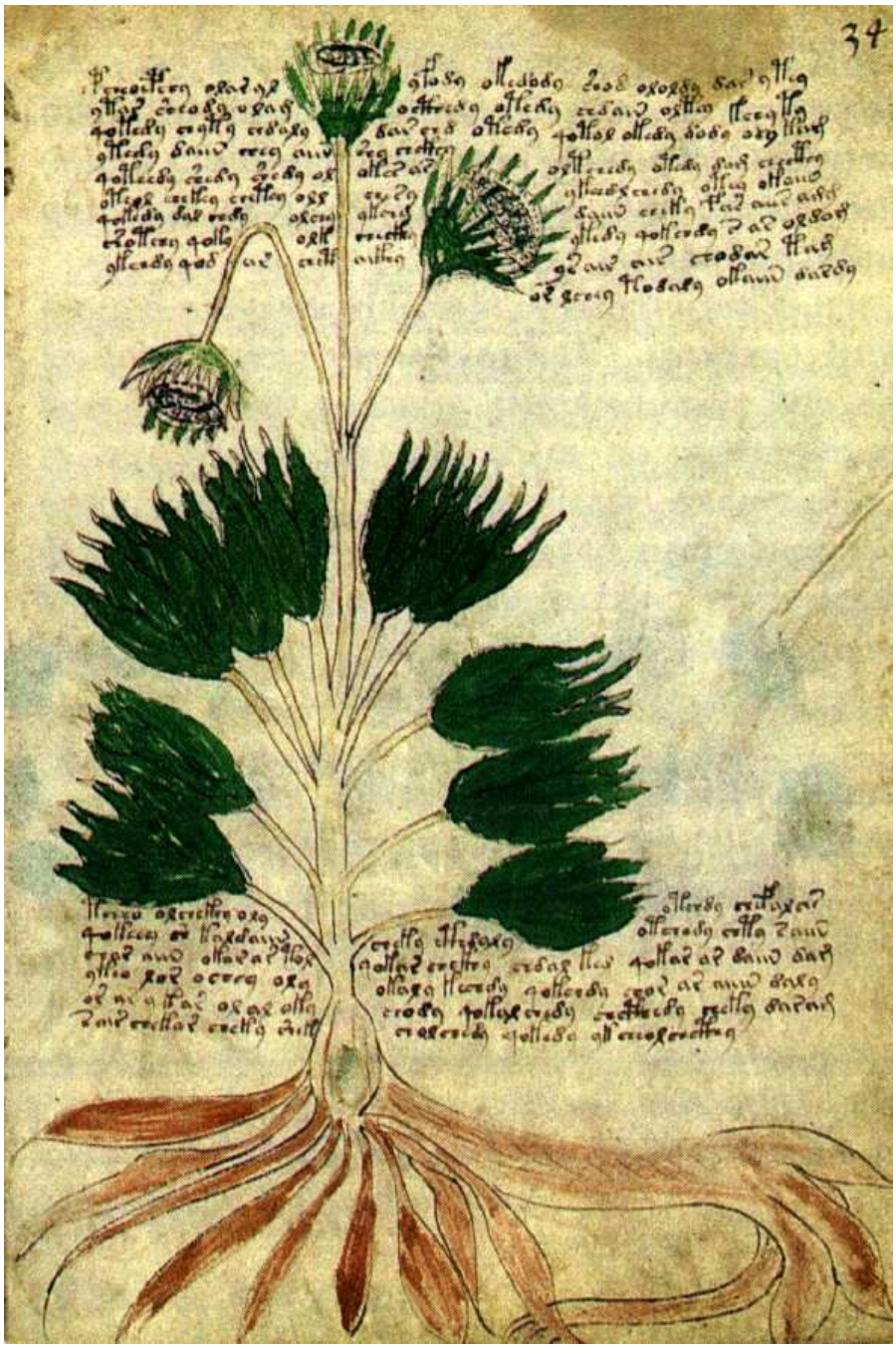


Figure 5 Le folio 34r est apparemment une plante : peut-on l'associer à l'arbre lunaire alchimique ? (Herbier).

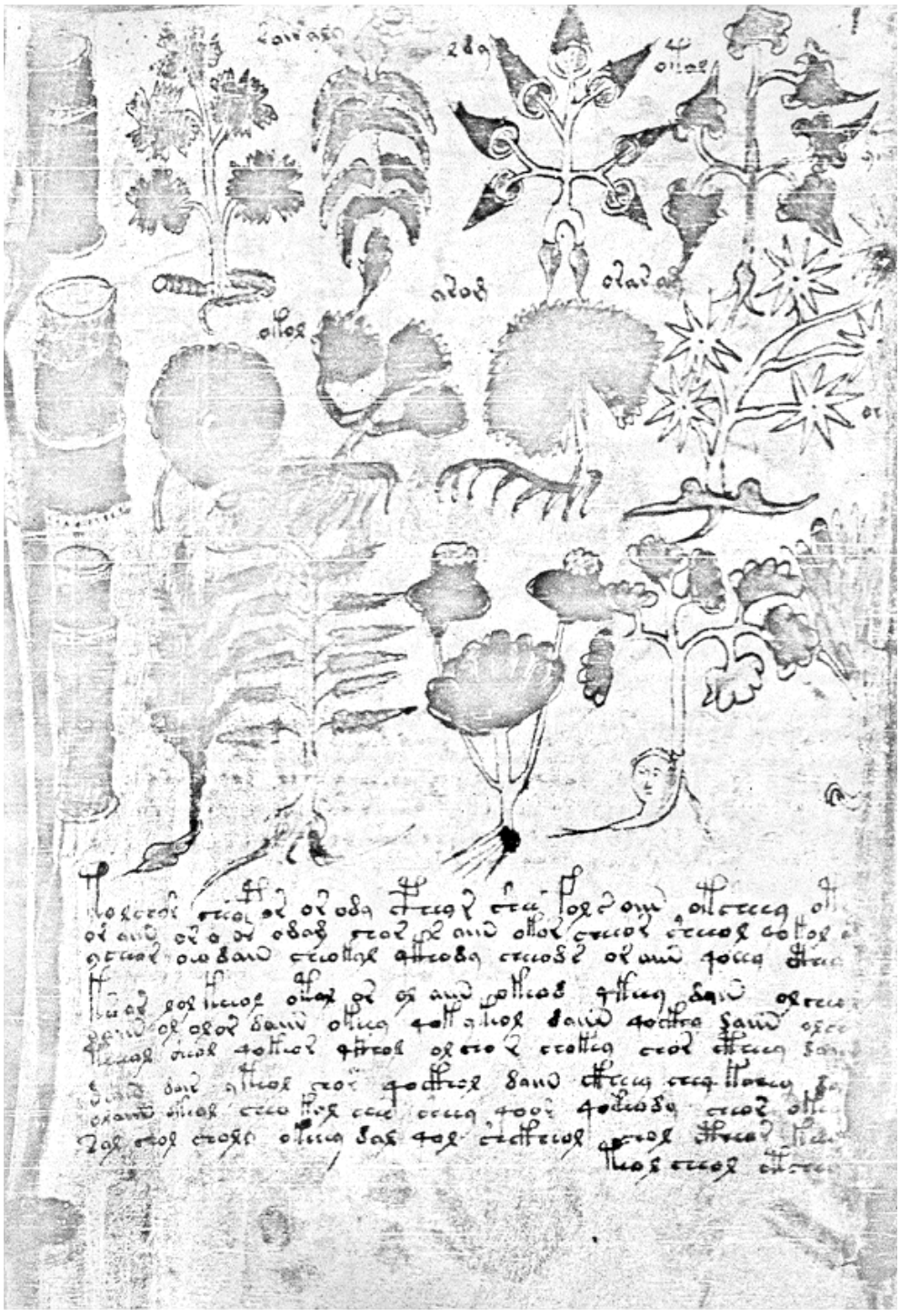


Figure 6 Le folio 105v avec un visage humain sur la racine (Pharmacie).

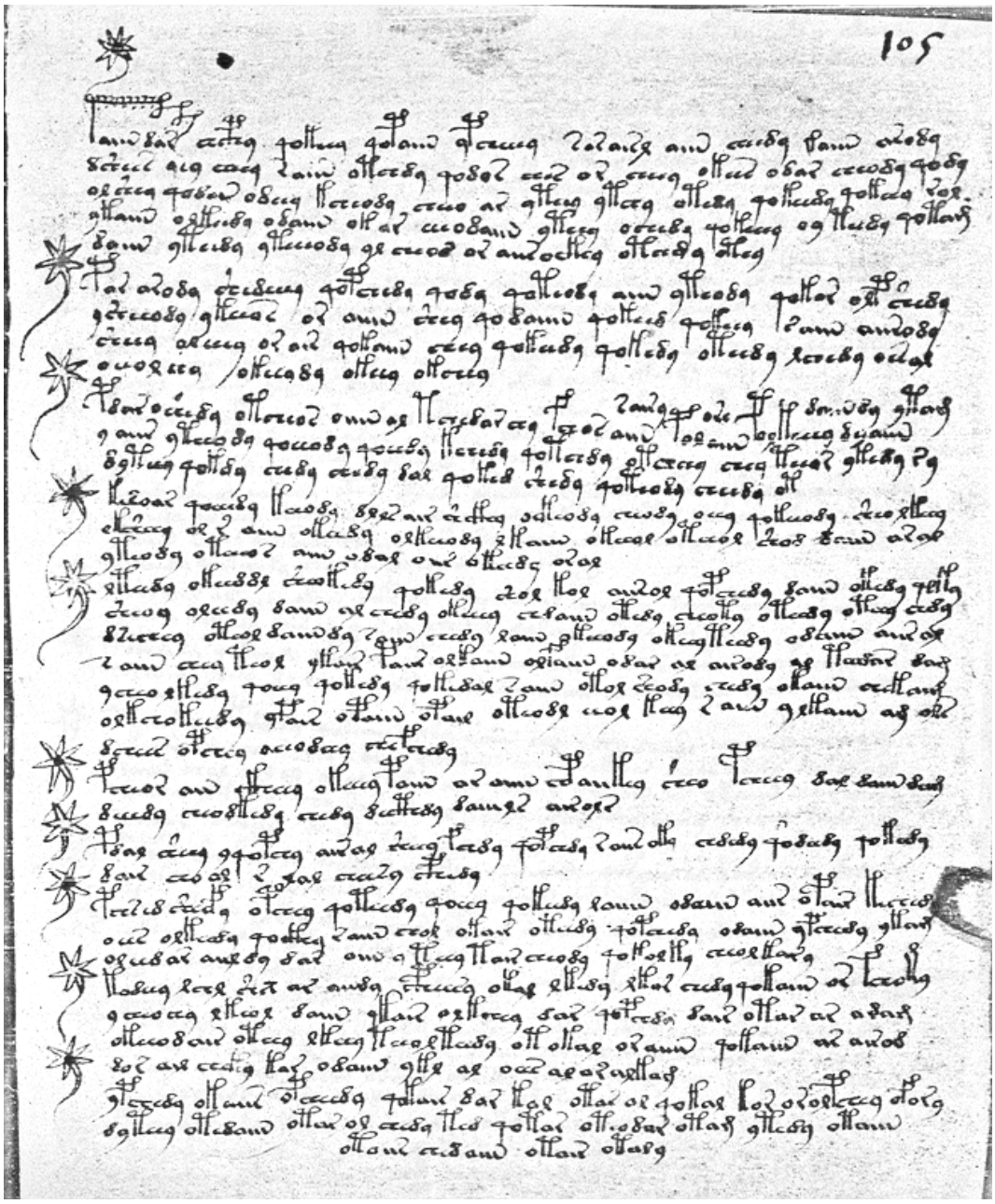


Figure 7 Le folio 105r est une liste indexée d'étoiles (Recettes).

Datation

71-§ Le manuscrit de Voynich apparaît comme le plus mystérieux des manuscrits et son histoire est parsemée d'amnésies qui ne laissent entrevoir que des séquences *Félliniennes*[41] d'histoires « omnibus ». En quelle année a-t-il été écrit ? Nous ne pouvons donner qu'un *terminus ad quem* c'est-à-dire une date approximative qui admettrait une fluctuation de plusieurs siècles.

72-§ Il semble avoir été écrit au 13ème siècle bien que certains détails comme les *fleurs de tournesol*, similaires à celles de VAN GOGH[42], laissent penser que le manuscrit serait postérieur à la découverte des Amériques en 1492, fait constater O'NEIL Hugh [NEIL1944]. En tout cas, il est antérieur à 1586 date à laquelle[43] John DEE tenta de le décrypter. Il considéra que ce manuscrit devait être celui de Roger BACON. Son hypothèse n'était pas qu'intuitive car il connaissait la vie et les écrits de ce moine Franciscain du 13ème siècle dont un des ouvrages —*De l'admirable pouvoir et puissance de l'art, & de nature, ou eſt traicté de la pierre philoſophale*— [BACO1557] énonçait sept[44] façons de crypter un message que le « vulgaire » n'était pas en mesure de lire.

> **Constat 1 Roger BACON — *De l'admirable pouvoir et puissance de l'art, & de nature, ou eſt traicté de la pierre philoſophale*— détaille les sept façons de dissimuler des écrits.**

73-§ La lettre de MARCI est riche en renseignements. Elle permit de reconstituer une chronologie de 1608 à nos jours[45]. Avant 1608, le manuscrit semble avoir été étudié par John DEE. Voynich raconte que Arthur[46] DEE, alors fils de John DEE, avait eu

---

[41] En référence au procédé cinématographique de Fellini (Histoire de Rome).

[42] En août 1888 à Arles, Vincent VAN GOGH a peint quatre versions des tournesols puis trois autres en 1889. Il est remarquable que ces couleurs et ces formes soient si proches. Nous ne savons pas si les tournesols du manuscrit de Voynich sont de réelles fleurs de tournesol. Cependant, il est devenu coutume de les appeler ainsi. Cette appellation est maintenant devenue le « fer de lance » de ceux qui pensent que le manuscrit ne peut pas être de Roger BACON.

[43] Entre 1584 et 1588.

[44] Il conseille l'emploi « d'énigmes ou de choses figurées » pour dissimuler ce que l'on écrit. L'insinuation est la deuxième de ses méthodes, elle consiste en une « façon de parler » qui ne permet pas aux autres « le vulgaire » de comprendre ce qui se dit. Puis la troisième méthode est l'utilisation d'un alphabet sémitique qui évite la cryptanalyse par l'étude des lettres de hautes fréquences. La quatrième façon de faire est l'utilisation de lettres de différents alphabets dont la conséquence est la représentation multiple. La cinquième méthode est l'insertion de lettres étranges empruntées à d'autres disciplines. La sixième se base sur l'interprétation de géométrie et de figures. La septième et dernière pratique concerne l'emploi de l'écriture sténographique.

[45] Bien qu'il disparaît à nouveau du XVIIIème au XIXème siècle.

[46] Né en 1579.

pour souvenir[47], un père intensément pris par l'étude d'un livre entièrement écrit en hiéroglyphes. Il date cet épisode aux alentours de 1586.

74-§ John DEE se rendit en Bohème entre 1584 et 1588, c'est dans cette période que le manuscrit fut acheté à un inconnu par Rudolph de Bohème. Dans sa lettre, MARCI raconte précisément ce fait. Cette coïncidence insinuerait pour Voynich que cet inconnu fût John DEE. Le second fait qui corroborerait cette hypothèse était que DEE avait une réelle passion pour les travaux de Roger BACON.

Constat 2 John DEE clamait que le nom réel de Roger BACON avait été David DEE son propre ancêtre.

75-§ Il est imaginable, qu'étant à la cour de Bohème dans les années 1580, il influença le nouveau propriétaire, que l'ouvrage ne pouvait être que du Docteur *Admirabilis*[48].

76-§ Le manuscrit fut en possession[49] de Jacobus de TEPENECZ après 1608 et jusqu'à quelques temps avant sa mort en 1622. A partir de ce moment et jusqu'à 1665-1666, le manuscrit disparaît à nouveau. Il réapparaît avec le décès de cet inconnu qui tenta en vain de le décrypter. MARCI ne se prêta pas à quelque affrontement avec les « Sphinx ». Il légua le manuscrit au père Athanasius KIRCHER qui vivait à Rome ; il l'accompagna d'une lettre qui indiquait que Roger BACON était l'auteur du manuscrit.

Hypothèse 1 Marcus MARCI (page 30) dit que le Docteur Raphaël pensa que le manuscrit avait été écrit par Roger BACON (Constat 1).

77-§ Nous perdons sa trace pendant près de deux siècles et demi. En 1912, Wilfrid Voynich découvre à nouveau le manuscrit dans la bibliothèque de la Villa Mandragone, en Frascati, non loin de Rome.

78-§ Depuis, le manuscrit a été étudié successivement par des personnalités extrêmement diverses. Leurs travaux n'ont pas pour autant apporté de solution satisfaisante.

Devons-nous en conclure que ce manuscrit est dépourvu de sens?

79-§ Le fait qu'aucun élément ne prouve l'impossibilité de résoudre cette énigme nous encourage à poursuivre son étude.

Cependant, les non-aboutissements des expériences passées sont significatifs d'une difficulté particulière qui révèle un dysfonctionnement dans le propre *artefact* de

[47] Vers l'âge de huit ans.

[48] Surnom donné à Roger BACON.

[49] Une étude du manuscrit aux infrarouges a révélé sur sa première page la signature de *Jacobj à Tepenece.*

chacun des analystes. C'est pour éviter de reproduire un même cheminement erroné d'idées que nous allons étudier les tentatives précédentes et rechercher la nature de leurs dysfonctionnements.

•

LE MANUSCRIT de Voynich semble avoir été étudié dès le seizième siècle. La première étude consacrée à cette énigme est faite par John DEE en 1586 mais aucune trace écrite n'est restée et seuls les souvenirs de son fils Arthur, alors âgé de huit ans, nous permettent de le présumer. Rudolph II de Bohème acquit le manuscrit entre 1584 et 1588. Il confia son étude à ses savants et experts. Le manuscrit fut confié à Jacobus de TEPENECZ probablement parce qu'il était le directeur du laboratoire alchimique et des jardins botaniques du royaume. Nous ne savons pas si TEPENECZ réussit à le décrypter. Le manuscrit change de mains à sa mort survenue en 1622. Grâce à la lettre de MARCI, nous savons qu'un inconnu a consacré la majeure partie de sa vie à tenter de déjouer les « Sphinx » entre 1622 et 1666 ; mais ceux-ci eurent raison de sa ténacité.

Hypothèse 2 Nous pensons que le manuscrit n'était pas décrypté en 1665–1666 puisque MARCI le transmit à Athanasius KIRCHER avec l'idée que celui-ci trouve la solution.

80-§ La première tentative sur laquelle nous possédons des traces écrites commence dès la redécouverte du manuscrit en 1912. Le Professeur William R. NEWBOLD était savant en science et en philosophie médiévale et il eut le privilège d'être le premier universitaire à qui une copie du manuscrit fut donnée par Wilfrid VOYNICH. Il présenta ses premières impressions en 1921. Quelques années plus tard, il mourut[50] soudainement et ce n'est qu'en 1928 que le Professeur Roland G. KENT publia les travaux de son collègue NEWBOLD. En 1943, Martin FEELY considérait que certains dessins n'étaient que des vues de dissections organiques. Dans cette même optique, Leonell STRONG alors cancérologue voit dans ce manuscrit une description viscérale. Quelques années plus tard, Robert BRUMBAUGH et Leo LEVITOV annoncèrent avoir abouti ; faux espoirs... Entre temps était venue l'ère des cryptologues professionnels. Leurs recherches furent plus prudentes mais les équipes[51] de William FRIEDMAN n'eurent guère plus de succès, il fallait attendre le Brigadier John TILTMAN et le Capitaine Prescott CURRIER pour entrevoir les prémices d'une analyse constructive.

Une clé pour NEWBOLD

81-§ Le Professeur NEWBOLD avait été nourri de philosophie mystique et ésotérique juive du Moyen Age. Il connaissait suffisamment la *kabbalah* pour être interpellé par

[50] L'année de la mort de NEWBOLD est 1926.

[51] « First Study Group » et « Second Study Group ».

un fragment de phrase placé à la fin de l'ouvrage. Sur ce folio 116v figurait la bribe « MICHI DABA MULTAS PORTAS [52]» dont le mot « PORTAS » évoquait pour le docteur NEWBOLD une référence à la cabale hébraïque de combinaisons de lettres. NEWBOLD postulait que Roger BACON était l'auteur du manuscrit et savait de lui qu'il était un familier de la science cabalistique [NOLA1902]. Il pensa alors que cette coïncidence rendait plausible cette supposition.

> **Hypothèse 3 Le postulat que BACON est l'auteur et que la bribe du folio 116v contienne le mot *PORTAS* font penser à NEWBOLD que le manuscrit est crypté par une cabale.**

> **Constat 3 Parmi les vingt-deux signes ou combinaisons diverses de points et autres, NEWBOLD reconnut quinze d'entre eux comme appartenant à un ancien système grec de sténographie.**

82-§ BACON les connaissait puisqu'il avait écrit une telle grammaire si familière aux savants ([PRAT1940]).

> **Hypothèse 4 Il resta donc sept signes sténographiques qui avaient dû être inventés[53] par BACON (Note 44).**

83-§ Thomas GURNEY écrivit, bien plus tard en 1789, que la sténographie est adaptable selon le contexte de dissimulation. A la base, dit-il,

> *Il n'y a rien d'autres que les positions distinctes d'un trait, horizontal, perpendiculaire et oblique ; tel que : _ | \ /, la courbe est variable de la même façon ; tel que : ⊂ ∪ ⊃ ∩*

puis le neuvième signe à connaître est le cercle o. La conjugaison de ces neuf signes permet de former[54] des motifs prononçables phonétiquement.

84-§ La sténographie de BACON comme celle de GURNEY reposent aussi sur le principe de la dissimulation que nous appelons *stéganographie*. Un signe est l'expression d'un son mais il est parfois le diminutif d'une expression, d'une préposition ou d'une terminaison courante.

85-§ Le signe « @ », appelé « arobace », que connaissent tous les utilisateurs de micro-ordinateurs contemporains, signifiait au dix-huitième siècle, et dans la sténographie de

---

[52] Transcription de NEWBOLD.

[53] La création de nouveaux symboles était conseillée.

[54] Les règles de construction ne sont pas exposées ici. Les règles sont souvent adaptées par le sténographe. Nous citons par exemple que l'ajout d'un point peut signaler que l'article « un, une » doit être précédé au mot.

GURNEY, le mot anglais « about ».

86-§ Les sept signes inconnus restants pourraient fort bien avoir été crées à cette fin d'économie que nous connaissons dans l'alphabet[55] MORSE. Toutefois, fait remarquer [PRAT1940] :

> *La sténographie grecque était connue ainsi que ses lacunes, il n'était pas spécialement difficile de trouver la signification des sept signes ajoutés et d 'arriver ainsi à traduire tout le texte en lettres*

87-§ aucune substitution simple ou double ne fut détectée. Cependant, le docteur NEWBOLD ne se découragea pas. Il fut intrigué par le mot « PORTAS » du folio 116v. Le professeur pensa que ce mot devait suggérer qu'une multitude de procédés avaient été utilisés. Au-delà de la transformation des phonèmes en signes, il devait exister un procédé supérieur à la substitution monoalphabétique[56]. NEWBOLD ne révéla jamais par quel raisonnement il se laissa guider vers l'idée que la substitution s'effectuait en deux étapes. Pour lui, un texte était recomposé en autant[57] de couples de lettres qu'il y avait de lettres dans le manuscrit. Chaque lettre du texte donnant naissance à deux lettres.

88-§ Le couple de lettres se détermine comme un état de transition markovien sur un digramme. Un couple de lettres est engendré par la lecture de deux lettres successives du texte avec le décalage d'une seule lettre après chaque lecture. La phrase cryptée ARS MAGNA devient la succession de couples de lettres AR, RS, SM, MA, AG, GN, NA. A l'issue de cette opération, les digrammes sont remplacés l'un après l'autre par d'autres digrammes d'un système ordonné[58]. Finalement, chacune des paires de lettres est remplacée par une seule lettre et toujours d'après un système ordonné[59]. NEWBOLD appliqua cette méthode au manuscrit et constata son échec. Le sphinx ne révéla pas son secret.

89-§ Le docteur NEWBOLD est tenace, il calcule les fréquences des lettres de l'alphabet

---

[55] Dans l'alphabet MORSE, les lettres couramment utilisées possèdent des séquences de signes, composés de traits et points, les plus courtes possibles. Dans la langue anglaise le point représente la lettre « e ».

[56] Note 158.

[57] En fait, le nombre de couples de lettres dépend de la parité en nombre de lettres du texte. Si le nombre est pair alors il existe autant de couples de lettres que de lettre dans le texte ; sinon ce nombre est soustrait de un.

[58] Il y a vingt-deux signes, il existe 22x22=484 couples possibles. Un couple est remplaçable par vingt-deux digrammes possibles. Les bigrammes qui contenaient au moins une des lettres du mot « commuta » ou la lettre « q » étaient sujets à une substitution particulière.

[59] Quelques lettres étaient considérées comme identiques quand il existait une similitude phonétique. Le son « d » et le son « t » étaient considérés comme un unique et même son. La procédure était identique pour les sons « o » et « u », « b » et « p » et cetera.

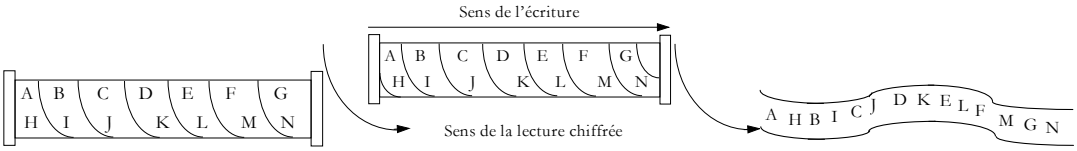
obtenu.

Constat 4 Il constate que ces statistiques sont très proches de celles du latin.

90-§ Aussi pense-t-il avoir franchi les « multiples portes » mais il doit en rester une qui empêche les phrases de se montrer pleines de bon sens. Seule une transposition[60] cryptographique désorganisait la cohérence de la succession des lettres en laissant comme signature la conservation[61] des fréquences des lettres utilisées ; il savait que cette dernière opération ne pouvait être qu'une transposition simple.

---

[60] La transposition consiste en un arrangement ordonné d'un texte clair dans une matrice aux dimensions faites de colonnes et de lignes et qui par désorganisation de ces colonnes provoque une désorganisation du texte clair en texte transposé. La première utilisation de la transposition semble être du V^ème^ siècle av. J.-C. Elle n'utilisait pas de grille de transposition mais un bâton de commandement appelé scytale. Ce bâton *« consistait en un axe de bois autour duquel on enroulait, en spires jointives, un ruban de papyrus, de cuir ou de parchemin »* [KAHN1980]. Nous obtenons cet objet sur lequel nous inscrivons une partie de l'alphabet (ABCDEFGHIJKLMN) en guise de message.

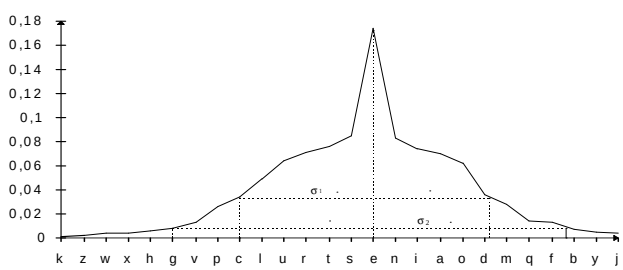


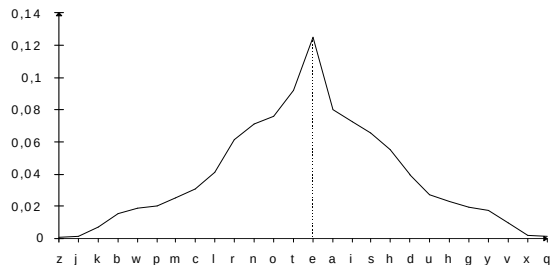
En déroulant la bande sur laquelle nous avons écrit cet alphabet, nous remarquons que la lecture passe d'une orientation « gauche-droite » à une lecture « haut-bas ». La bandelette déroulée contient la transposition de l'alphabet qui peut alors être dissimulée aisément comme bandeau ou ceinture. Le récepteur du message transposé devait posséder une scytale du même diamètre que celle de l'expéditeur pour pouvoir reconstituer le message transposé en message clair. Il est à noter que dès cette époque AENEAS le Tacticien préconisait le remplacement des voyelles par des points. L'alpha était remplacé par un point , l'epsilon par deux points et ainsi de suite jusqu'à sept points pour l'oméga [AENE1990].

Aujourd'hui nous utilisons des matrices mais le procédé demeure identique bien que les textes peuvent être transposés plusieurs fois de suite ; comme si nous utilisions plusieurs scytales de diamètres différents, la première fournit le premier texte transposé à la deuxième scytale qui elle-même transpose le premier texte transposé en un autre texte doublement transposé, et ainsi de suite, jusqu'au nombre total de scytales.

Contrairement au chiffrement par substitution d'un alphabet clair par un alphabet décalé la transposition conserve les lettres utilisées pour écrire le message.

[61] Dans la première étape d'analyse le cryptanalyste recherche la langue de rédaction du message. La transposition monoalphabétique et la double transposition sont détectées par la distribution normale des statistiques monogrammiques. Quelque soit le nombre de transposition, le message transposé conservera les statistiques monogrammiques de référence.





91-§ Féru de savoir sur l'époque médiévale, il se souvenait qu'une pratique courante consistait à faire l'anagramme de noms propres et parfois de textes plus importants. Il reconstitua les anagrammes des pages qui étaient ornées de dessins. Les dessins guidaient son intuition dans l'associativité des lettres dispersées par la transposition.

92-§ Le texte qu'il obtînt était remarquablement étonnant. Il établissait la preuve que Roger BACON avait découvert et utilisé le microscope, dès le treizième siècle, bien qu'il fût inventé[62] à la fin du seizième siècle [PRAT1940].

93-§ Les dessins ont aidé à la reconstruction anagrammatique, les anagrammes décrivaient à leur tour les dessins.

Ainsi, le texte disait ce que le dessin suggérait, on discutait de spermatozoïdes dans le folio 75, les dessins y faisaient penser dans toute leur subjectivité.

94-§ Peut-on imaginer plus extraordinaire ? Les anagrammes révélaient, selon le professeur NEWBOLD, que parmi les dessins astronomiques se trouvait la *nébuleuse spirale*[63] *d'Andromède* et une *éclipse annulaire*[64] qui ne furent découvertes qu'au dix-neuvième siècle par de puissants télescopes.

95-§ NEWBOLD fut confronté à l'obligation de preuve. Qui en effet peut admettre que plusieurs découvertes capitales puissent être le fruit d'un seul esprit qui a vécu plusieurs siècles avant leurs découvertes ? Les exemples existent pourtant. Leonardo Da VINCI avait été un visionnaire et un créateur de procédés développés plusieurs siècles après sa mort. Cependant, notre démarche intellectuelle est différente dans le cas des descriptions dont NEWBOLD fait état. Nous constatons le fait que les objets observés ne sont observables que par une technologie du dix-neuvième et du

---

Distribution normale de monogrammes Français (à gauche). Statistiques monogrammiques de la langue anglaise (à droite).

Chaque langue a sa caractéristique dit STOLFI (page 135). Les lettres ne sont pas employées dans les mêmes proportions. Le digramme TH est très courant en Anglais tandis que pour la langue Française le digramme LE est le plus courant. Dans une distribution de lettres les redondances caractérisent la langue. Pour distinguer les distributions statistiques propres à chaque langage on peut calculer différents coefficients mettant en exergue les variations de redondances.

L'écart-type peut distinguer les langages, le Mode peut aussi montrer que si la présence de la lettre E est de 17 % alors il est fort probable que le langage soit français, si elle n'est que de 12 % il est possible que ce soit l'anglais. W. FRIEDMAN montre que l'indice de coïncidence permet de distinguer les langages [FRIE1922]. Le calcul d'indice de coïncidence peut être étendu aux digrammes et n-grammes mais dans ce cas le résultat ne peut montrer que le chiffrement est un procédé de Transposition.

[62] Attribué à un lunetier nommé Zacharie JANSEN, *Encyclopédie Générale Larousse, page 497, Tome 2.*

[63] Folio 68v.

[64] Folio 67v.

vingtième siècle donc nous supposons que l'observateur a dû créer cette technologie. La démarche est donc inverse à celle des travaux de Leonardo da VINCI qui décrivaient des techniques pour voler, naviguer sous l'eau, avant de raconter ce qu'il observa en utilisant ces techniques.

Les descriptions manquantes dans le manuscrit sont celles des outils nécessaires à l'observation des faits rapportés par NEWBOLD.

96-§ Par contre, les écrivains catholiques voyaient dans ces résultats le triomphe de la philosophie scolastique médiévale[65] et en quelques sortes ils minimisaient les persécutions et le manque d'égard des supérieurs de l'ordre Franciscain pendant cette sombre période du treizième siècle [IMPE1980].

La croyance n'était pas une preuve suffisante, il fallait une preuve scientifique.

97-§ Dans l'esprit de NEWBOLD, l'auteur était sans aucun doute Roger BACON. Il voyait en ce franciscain un génie extraordinaire qui pourtant s'était permis d'écrire un traité d'alchimie particulièrement erroné et si éloigné de la brillance de cet esprit visionnaire. Il pensa aussitôt que ce traité était volontairement rendu absurde ; pour quelle raison, avait-il fait cela ?, certainement pour dissimuler quelques secrets que seul l'initié était en mesure de lire. Comment devait-on procéder pour lire ces secrets cachés ? NEWBOLD concluait que BACON avait dû utiliser un système de dissimulation analogue à celui utilisé dans le manuscrit ; la dissimulation était donc anagrammatique. Il appliqua sa méthode de reconstruction anagrammatique sur ce traité d'alchimie et obtint le résultat suivant :

> *26 février 1273. Le roi Edouard a ordonné au clergé d'entreprendre une enquête systématique contre les criminels. Le clergé l'a entreprise mais, en raison de l'hostilité de la noblesse, y a bientôt renoncé. A Oxford, les chevaliers ont assiégé les moines ; de longs discours ont été échangés. BACON a fait exploser de la poudre à canon pour effrayer les assaillants en leur faisant croire que l'enfer s'entrouvrait et que les démons en sortaient.*

98-§ Les archives du royaumes avaient fait état d'une telle enquête. Il n'en fallut guère plus à NEWBOLD pour considérer que cette preuve montrait que sa méthode était la bonne. Il exposa ses résultats en 1921. Il fut immédiatement attaqué par ceux qu'on attendait le moins : les chimistes montèrent aux créneaux et usèrent de l'argument que l'encre utilisée était excessivement épaisse : « presque aussi consistante que l'encre

[65] Méthode d'enseignement fondée sur la tradition et l'emploi de syllogisme. Le syllogisme étant un raisonnement qui contient trois propositions (la majeure, la mineure, et la conclusion) et tel que la conclusion est déduite de la majeure par l'intermédiaire de la mineure. (Exemple : *Tous les hommes sont mortels* [majeure], *Pierre est un homme* [mineure], *donc Pierre est mortel* [conclusion]).

d'imprimerie ».

> **Constat 5 L'encre est trop épaisse pour dater le manuscrit du treizième siècle ; ce qui remet en cause l'Hypothèse 3 et par implication toute la méthode de décryptage de NEWBOLD.**

99-§ Le conflit s'étendait aux cryptologues qui étaient demeurés jusqu'alors sur leurs réserves ; probablement parce qu'ils avaient connaissance de la difficulté de ces travaux mais aussi peut-être parce qu'eux-mêmes n'avaient pas de meilleure solution. Quoiqu'il en soit, ils finirent par prendre la parole. Ceux-ci soumettaient deux objections basées sur la bijection cryptage-décryptage et sur la reconstruction anagrammatique.

> **Constat 6 La réciprocité des méthodes d'encryptage et de décryptage était impossible.**

> **Constat 7 Le manque de clarté lors de la reconstruction anagrammatique ne permet pas de valider cette méthode.**

100-§ Leur première remarque repose sur le simple constat de réciprocité entre le procédé d'encryptage et le procédé de décryptage. NEWBOLD n'a jamais clairement définit la clé qu'il utilisa pour transformer chaque digramme en lettre unique. Il n'expliqua guère plus le processus de déchiffrement dans tous ces rouages. C'est certainement pour cette raison qu'il lui fût dit, compte tenu de l'inconstance de la clé, qu'il n'etait pas possible d'établir clairement le processus d'encryptage. J-M BIRD du « Scientific American Monthly » montrait du doigt le manque de clarté de NEWBOLD. Il n'expliquait pas comment il était possible d'aboutir à l'avant dernière forme de la phase d'encryptage : AR, RS, SM, MA, AG dont la forme[66] finale cryptée était ARS MAGNA. Le docteur NEWBOLD rétorqua que Roger BACON ne s'était pas forcément servi de la même méthode mais

> *qu'elle était un moyen de s'approcher du résultat que BACON avait atteint par une autre voie [PRAT1940].*

101-§ Toutefois , la non réciprocité des procédés d'encryptage et de décryptage ne confortait pas l'idée que la méthode de déchiffrement proposée par NEWBOLD fut adéquate.

102-§ La deuxième objection était exposée cinq ans après la mort, survenue en 1926, du Professeur NEWBOLD. John MANLY démontra en particulier[67] que la dernière étape

[66] Les deux formes proposées sont des exemples.

[67] En 1931, il émit d'autres objections comme celle de la confusion de signes minuscules sténographiques avec des bavures d'encre épaisse.

de reconstruction anagrammatique était source d'une contestation sérieuse [KAHN1980]. Fletcher PRATT nous rappelle[68] que

> *la première qualité de tout bon procédé de chiffrement est de fournir au chiffrement un message ne prêtant pas à ambiguïté ; on ne peut admettre qu'il puisse offrir deux interprétations possibles.*

103-§ Or, nous savons que la force des transpositions est de favoriser une multitude d'interprétations possibles. L'astronome anglais Proctor montra qu'en raison de la forte redondance[69] des lettres la reconstruction consciente ou inconsciente de l'anagramme[70] permettait à chacun d'élaborer son propre message [PRAT1940] comme dans le carré magique[71] des chrétiens dont la disposition matricielle des lettres permet une lecture du carré par diverses entrées,

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

et de construire de multiples mots latins. Le professeur NEWBOLD s'est donc confronté à la problématique des transpositions alphabétiques.

---

[68] Selon Auguste KERCKHOFFS (page 166) les qualités d'un chiffre sont les suivantes : –le système doit être matériellement, sinon mathématiquement, indécryptable ; –il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénients tomber entre les mains de l'ennemi ; –la clé doit pouvoir en être communiquée et retenue sans le recours à des notes écrites, et être changée et modifiée au gré des correspondants ; –il faut qu'il soit applicable à la correspondance télégraphique ; –il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ; –le système doit être d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

[69] La raréfaction des lettres dominantes d'une langue réduit le vocabulaire disponible et donc aussi les possibilités anagrammatiques.

[70] Ici la difficulté repose sur la désorganisation des caractères du message clair. Pour la substitution monoalphabétique, on voit que l'analyse statistique monogrammique permettait de débuter le décryptage ; pour la transposition, il faudrait tenir compte des longueurs factorielles de la clé de permutation. La méthode qui s'offre à nous est la reconstruction du message par l'étude des anagrammes du texte. Mais si le mot NEIGE est unique, la permutation de ses lettres crée de nouveaux mots comme GÉNIE ou NOEL se transforme en LÉON et IMAGE en MAGIE. Nous voyons donc que nous nous exposons aux problèmes des anagrammes.

[71] Sur le grand arc du choeur de la chapelle de Saint Laurent à Rochemaure en Ardèche on peut trouver gravée dans la pierre une matrice, de 5 lignes sur 5 colonnes, contenant 25 lettres de notre alphabet : cette matrice est appelée «Carré Magique» [VIVA1967] et est présente sur des ouvrages du X^{ème} et XII^{ème} siècle. Nous constatons qu'un ensemble de lettres est inclus dans une matrice 5 sur 5. Le message ne présente pas de clarté immédiate. La clarté littérale n'apparaît pas car les lettres ont été transposées, arrangées, de telle sorte que le Carré magique cache une connaissance aussi bien linguistique, symbolique, que religieuse. On retrouve dans ce carré une doctrine de ralliement des chrétiens qui est *Pater Noster*.

104-§ Le cryptanalyste connaît cette difficulté[72]. Elle demeure encore d'actualité[73] [BARK1995] et elle ne peut être résolue que dans des cas particuliers où sont connus à la fois le langage et au moins un mot spécifique[74] [CALL1985d]; mais aussi, il est possible de comparer[75] une succession de cryptogrammes supposés être encryptés selon le même procédé.

105-§ Le docteur NEWBOLD n'était pas dans cette connaissance. Il avait un unique cryptogramme. La langue du manuscrit était supposée latine mais rien ne l'affirmait. Quant aux mots probablement présents dans les folios analysés, nous ne disons pas que l'établissement du lien qu'il fit entre les dessins et le texte crypté soit une erreur. En revanche, le piège dans lequel le professeur s'est enfermé est celui de l'*interprétation* des images selon son propre *système de référence*.

106-§ Il n'est alors pas anormal que les découvertes faites par le rédacteur du manuscrit soient celles du dix-neuvième siècle plutôt que celles de sa propre époque. La grande

---

[72] Nous avions travaillé sur la cryptanalyse de la double transposition au cours de l'année 1994. A cette époque cette méthode d'encryptage bénéficiait d'une protection de secret militaire qui ne fut levée qu'en mars 1995 par la National Security Agency Américaine. Seulement cette déclassification ne s'est pas accompagnée de la diffusion de la méthode de résolution. La méthode d'encryptage de la double transposition est identique à la méthode d'encryptage de la transposition simple mais répétée une deuxième fois. Il existe alors deux clés de transposition. Le texte transposé dans un premier cryptogramme est réinséré dans une deuxième grille de transposition. A l'issue de cette deuxième étape nous obtenons le cryptogramme doublement transposé. La force de la double transposition en matrice rectangulaire est de dissimuler un texte clair non pas dans la distribution des fréquences des lettres mais dans la désorganisation des lettres du texte clair.

[73] Note 75.

[74] L'analyse de cryptogrammes obtenus par une clé redondante avec un alphabet standard d'encryptage peut être effectuée par la méthode du « mot-probable » [CALL1985d]. Une application célèbre de cette méthode fut faite sur le télégramme de PANIZZARDI dont le mot-probable était « DREYFUS » (page 211).

[75] La méthode Wayne G. BARKER nécessite la reconstruction du texte transposé en texte clair sans pour autant connaître les clés de transposition. Le principe est une reconstruction anagrammatique qui présuppose une structure de texte stéréotypée. Il constate que dans la pratique il existe des probabilités importantes pour que des messages de même dimension soient transposés avec les mêmes clés de transpositions. Il propose de réunir ces cryptogrammes afin de les étudier en même temps. Ces messages sont placés l'un en dessous des autres et chaque colonne ainsi obtenue est numérotée. La deuxième étape consiste à repérer les lettres qui devraient être rares mais qui apparaissent trop fréquemment. La lettre 'X' est souvent utilisée pour compléter un message qui aurait une dimension inférieure à la grille de transposition. Puisque les cryptogrammes sont placés les uns en dessous des autres, nous pouvons détecter les colonnes qui contiennent cette lettre qui normalement devrait être rare. La remarque de BARKER est que la colonne contenant le plus cette lettre est la dernière ligne de la matrice puis celle qui est un peu moins pourvue de cette lettre rare est l'avant dernière ligne. Ces deux colonnes de positions différentes dans le cryptogramme sont en fait juxtaposées dans le texte clair. En procédant ainsi, récursivement et jusqu'au possible, nous connaissons une partie de la transposition.

Cette approche est « anagrammatique » car la validation des positions des colonnes par rapport à leur effectif en lettre rare est fonction des probabilités n-grammiques des anagrammes formés par la juxtapositions de ces colonnes. La reconstruction complète du texte clair est surtout rendue possible par l'induction nécessaire de la présence d'une forme stéréotypée du message comme un message militaire ACP127 peut l'être. Il attend donc les mots du type « TO COMMANDING GENERAL », « TO COMMANDING OFFICER », « TO SIGNAL OFFICER » et aussi par exemple la présence du vocable « QUERY » dont la lettre rare « Q » s'associe avec une lettre fréquente « U ».

difficulté ici se trouve dans notre capacité à changer notre système de référence et d 'apprécier l'information picturale et écrite dans son contexte d'expression. Et ce contexte quel est-il ? Quatorzième, quinzième, seizième siècle ? NEWBOLD connaissait l'époque médiévale ; comment s'est-il laissé déporter du treizième siècle au dix-neuvième siècle ? S'est-il enivré du manuscrit au point de perdre de vue la notion de contexte et d'indexicalité ? Toutes ces questions demeureront sans réponses, et surtout, nous nous interrogeons sur les interactions possibles entre les dessins et le texte du manuscrit ;

le folio 34r contient ce qui apparaît être une plante ; puisqu'elle possède : un système de racines au bas de la page, des ramifications verdoyantes vers le haut de cette page et trois fleurs.

107-§ Devons-nous considérer que cette plante existe réellement dans la nature ou bien est-elle la représentation d'une idée particulière ?

Hypothèse 5 Ses treize feuilles peuvent-elles être comparées au treize phases de la lune que l'alchimiste représente par un arbre[76] à treize têtes ? Et si cela est exact que peut signifier l'unique feuille[77] brisée de cette plante ?

Gynécologie de FEELY

108-§ Joseph Martin FEELY[78] publie en 1943 l'article *Roger BACON's cipher : The right key found*. Il pense tout comme NEWBOLD que le manuscrit est de Roger BACON ; mais contrairement au docteur il ne possède pas d'exemplaire du manuscrit. Il travaille sur des reproductions de folios qui ont été publiés dans le livre de KENT.

109-§ Sa première idée est que si le manuscrit est effectivement de BACON alors il convient d'étudier les statistiques des oeuvres de BACON. Il se limite à deux ouvrages : *De perspectiva* et *Communia naturalium*. Il constate que le groupe des lettres les plus fréquentes est constitué des lettres *« E, I, T, A, N, U, S »*. Il compare ce groupe avec le groupe obtenu dans le texte de VOYNICH.

[76] Symbole du mercure.

[77] La sixième en partant de la gauche.

[78] Juriste.

Constat 8 Les statistiques latines et les statistiques du manuscrit sont proches[79] et laissent penser que la différence s'inscrit dans la substitution monoalphabétique.

110-§ Toutefois, FEELY remarque un point important :

Constat 9 Le style d'écriture de BACON est très abrégé et montre une différence entre le latin de l'époque médiévale et le latin classique.

111-§ Pour FEELY, les abréviations de BACON réduisent son écriture d'environ trente-cinq pour-cent par rapport au latin classique.

112-§ Sa deuxième démarche est une tentative d'interprétation des dessins pour décrypter les étiquettes qui parfois les accompagnent.

Hypothèse 6 FEELY était assuré que les deux « nuages » situés en haut à gauche du folio 79v étaient des ovaires.

113-§ Le conduit reliant le haut de la page (folio 79v, page 49) au milieu de la page transmettait « l'ova » qui était alors ensaché dans l'un des deux sacs. Cette association établissait une relation entre l'étiquette écrite dans un langage crypté et l'interprétation que FEELY faisait des dessins. Le texte obtenu était informe, juge Elizabeth FRIEDMAN ; son texte ressemblait à du latin abrégé qu'il traduisait en anglais.

Hypothèse 7 FEELY étudia le folio 78r qui représentait à ses yeux des dessins gynécologiques.

114-§ Il continua de procéder selon la même méthode. Il déclara avoir trouvé des mots grecs et avoir décrypté une référence mystérieuse à la statue de *Memnon* dans le folio 68v [FEEL1943]. Il conclut que le manuscrit était le journal d'un savant qui relatait ses observations agrandies des cellules vivantes dont l'irrégularité des notes montrait l'utilisation d'un procédé de dissimulation.

115-§ FEELY demeura très attaché à l'idée que l'auteur était Roger BACON. En fait, souligne Elizabeth FRIEDMAN, bien qu'il constitua un alphabet de substitution celui-ci fut obtenu par des approximations successives. Quant à sa méthode, TILTMAN la résume sévèrement

sa méthode dépourvue de méthode produit un texte dans un latin médiéval inacceptable dans des formes abrégées non authentiques.

[79] Ce constat se réfère au texte du manuscrit et est différent du Constat 4 qui lui se réfère à un calcul statistique après manipulation de texte du manuscrit.

116-§ Toutefois, le travail de FEELY montra que Roger BACON écrivait dans ses ouvrages avec un style abrégé qui se distingue du latin classique.

Enfantement de STRONG

117-§ Le professeur Leonell C. STRONG était un scientifique qui faisait des recherches contre le cancer à l'université de Yale. Pendant cinq ans il essaya d'obtenir des copies du manuscrit de Voynich. Il n'eut aucun succès et il devait se contenter des illustrations présentes dans les publications déjà éditées. Il présuma que le système d'encryptage utilisé était un double système particulier de progression arithmétique d'un alphabet multiple très voisin de ceux de TRITHÈME, PORTA et SELENI. Il obtint un texte [STRO1945] qu'il disait être de l'anglais médiéval

> *When skuge of tun'e-bag rip, seo uogon kum sli of se mosure-issue ped-stans skubent, stokked kimbo-elbow crawknot.*

STRONG traduisait cette bribe en

> *Lorsque la déchirure des veines (ou des membranes) est satisfaisante, l'enfant sort adroitement de la mère qui enfante avec une position pliée et courbée des jambes, tant que les bras, courbés sur les coudes, sont noués (au-dessus de la tête) comme les pattes d'une écrevisse*[80].

118-§ Nous voyons que ce professeur a décrypté un message dont le sens est proche de celui trouvé par FEELY. La critique faite à STRONG fut du même ordre que celle faite à FEELY. L'extrait décrypté par STRONG n'était pas de l 'anglais médiéval, aux yeux des spécialistes, nous rapporte Elizabeth FRIEDMAN [FRIE1962]. Les cryptologues disaient aussi manquer de détails sur sa méthode cryptanalytique.

> *Sur le peu que STRONG expliqua de la méthode de chiffrement, les cryptologues n'y trouvèrent rien qui fut suffisamment sensé [FRIE1962].*

119-§ Elle ne fut apparemment jamais expliquée et l'on considéra que la problématique n'avait pas été résolue.

---

80 *When the contents of the veins rip (or tear the membranes), the child comes slyly from the mother issuing with the leg-stance skewed and bent while the arms, bent at the elbow, are knotted (above the head) like the legs of a crawfish.*

Quadrix nonix de BRUMBAUGH

120-§ Un professeur de Philosophie Médiévale de l'université de Yale annonça, dans un article paru dans *Speculum* en 1974, avoir résolu le mystère du manuscrit. Il avait, disait-il, lu quelques étiquettes de dessins de plante et il trouva le nom de BACON dans la clé du folio 116v que NEWBOLD avait lui-même exploitée.

121-§ Il pensait que le manuscrit était une contrefaçon qui avait été créée délibérément à l'intention du crédule Rudolph II de Bohème. Cette idée n'est pas novatrice souligne TILTMAN ; mais BRUMBAUGH voit son hypothèse confirmée dans deux séquences de lettres placées dans les marges droites et gauches du folio 1r. Il trouve ce qu'il appelle un chiffre standard du treizième siècle. Les lettres apparaissent comme des lettres substituées par un unique alphabet. La première monosubstitution a pour référence la lettre « a » et la deuxième monosubstitution a pour référence la lettre « d ». BRUMBAUGH utilise ce système d'encryptage par substitution monoalphabétique auquel il joint un réarrangement de syllabes. Le texte[81] « MICHI CON OLADA BA » du folio 116v révèle le texte « RODGD BACON ».

122-§ C'est une conclusion logique pour Robert S. BRUMBAUGH qui considère que le nom de BACON doit être aisément découvert afin que la contrefaçon paraisse écrite de la main propre de Roger BACON. Toutefois, cette découverte ne permet pas de décrypter le manuscrit.

123-§ Toujours à partir de la notation du folio 116v, BRUMBAUGH voit les mots *Quadrix nonix* dans lesquels il reconnaît une appellation de chiffrement des alchimistes et des astrologues.

> **Hypothèse 8 *Quadrix nonix* est la déclaration qui dit, selon BRUMBAUGH, qu'une structure *Four-by-nine box* a été utilisée.**

124-§ BRUMBAUGH énonce que l'encryptage s'effectue en deux étapes. La première étape consiste à remplacer les lettres par des nombres en utilisant une matrice de neuf colonnes par quatre lignes. La première ligne contient une clé numérique de neuf chiffres et les lignes suivantes contiennent le texte à chiffrer. Les chiffres ne sont pas limités à neuf formes. Un chiffre peut être écrit dans des représentations différentes selon les âges, les alphabets et autres abréviations scientifiques [IMPE1980]. Ainsi ce que nous croyons être un alphabet de lettres est un alphabet de chiffres aux représentations multiples (Figure 16 de [IMPE1980]). Dans les trois lignes restantes de la matrice *Four-by-nine box* le texte clair y est inséré comme dans un système de transposition alphabétique à matrice incomplète.

125-§ La critique vient encore une fois du brigadier TILTMAN. Il accorde à BRUMBAUGH

[81] Selon les analystes le message change (page 99 et 101 de [IMPE1980]).

qu'il existe une part de probabilité que le manuscrit soit une contrefaçon. Mais cette idée avait déjà été soulevée auparavant par lui-même lors d'une communication écrite [TILT1951] avec William F. FRIEDMAN en 1951. Quant à l'idée d'utiliser une *Four-by-nine box*, il n'est guère pratique de reconstruire le message clair puisque chaque chiffre du manuscrit est le représentant[82] de deux à trois lettres possibles. Par contre,

> **Constat 10 TILTMAN ne semble pas surpris par l'idée de représentations de formes multiples des chiffres.**

Et qu'en fait,

> *BRUMBAUGH n'est pas le seul à prétendre que les symboles sont des chiffres dans des formes variées. Ceci a été suggéré de nombreuses fois.*

126-§ TILTMAN est plus sévère à l'encontre des travaux de BRUMBAUGH. Il estime que bien qu'ils soient tout à fait plausibles compte tenu des évidences qu'il présente, les solutions qu'il propose sont bien plus basées sur les phénomènes observés dans le manuscrit et de son histoire reconstruite que celles d'un quelconque déchiffreur.

127-§ TILTMAN tenta lui-même le procédé suggéré par BRUMBAUGH. Il obtint des mots ressemblant autant que possible au latin ou à un pseudo-latin. Certains étaient similaires comme nous nous y attendons dans le cas d'un texte où les lettres sont très redondantes.

Les groupes de FRIEDMAN

128-§ Nous présentons William F. FRIEDMAN en page 168. Nous montrons qu'il est le fondateur de la cryptanalyse américaine. Il contribua à la diffusion de la cryptanalyse bien que son emploi l'obligea, contre sa nécessaire reconnaissance médiatique, à tenir ses découvertes pour secrètes. Autour de lui vont se créer deux groupes de travail sur le manuscrit de Voynich ; bien que les espérances furent grandes d'aboutir à une solution ; nous constatons que ces associations n'ont pas été à la hauteur des résultats escomptés si bien que nous pourrions nous demander si ces deux groupes avaient réellement pour objectif de contribuer à la cryptanalyse de ce manuscrit. Trop peu d'informations ont été communiquées à ce propos et nous ne pouvons guère dire plus que ce qui suit[83].

[82] La transformation du texte clair en un texte substitué est le processus inverse de la substitution à représentations multiples puisqu'à une lettre cryptée correspond trois lettres (ou chiffres) possibles.

[83] Qui soit en relation directe avec la cryptanalyse du texte manuscrit.

First Study Group

129-§ La deuxième guerre mondiale a contraint les nations alliées à s'unir pour la victoire contre le nazisme. L'activité des services cryptologiques était en permanente augmentation. La mobilisation et la coopération des services cryptologiques[84] ont permis de faire rencontrer des *savoir-faire* linguistiques, mathématiques et méthodologiques. William F. FRIEDMAN alors chef du SIS[85] profita de cette rare opportunité pour constituer le premier groupe d'étude du manuscrit de Voynich.

130-§ Le 26 mai 1944, dix jours avant le débarquement des troupes alliées en Normandie, des spécialistes[86] en philologie, paléographie, en langues anciennes, classiques et médiévales ; égyptologues, mathématiciens, et autres autorités en sciences se penchèrent sur le manuscrit.

131-§ A partir des copies du Docteur PETERSEN, ils établirent la transcription des symboles en lettres et caractères spéciaux assimilables par un calculateur IBM. Ils obtinrent, à l'issue de leurs réunions bimensuelles, un alphabet de vingt-six lettres. Des voies historiques furent explorées. Quels étaient les travaux d'Athanasius KIRCHER ? qui était John DEE ? Que connaissons-nous de l'époque médiévale ? Autant de questions qui animaient les assemblées où le savoir était partagé mais qui souffrait du manque de résultat et rendra les rencontres plus sporadiques entre 1945 et 1946.

132-§ Il semble que dans ces réunions il y avait des savants mais pas de commis secrétaire. Nous avons connaissance du travail de transcription, mais mis à part ça, nous ne savons rien des investigations particulières qui ont été menées par ce groupe ; excepté le fait que l'IBM permit de calculer les tables de fréquences.

133-§ La fin de la deuxième guerre mondiale a été la fin de la coopération des talents particuliers. Tous finirent par intégrer à nouveau leurs laboratoires d'avant-guerre.

Second Study Group

134-§ FRIEDMAN avait tenté une première fois de constituer un groupe de travail qui n'avait pas résisté à la capitulation de l'Allemagne nazie. En 1962, FRIEDMAN tenta à nouveau l'expérience sous la houlette financière de la Radio Corporation of America (RCA). Le *First study group* avait permis de transcrire le manuscrit en symboles opérables par un ordinateur IBM. Depuis, la notion de programme avait été développée par Alan TURING dans sa *machine universelle* [HODG1988] mais elle n'avait pu être utilisée par le premier groupe de travail de 1944. Le deuxième groupe

[84] Bureau 40 Service du chiffre anglais appelé par le nom officiel ID 25 (section 25 de l'Intelligence Division), SIS (Signal Intelligence Service USA) dirigé pendant la deuxième guerre mondiale par W. F. FRIEDMAN.

[85] Cf. Note de ci-dessus.

[86] Seize participants.

bénéficia de la programmabilité de la nouvelle génération d'ordinateur IBM. Le groupe étudia les successions de lettres appelées *n-graphes*[87]. Il passa en revue les séquences de un à six caractères. Il classa les mots et séquences de mots en fonction de leurs occurrences et de leurs dimensions ; et pratiqua une recherche des occurrences de lettres à des positions différentes des mots. Il effectua une analyse linguistique complète[88] par ordinateur [IMPE1980]. Pourtant en 1963, ce plan spécial d'études connaît le même sort que le premier groupe de travail. La RCA décidait de couper court à leur enlisement dans ce projet avant que tout résultat soit obtenu. FRIEDMAN considéra que cette deuxième tentative demeurée infructueuse ne lui avait pas permis de réunir assez de « matière » pour écrire un article[89] qui apporte des faits nouveaux. En fait, il ne s'était prononcé qu'indirectement à travers un autre sujet de cryptologie qui parut dans *Philological Quartely* de janvier 1959.

> *Je ne me fie pas aux anagrammes acrostiches*[90]*, pour le peu de valeur réelle qu'ils ont, -Un gaspillage -Et, ne peut rien prouver -Fin [FRIE1959].*

Conclusion 1 Pour FRIEDMAN, tout comme TILTMAN, la théorie de l'anagramme n'était pas envisageable dans le manuscrit de Voynich.

TILTMAN et l'hypothèse des langues synthétiques

135-§ FRIEDMAN connaissait le brigadier TILTMAN. Il le savait être un cryptologue compétent qui se prévalait d'une longue expérience comme professionnel du domaine. En 1950, FRIEDMAN initia TILTMAN au manuscrit et lui demanda son opinion ; TILTMAN accepta d'étudier cette énigme. FRIEDMAN lui communiqua quelques folios qui n'étaient pas pourvus de dessins[91].

136-§ TILTMAN fut pris d'une réelle motivation comme tous ceux qui avaient approché le manuscrit. Il étudia les folios que FRIEDMAN lui avait transmis et effectua son *modus operandi* de cryptologue.

---

[87] Le *n* de *n-graphes* indique le nombre de lettres de la séquence choisie.

[88] D'après ce que rapporte Maria d'Império [IMPE1980] ; en fait, nous ne possédons que les résultats de la discrétisation des symboles de Voynich en lettres alphabétiques. Nous ne doutons pas du réel travail cryptologique réalisé par ces deux groupes mais il souffre de l'absence de leur communication.

[89] Il aurait pu, comme beaucoup d'autres, publier une certaine histoire de ce qui était déjà su ; mais l'ensemble des articles de FRIEDMAN montre une rigueur qui le conduisit toujours à publier pour communiquer des faits nouveaux.

[90] Pièce de vers composée de telle sorte que la suite des initiales de chaque vers, lues dans le sens vertical, forme le nom d'une personne ou d'une chose à laquelle se rapporte le poème.

[91] Nous présumons que ce choix a été guidé par l'évitement des « erreurs » commises par NEWBOLD, FEELY et STRONG, qui ont associé, à tort ou à raison, les dessins au texte.

137-§ Il commença par calculer les données statistiques fondamentales puis dans un deuxième temps, il étudia les lettres d'effectifs importants en portant un regard sur leurs combinaisons avec les autres lettres.

> **Constat 11 Pour TILTMAN, il apparaissait évident que des structures de symboles étaient présentes dans les mots et que nous pouvions les décomposer simplement en trois parties : « Beginners », « Middles » et « Enders ».**

138-§ Il s'intéressa à l'organisation de ces symboles dans la logique des trois parties. Il remarqua que les symboles 𝆕 et 𝆖 avaient cette tendance à se placer après les symboles, 𝆐 ou 𝆑, et avant 𝆗 , 𝆘 , 𝆙 , 𝆚 [TILT1951].

139-§ TILTMAN trouva cette découverte très intéressante, surtout lorsque la succession fréquente de symboles lui fit penser que la forme[92] 𝆐𝆘𝆐𝆘𝆐𝆗 pouvait être « xxv », c'est-à-dire, l'expression d'un nombre romain.

Commençait-il à s'égarer en tentant d'associer la forme et le sens ?

Dans un sursaut, TILTMAN revint à la raison qui lui fit remarquer que l'utilisation d'un moyen de chiffrement pouvait être la raison de cet effet : « Somme toute, à chaque cause son effet », et bien que l'intuition soit un outil indispensable pour le cryptanalyste ; elle n'est pas la seule à détenir la solution de l'énigme : FEELY, STRONG et NEWBOLD en avaient fait l'âpre expérience.

140-§ TILTMAN aboutissait à la même conclusion que FRIEDMAN

> *Comme vous savez, dès le début je m'étais forgé l'opinion, laquelle vous aviez eu avant moi, qu'il n'exista aucun cryptage.*
>
> **Hypothèse 9 Pour FRIEDMAN et TILTMAN, le manuscrit n'a pas été crypté avec une méthode compliquée. Il est plutôt probable que le langage utilisé est un *langage universel synthétique* comme celui de Bishop WILKINS.**
>
> *L'ensemble ressemblant plus à une forme primitive de langage universel synthétique, tel que Bishop WILKINS [TILT1951] avait développé dans sa « Classification philosophique des idées » en 1667.*

[92] Elle ne fut pas la seule mais celle-ci figure à titre d'exemple. Un autre cas : 𝆛𝆙 serait interprété en « iij ».

141-§ Ceci expliquerait que la simple substitution alphabétique ne soit pas le système d'encryptage employé. Mais surtout, TILTMAN sous-entend que le concept de langages synthétiques et universels est en adéquation avec l'apparition[93] du manuscrit. TILTMAN quittait le contexte du treizième siècle pour s'intéresser particulièrement à deux auteurs du dix-septième: Bishop John WILKINS et George DALGARNO. Il trouve que chaque symbole du manuscrit est la représentation d'une forme linguistique plus évoluée. Ainsi, dans l'esprit de TILTMAN et tout comme ce fut le cas dans l'esprit de FRIEDMAN, une lettre du manuscrit vaut pour un mot et par induction, un mot du manuscrit vaut pour une proposition. Les deux cryptologues ne pensent, à aucun moment, que le manuscrit de Voynich est issu du procédé de l'un des deux auteurs du dix-septième siècle ; le manuscrit ayant été détenu dès la fin du seizième siècle ; mais ils pensent qu'il existe une analogie suffisante pour que ces cas soient étudiés.

WILKINS

142-§ TILTMAN étudia les travaux de WILKINS, à travers : *Mercury, or the secret and swift messenger*, et, *An essay toward real character, or a philosophical language,* complété par *An alphabetical dictionary*, pour comprendre l'organisation de la méthode proposée.

143-§ WILKINS cherche la langue parfaite dans les notions communes et dans la nature des choses sur lesquelles l'humanité tout entière pourrait être en accord [ECO1994]. Pour cela, WILKINS énumère l'ensemble des choses animées et inanimées et il les organise hiérarchiquement dans l'arbre de la *tradition aristotélicienne*.

144-§ A l'origine de l'arbre se trouve les *mots* dont certains décrivent des *choses transcendantales* et les autres sont des *choses spéciales*. La première branche décrit les relations générales de mixité et de l'action. La deuxième se décompose en branches opposant le *Créateur* aux *créatures*. Les créatures réunies constituent le monde et lorsqu'elles sont réparties, elles sont distributives. Cette décomposition par opposition des substances aux accidents le conduit à dissocier la nature des *pierres* à celle des *métaux* pourtant toutes deux de nature *végétative et imparfaite.*

145-§ Jusqu'alors le rapport de ce procédé avec le manuscrit semblait inexistant ; mais WILKINS introduit la proposition qui relie les *choses* organisées de son arbre comme *comparables, opposables, différentes*. Il assigne un signe à chaque *caractère réel*. Il y a quarante genres, quarante signes les représentent. Neuf signes servent à indiquer les différences et neuf autres signes sont utilisés pour définir l'espèce. L'ensemble constitue cinquante-huit signes ; mais il en existe d'autres qui servent à marquer les oppositions, les formes grammaticales, les adverbes, les prépositions *et cetera.*

[93] Aux alentours de 1550. Toutefois, la date historique est située entre 1584 et 1586.

146-§ WILKINS propose aussi la version parlée de la langue universelle qui est similaire de principe à la version pasigraphique[94] de cette langue. Cependant, la différence est que chaque genre est représenté par un morphème ou un phonème[95] qui se prête aisément à la sténographie.

DALGARNO

147-§ Les tableaux de DALGARNO de son *Ars signorum,* paru en 1661, sont plus sommaires que ceux de WILKINS. Il réduit à dix-sept le nombre de genres fondamentaux auxquels dix-sept lettres[96] majuscules sont associées. DALGARNO utilise trois lettres[97] *subalternes* pour indiquer, *l'opposition, le moyen*, ou que les lettres qui suivent doivent être lues comme des chiffres.

148-§ La classification proposée permet à DALGARNO de nommer *nebghnagbana* ce que nous appelons l'ail. SLAUGHTER[98] décortique chaque lettre de ce mot étrange et obtient la description de l'ail [ECO1994]:

> *n=concretum physicum, e=in radice, b=vesca, g=qualitas sensibilis, h=sabor, n=pingue, a=partes annuae, a=folium, b=accidens mathematicum, a=effet prima, n=longum.*

149-§ Le système de DALGARNO est un système de définition approximatif. Il est laissé à l'utilisateur le moyen d'établir la profondeur de l'arbre de la classification jusqu'à aboutir à une précision suffisante.

150-§ Contrairement à la langue universelle de WILKINS, le système de DALGARNO abandonne l'esprit universel pour une créativité linguistique propre à chaque utilisateur. De ce fait, toute énumération qui prend la forme de classification, comme celle que nous trouvons dans un *herbier*, peut devenir un réel système crypté par l'organisation propre de l'auteur.

151-§ Dans son étude, TILTMAN tente de positionner le manuscrit de Voynich par rapport à ces deux systèmes de WILKINS et DALGARNO. Il constate que les similarités

---

[94] La pasigraphie est une représentation d'une langue écrite qui ne se prononce pas phonétiquement.

[95] Les *différences* sont exprimées par les neufs consonnes b, d, g, p, t, c, z, s, n. Les *espèces* sont déterminées par sept voyelles a, ɑ, e, i, o, u, y, et deux diphtongues du y.

[96] A (entité), I (concret, composé, complet), E (accidents), H (substance), U (homme), Y (spirituel), O (corporel), B (mathématique-accidents), D (physique), P (sensitif) , S (commun), K (politique), G (qualités sensibles), T (rationnel), N (physique), F (artefacts), M (mathématiques-corporel).

[97] Le « R » signifie l'opposition, le « V » indique que les lettres qui le suivent sont des chiffres, le « L » indique le moyen.

[98] Mary SLAUGHTER, *Universal languages and scientific taxonomy in the seventeenth century,* Cambridge, 1982.

statistiques et le *style* du manuscrit sont moins matures pour avoir été inspirées par ces deux langages. Ils sont en effet que trop systématiques, trop réguliers, en comparaison avec ce qui se passe dans le texte de VOYNICH ; ceci le conduit à penser que [TILT1951]

> **Conclusion 2 Le langage employé dans le manuscrit est un mélange très illogique de différents genres de substitution.**

152-§ TILTMAN n'est nullement découragé. La conclusion qu'il formula précédemment n'était pas le résultat d'un échec puisqu'il mettait en exergue les deux termes « illogique » et « mixé ». C'est probablement pour cette raison que TILTMAN étudia le cas de la *langue universelle* de Cave BECK dont le système est à la fois imprégné de lettres et de chiffres.

BECK

153-§ Au milieu du dix-septième siècle, Cave BECK [BECK1657] proposa sa conception du langage universel qu'il appelle

> *le caractère universel, par lequel toutes les nations du monde pourront comprendre les conceptions d'autrui, lisant à haute voix une écriture commune à leurs propres langues maternelles.*

154-§ Sa conception s'imprègne fortement de la polygraphie Kirchérienne (page 193) de 1663. Sa méthode fait appel à l'effort de mémoire. Les mots sont référencés par un numéro, compris entre 1 et 3999, dans leur ordre alphabétique. Chacun de ces mots est alors représenté par un code de quatre chiffres qui constitue la base du langage. Une autre série d'environ cent soixante-quinze mots est représentée par un code de trois lettres qui exprime une certaine variation du mot codé par les quatre chiffres du premier code. La proposition de BECK est donc un ensemble de deux codes constitués de quatre chiffres et de trois lettres. Le système de codification des trois lettres du deuxième code attire l'attention de TILTMAN ;

> **Constat 12 TILTMAN dit que dans le système de Cave BECK les trigraphes spéciaux commencent tous avec « s » ou « t ».**

155-§ Il associe cette remarque avec la structure tripartite des mots qu'il détermina dans le manuscrit. Le « s » ou le « t » pourrait donc être le terme « moyen » qui découpe chaque mot en « début, milieu et fin ».

156-§ Dans son système de langue universelle BECK fait précéder tout substantif par la lettre « R », les adjectifs et groupes d'adjectifs par la lettre « Q ». Il réduit l'ensemble des vocables en attribuant aux synonymes d'un vocable le même code de quatre chiffres. TILTMAN s'intéresse à l'expression du pluriel des noms.

Constat 13 Cave BECK ajoute la lettre « s » ou le chiffre « 8 » pour signifier que le mot codé est sous sa forme plurielle.

157-§ Les verbes sont précédés par un préfixe de trois lettres pour que toutes les propositions soient écrites sous une forme codée. BECK voulait, comme WILKINS, que son langage soit prononçable ; il attribua à chaque chiffre une syllabe pouvant être composée d'une consonne et d'une voyelle, d'une voyelle et d'une consonne ou d'un triplet consonne-voyelle-consonne.

Constat 14 TILTMAN faisait remarquer que le système codique de Cave BECK se transformait en un système de substitutions digraphiques[99] et trigraphiques.

158-§ Les associations mixtes de lettres et de chiffres étaient génératrices de confusions entre mots d'une même proposition ; pour cela, BECK ajouta un séparateur permettant de distinguer les différentes formes présentes dans la proposition.

Hypothèse 10 Le brigadier TILTMAN pensa que le terme `[8G]` placé dans le groupe de terminaison était composé d'un pluriel « s » (Constat 13) suivi d'un séparateur `[G]`.

159-§ L'aspect « illogique » que TILTMAN avait découvert dans le manuscrit se comprenait dans un tel système[100] de codification.

160-§ Seulement, TILTMAN fut dans le cas où le dictionnaire indexé, par des codes chiffrés, était inconnu. De même, les caractères spéciaux régissant l'aspect du verbe et des adverbes, ainsi que le séparateur de mots, étaient eux aussi inconnus.

---

[99] La méthode est toujours une substitution mais nous ne l'avons pas classée avec les méthodes de monosubstitution car elle procède par une substitution digraphique. La méthode PLAYFAIR trouve ses origines conceptuelles dans le carré de 25 de l'historien POLYBE. La méthode de POLYBE consiste à assigner des coordonnées à l'ensemble des lettres d'un alphabet

	1	2	3	4	5
1	A	L	P	H	B
2	E	T	C	D	F
3	G	I	K	M	N
4	O	Q	R	S	U
5	V	W	X	Y	Z

Chaque lettre est représentée par un couple de nombre compris dans l'intervalle 11, 55. Ainsi le message "POLYBE EST UN PHILOSOPHE" devient chiffré en une séquence numérique : 13 41 12 54 15 21 21 44 22 45 35 13 14 32 12 41 44 41 13 14 21. On retrouve cette notion de carré de 25 dans le signe de ralliement des chrétiens appelé « carré magique ». En Russie, au dix-neuvième siècle, les nihilistes exploitent cette méthode pour communiquer dans les prisons qui les détiennent. Le carré devient une matrice de trente cinq cases adaptée à la dimension de l'alphabet russe.

[100] Il s'intéressa par la suite à un autre langage synthétique modelé par Johnson mais TILTMAN ne rapporta rien à ce propos.

161-§ L'aspect sténographique du manuscrit que NEWBOLD avait mis en évidence (Constat 3) laissait supposer que le langage écrit était la forme orale[101] du discours.

162-§ Entre 1957 et 1975, le brigadier s 'intéressa à une ligne de recherche complémentaire. Il passa beaucoup de temps à comparer des *herbier*s et des manuscrits médicaux avec le probable *herbier* du manuscrit de Voynich. Mais en vain, même l'avis des experts de ce domaine ne lui permit pas de trouver quelque corrélation. Il conclut en ces termes

> *D'après tout ce que je sais, personne n'a été capable de trouver un point de connexion avec un quelconque autre manuscrit médical. Ceci est particulièrement étrange parce que le nombre d'ouvrage traitant d'herbier, du début du moyen âge jusqu'au 16ème et voire au 17ème siècle, sont en fait très limité... En général, les premières illustrations des premiers herbiers imprimés étaient limitées à deux ou trois collections de copies stylisées et gravées sur bois, maintes et maintes fois, dans des formes de plus en plus dégénérées.*

163-§ Bien que TILTMAN exprima une certaine désespérance, il en fut tout autrement pour le Docteur LEVITOV qui simplifia la problématique du *sphinx* par l'introduction de l'idée que ce manuscrit était un récit Cathare dont les symboles étaient des représentions purement phonétiques ; seulement son enthousiasme n'est pas particulièrement partagé par les linguistes mais toutefois ses travaux montrent quelques approches intéressantes.

Docteur Leo LEVITOV et l'expérience Cathare

164-§ Le livre *The code breakers* de David KHAN, publié en 1967, est l'ouvrage qui conduit le Docteur LEVITOV à s'intéresser au manuscrit de Voynich. Il lui apparut que la plus remarquable solution fut apportée par le Professeur NEWBOLD, mais comme sa tentative avait été soumise à une critique acide, LEVITOV poursuivit ses analyses à l'écart des contestataires. En l'espace d'un peu plus de deux ans, il interpréta à nouveau les résultats précédents et faisait remarquer que

> **Constat 15 Il est très improbable que John DEE vendit ce manuscrit à Rudolph II de Bohème.**

165-§ Seule la lettre de 1675[102] rapportait qu'Arthur disait qu'il avait vu son père tentant de décrypter un manuscrit entièrement en hiéroglyphes ; et pour LEVITOV, ce cheminement d'idées incluant : ouï dire, hypothèse de calcul quant à l'âge probable

[101] Chaque symbole du manuscrit est le représentant phonétique d'une substitution digraphique ou trigraphique.

[102] Lettre écrite en 1675 par Sir Thomas BROWNE à Elias ASHMOLE. Il rapporte les paroles d'Arthur DEE [IMPE1980].

qu'avait Arthur DEE lorsqu'il assista à la scène, et puisque John DEE clamait sa filiation avec Roger BACON, alors la conclusion ne pouvait être que John DEE avait vendu ce manuscrit à la fin du seizième siècle lors de son voyage à Prague. LEVITOV n'admet pas ce cheminement et remet en cause[103] implicitement l'Hypothèse 1, l'Hypothèse 3 et l'Hypothèse 4, et réfute[104] par incidence les constats d'analogies avec les travaux de BACON ; par cela le Constat 5, le Constat 6 et le Constat 7, sont confirmés, l'analogie avec les travaux de BACON n'est plus fondée et éradique le Constat 9.

Constat 16 LEVITOV remet en cause l'auteur probable Roger BACON et par implication les travaux de NEWBOLD et de FEELY, mais pas ceux de BRUMBAUGH qui suggère la contrefaçon d'ouvrage n'ayant jamais été écrit par BACON.

166-§ LEVITOV semble en désaccord avec la plupart des constats et hypothèses. Quand KRAUS décrit le type de symboles servant à la rédaction du manuscrit, LEVITOV dit qu'il s'agit de caractères carolingiens et non romans[105] ; ainsi de suite, il finit par exposer sa propre conclusion, qui procède de la même démarche que celle de FEELY à propos de l'association *ovaire-dessin*, et dit qu'il y a suffisamment de descriptions de rites Cathares pour conclure que le manuscrit est cathare ; il y a assez, de symboles de la Déesse Isis, d'images d'elle, d'allégorie anti-sacerdotal, pour conclure que ce manuscrit est à la fois une Hérésie Cathare et un manuel du culte d'Isis.

Conclusion 3 Pour LEVITOV, les dessins ne font aucun doute : le manuscrit est à la fois une Hérésie Cathare et un manuel du culte d'Isis. Il s'agit de *La Grande Hérésie.*

167-§ Sa conclusion pose un état de fait qu'il est nécessaire de relier les dessins avec le texte qui sommes toutes est le sujet en question. LEVITOV se demande si le texte apparaît dans sa nature propre et qu'alors si cela est le cas il doit être lu comme n'importe quel texte moyenâgeux.

---

[103] Rappel : Marcus MARCI (page 30) dit que le Docteur Raphaël pensa que le manuscrit avait été écrit par Roger BACON (Constat 1). Hypothèse 3 Le postulat que BACON est l'auteur et que la bribe du folio 116v contienne *le* mot PORTAS font penser à NEWBOLD que le manuscrit est crypté par une cabale. Il resta donc sept signes sténographiques qui avaient dû être inventés par BACON (Note 44).

[104] Rappel : L'encre est trop épaisse pour dater le manuscrit du treizième siècle ; ce qui remet en cause l'Hypothèse 3 et par implication toute la méthode de décryptage de NEWBOLD. La réciprocité des méthodes d'encryptage et de décryptage était impossible. Le manque de clarté lors de la reconstruction anagrammatique ne permet pas de valider cette méthode. Le style d'écriture de BACON est très abrégé et montre une différence entre le latin de l'époque médiévale et le latin classique.

[105] Dérivés du latin comme les caractères de l'alphabet italien, français, espagnol, portugais et roumain pour ne citer que les principaux.

Est-ce que l'auteur de cette G*rande Hérésie* a tenté de dissimuler la nature de ses pensées par un artifice cryptographique ?

168-§ La question semble presque dénuée de bon sens quand LEVITOV[106] fait remarquer que parmi les 400 plantes dessinées dans le manuscrit, aucune d'elle n'existe, de même, ce qui apparaît être des signes du zodiaque ou des constellations ne sont pas des signes du zodiaque ni même des constellations ;

Hypothèse 11 Pour LEVITOV, les en-têtes, les légendes, les sous-titres, ne sont pas ce qu'ils semblent représenter.

169-§ Pour preuve, la dimension du manuscrit n'est pas plus grande ou plus courte que ce qu'elle doit être mais chaque signe est un symbole dont la valeur a été perdue ; toutefois, nous pouvons en retrouver le sens. D'une façon obsessionnelle , il voit *l'œil d'Horus* dans chaque zone centrale d'une figure[107] quelque peu ovoïde. Lorsqu'il voit ce que nous appelons des *racines,* partie ramifiée de couleur marron symétrique à la verdure de la plante, et des tiges, il dit[108] que ce sont *les serpents enlacés sur la Tiare[109] d'Isis.*

La méthodologie de LEVITOV nous rappelle celle de FEELY et celle de STRONG qui accordaient des relations, voire des confusions, entre ce qu'ils observaient dans les dessins et les probables secrets contenus dans le manuscrit ; mais LEVITOV travaillait sur des reproductions faites de sa propre main et quelques détails nous paraissent étranges.

170-§ Le folio 79v est particulier, il fait partie d'une succession de représentations engageant des figures humaines entremêlées avec des tubes et des bains dans lesquels s'écoule apparemment un liquide où se vautrent des *chimères[110]* (Figure 3, page 49). Le personnage placé en haut à gauche de ce folio tient dans sa main un crucifix, le deuxième personnage est allongé et *mourant* nous dit LEVITOV, le troisième personnage apparaît tondu et orné d'une corne que nous ne constatons pas dans notre reproduction. Cette différence est problématique car elle change l'interprétation de la scène. Selon LEVITOV cette scène est démonstratrice que le manuscrit procède

---

[106] Les dessins entrent dans une dimension autre que la description simple et naturelle des choses de notre monde. Les dessins sont des créations dédiées à un système de représentation. L'hermétisme qui les accompagne est suffisant pour dissimuler le message au profane qui doit alors faire l'effort de retrouver la symbolique des images et du texte.

[107] Figure 3, 10, 11 de son livre [LEVI1987].

[108] LEVITOV est enclin à croire que l'Eglise Cathare est l'Eglise d'Isis.

[109] Ornement de tête des souverains, chez les Mèdes et chez les Perses. On retrouve cette coiffe dans le Tarot de Marseille de Paul MARTEAU dont le *Pape* et la *Papesse* sont coiffés de tiares et sont liés à la spiritualité, aux prémonitions et à l'intuition.

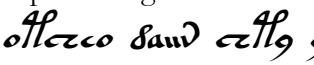
[110] Nous utilisons ce terme parce que nous avons quelques difficultés à définir leur nature réelle : animaux, hybridations d'animaux, sirène, ou animaux fantastiques.

de *la grande hérésie ;*. Il la décrit comme suit :

> *Dans cette figure nous voyons, dans le coin haut à gauche, une Madone tenant un crucifix et un flux de liquide saint s'écoule sur une femme mourante. La figure de dessous est une étrange none satanique, bisexuelle, tondue et ornée d'une corne... Pendant que la femme descend dans les eaux de l'enfer, elle est immédiatement ingurgitée par un démon écailleux...*

171-§ Nous laissons la description, étrangement perçue, au Docteur LEVITOV mais nous trouvons curieux que cette *none satanique* devienne un personnage « commun » lorsque nous l'observons dans notre reproduction : qu'est devenue la corne qui s'associe si bien à Satan ? Quelques pages plus loin cette description infernale le Docteur LEVITOV s'accorda avoir commis quelques erreurs[111] de copies manuscrites sans pour autant remettre en question sa description par un *sublata causa, tollitur effectus*[112] et sans pour autant signaler quelles ont été ses erreurs de copies.

L'interprétation des dessins est très personnelle, lorsqu'il étudie la figure 6 de sa transcription, il voit le premier personnage placé en haut et à gauche du folio qui tient un objet dans sa main gauche : sa conclusion est qu'il ne peut s'agir que d'une *sistre*[113], c'est probable, mais comment l'intégrer d'office dans un raisonnement qui ne conçoit pas la réfutation ?

172-§ De même, sa première démarche analytique n'est pas de rechercher une quelconque structure de mots ; il tente de prendre directement le raccourci qui associe la scène à l'écriture, traitant le manuscrit comme une bande dessinée, le folio 66r lui apparaît être le point de départ. On voit sur ce folio un grand texte, puis en bas pour finir, se trouve un personnage caractérisé de *mourant* par LEVITOV ; au-dessus de lui est écrit un *titre*  qu'il associe à une mixture Franco-germanique *ALVIA TEM VLETH THEDEESVISETH* que l'on dit plus simplement *All the time someone will die*[114]. Il conçoit que cette traduction n'est pas très correcte ; il réorganise les lettres jusqu'à aboutir à une sémantique « adéquate » : *AILVIA TEM VILTEH THE DEESVISETH* dont l'évidence nous conduit à la traduire en *When one is a sick as he is, he wants to know death.*

Nous comprenons en fait que LEVITOV associe d'une certaine façon les symboles avec des sons mais selon Jacques GUY[115], alors linguiste de

---

111 Cf. Page 19 de [LEVI1987].

112 La cause supprimée, l'effet disparaît.

113 Instrument de musique égyptien composé d'une lame métallique recourbée et fixée à un manche traversé par une baguette mobile qui retentissait lorsqu'on l'agitait.

114 Qui est la conclusion approximative du bon syllogisme de la Note 65.

115 *On levitov's decipherment of the Voynich manuscrit,* Jacques B. M. GUY, 9 décembre 1991, EVMT.

l'équipe de recherche de l'EVMT, il subsiste de nombreuses incohérences qui ne permettent pas de considérer ce travail comme exhaustif.

173-§ LEVITOV dégage un ensemble de vingt-cinq sons correspondant aux symboles de VOYNICH ; cependant, il manque les lettres B, G, H, J, P, Q, U, X, Y et Z. Il élabore la base de son vocabulaire avec vingt-trois racines[116] de vocables et constate que

Constat 17 (Selon LEVITOV) Les lettres [M], [N], [J], [6], sont seulement présentes à la fin des mots.

174-§ Sur ce point nous ne sommes pas d'accord[117]. Le Tableau 14 montre que **[M]** et **[N]** sont aussi présents dans les autres positions de vocables ; et le Tableau 15 indique qu'ils ne sont pas toujours au début des vocables. Finalement **[M]** et **[N]** occupent l'ensemble des positions possibles dans les vocables (Constat 28 page 127, Constat 29 page 128) et seules **[J], [6]** ne commencent ni ne finissent un vocable.

Constat 18 Le Constat 17 est contredit par le Constat 28 et le Constat 29.

175-§ LEVITOV décrit six voyelles[118] et le langage[119] serait alors dérivé de l'allemand. Cependant fait remarquer J. GUY : le son anglais « oo » est équivalent au son « oe » en allemand et qu'alors parmi six voyelles il ne resterait plus que trois voyelles ; la

---

[116] Infinitif, dérivation, substantif, verbe.

LEVITOV commet quelques erreurs ; selon son principe, la lettre devrait être prononcée « a » (comme dans « papa ») mais il l'étend à [e] et [o].

Quant à l'utilisation des temps, LEVITOV énonce qu'il n'existe pas de déclinaison de substantif ou de verbes conjugués autres que le présent, or la forme dite : « to die », s'écrit « den » et correspond aux symboles  , et la forme « dieth » des symboles est traduite « it is dying » qui est un présent progressif.

De même, lorsque LEVITOV utilise les formes pluriels ; le  et le  servent à l'exprimer et qu'alors les formes  et  sont respectivement « awns » et « awneth », c'est-à-dire « ones ». Seulement, cette formation du pluriel n'est pas valide en allemand (suffixe « –en ») et en germain (suffixes –n, –en, –er, e). Jacques GUY conclut que le pluriel décrit par LEVITOV est purement anglais (certainement inspiré par les deux formes plurielles de « speak » en « speaks » et « speaketh »).

[117] Nous appelons un fait que nous constatons plus loin dans cette étude ; mais compte tenu de l'invraisemblance du Constat 17, nous devons éviter aux lecteurs le risque de se noyer dans des affirmations erronées.

[118] [a], [e], [o], [E], [i], [i:].

[119] LEVITOV dit que son langage est un « *polyglot oral tongue* » qui se comprend, selon Jacques GUY, comme *un langage qui n'a jamais été écrit avant et lequel emprunte des mots à partir de langages différents*. Cette hypothèse n'étant pas illogique puisque les langues empruntent, interprètent à nouveau des mots étrangers comme le vocable « sky » dont l'origine est danoise et est utilisé aussi par les anglo-saxons.

conséquence est fâcheuse puisqu'il ne serait plus possible de distinguer « last », « lest » et « lost ».

176-§ De même, les douze sons consonantiques décrits par LEVITOV sont trop peu nombreux si l'on considère que le langage parlé est européen ; et dans son système, il manque les sons [g], [b] et [p] dont [b] et [p] sont essentiels selon J. GUY :

> *Je ne peux penser qu'un seul langage au monde puisse se passer à la fois de [b] et [p]*[120].

177-§ Cependant, LEVITOV pensait que le manuscrit de Voynich était un langage simple avec un vocabulaire peu étendu mais très diversifié,

> **Hypothèse 12 LEVITOV pensa que la diversité des vocables avait pour cause l'utilisation d'un apostrophisme.**

178-§ Les vocables sont ambigus, souligne-t-il, propice à des significations différentes, dont la source ne peut être que la substitution ou la suppression d'une ou plusieurs lettres d'un mot par un caractère dit « apostrophe ». Les exemples sont courants, en anglais, l'expression « can not » peut s'écrire « cannot » voire « can't » et l'apostrophisme consiste ici à remplacer les lettres « no » par « ' ».

179-§ Toutefois, bien que nous avons montré les différents aspects problématiques de l'analyse du Docteur Leo LEVITOV, deux idées originales[121] ont émergé de son travail. En premier lieu, il a marqué son intérêt pour les dessins de roues emboîtées sur lesquelles des segments sont disposés et étiquetés.

> **Constat 19 LEVITOV observe que des étiquettes de dessins ne sont pas forcément cryptées, il prend pour exemple le folio 71r et 70v2 (bien qu'il infirme l'Hypothèse 11).**

180-§ Et, le dessin d'un *taureau (folio 71r1)* est étiqueté avec une inscription très proches de celle du nom *mars* dont la corrélation astrologique est réelle. Nous constatons le même fait avec le folio 70v1 qui a pour centre le dessin d'un *bélier*[122] et dont l'inscription qui s'y rapporte semble indiquer le mois astrologique d'avril.

> **Pour autant, le folio 70v2 a pour centre deux poissons et deux étoiles dont une seule est connectée aux deux poissons par un trait ; entre ces deux**

120 Il précise que l'espagnol dispose de 5 sons de voyelles, 17 consonantiques et 2 assimilées.

121 Trois avec l'Hypothèse 12.

122 Il n'est pas évident de savoir si il s'agit d'un bélier ou d'un capricorne ; seule la logique de la succession des signes zodiacaux nous pousse à penser que le folio du bélier précède le folio du capricorne.

poissons apparaît encore l'inscription proche de celle trouvée à coté du taureau, peut-on penser que la succession astrologique entre signes zodiacaux des poissons au taureau soit en relation avec cette observation ?

181-§ Les expériences successives de NEWBOLD, FEELY, STRONG et LEVITOV, montrent que formuler l'hypothèse dans l'expectative d'en attendre la réponse voulue est dangereux pour la crédibilité et la construction d'une méthodologie cryptanalytique.

182-§ Ce que NEWBOLD « décrypta » était ce qu'il attendait ; son postulat, que BACON était l'auteur, l'empêcha d'explorer d'autres voies ; il s'enferma dans cette logique ou l'hypothèse est tenue pour un fait, il demeure logique qu'il découvre alors dans l'anagramme la solution adéquate à ce qu'il veut tenir pour assuré.

183-§ Quant à FEELY, alors juriste, il n'approcha que succinctement le manuscrit et proférait sans expliquer la démarche qui le conduisit à cette conclusion que les dessins étaient le résultat d'observations scientifiques ; pour STRONG, la solution était encore plus simple, il s'agissait de descriptions de corps organiques qu'ils comprenaient merveilleusement bien puisqu'il était lui-même cancérologue. Seulement, et comme dans le cas de LEVITOV, il existait ce point commun qui contribua au non-aboutissement : tous se sont hâtés vers une solution qu'ils présumaient d 'avance.

184-§ Peut-être est-ce ceci qui distingue l'approche faite par ces diverses personnalités de celles entamées par les cryptanalystes, FRIEDMAN, CURRIER et TILTMAN, qui par expériences savent qu'il ne faut pas attendre une solution « immédiate » à tous cryptogrammes[123] ; cependant, leurs recherches ont permis de développer trois axes importants pour la poursuite d'analyses futures. Les groupes de FRIEDMAN ont apporté la transcription du manuscrit en séquences de symboles plus facilement malléables et propices aux traitements informatiques. L'étude faite par le Capitaine Prescott CURRIER prend la voie d'une recherche d'identification du manuscrit en posant la question : combien[124] de personnes ont participé à sa rédaction ? Existe-t-il des variations dans leurs écritures nous permettant de présumer les variations[125] de systèmes d'encryptages ? Quant à TILTMAN, il a ouvert la voie de la recherche de structures particulières indépendantes de toutes inductions linguistiques.

---

[123] Il était même de coutume d'attribuer des salaires supplémentaires aux cryptanalystes des *Cabinets Noirs* quand ceux-ci butaient sur un cryptogramme inhabituel car ceci signifiait qu'un nouveau procédé cryptographique était employé par « l'ennemi ».

[124] Il estime que cinq à huit types d'écritures sont présentes dans le manuscrit. Seulement : « peut-on conclure qu'il s'agisse de personnes différentes ? ».

[125] D'après CURRIER il existe deux langages différents dans lesquels les lignes du texte sont des unités particulières de par leurs structures —dans leurs débuts et leurs finitions— et elles gouvernent l'occurrence de certains mots bien qu'il reconnaisse ne pas savoir quel procédé elles utilisent.

185-§ Nous allons donc tenter de poursuivre ce travail de fondement en nous basant sur ces trois axes d'études. Nous récupérons les travaux de transcriptions qui vont nous permettre une étude des groupes de lettres dans leurs proportions et leurs qualités. Plus nous avancerons dans nos recherches et plus nous tenterons de trouver les structures fondamentales du manuscrit en nous détachant progressivement du problème majeur des inductions linguistiques.

II

Quel cheminement emprunter ?

14 novembre 1998 —Première édition

Partie II

Quel cheminement emprunter ?

•

Sommaire

14 novembre 1998 —Première édition

186-§ La diversité des hypothèses et les non-aboutissements des expériences passées nous placent dans une situation délicate de crainte de l'égarement. Nous tenterons donc une première approche que l'on peut considérer comme « traditionnelle ».

187-§ La première étape consisterait à déterminer le langage de rédaction du message étudié afin d'utiliser les outils mathématiques probabilistes et statistiques en fonction de cette langue probable. Nous référençons dans une certaine mesure les langues par des caractéristiques statistiques mais ces indices sont perceptibles dans le cas unique où le texte d'origine n'a pas subi de polysubstitutions. Dans le cas d'un encryptage par transposition ou par plusieurs transpositions successives[126] il y a conservation des lettres claires dans le texte crypté: la difficulté étant ici de retrouver l'ordre des transpositions et non la langue de rédaction[127].

188-§ Dans le cas où les statistiques naturelles d'un texte clair sont dissimulées par le chiffrement, ce qui orientera nos recherches sont les paramètres sociologiques et géographiques, nous pourrons nous poser les questions suivantes : de quelle communication provient ce message ?, quelle peut être la nature des informations ?, si nous avons les réponses correspondantes à ces questions, nous déterminons alors : la ou les langues[128] usitées dans le pays où a eu lieu la capture[129] du message, la ou les langues connues[130] du rédacteur[131], la ou les langues connues du récepteur et les caractéristiques du texte.

Ces informations sont souvent obtenues indépendamment de toutes approches statistiques.

189-§ La difficulté majeure serait de ne pas connaître la langue de rédaction, le rédacteur du message et le type d'information contenue dans le texte car toute étude basée sur l'analogie est alors impossible. Or, nous rappelle Maria D'IMPÉRIO, ceci est précisément le cas rencontré dans le manuscrit de Voynich

[126] Qu'on appelle succinctement « n-transpositions » ; le « n » indique le nombre de transpositions effectuées.

[127] Transposition monoalphabétique générale (note 60).

[128] Italien, latin.

[129] Le manuscrit a été retrouvé en Italie.

[130] Roger BACON connaissait les langues sémitiques, le grec, le latin, l'anglais, le français et l'allemand.

[131] La lettre de MARCI dit qu'il s'agit de Roger BACON (Hypothèse 1, page 56).

> *Nous sommes toujours ignorants du langage sous-jacent; nous avons vraisemblablement de petits indices sur la nature de ce chiffre, code, ou système d'écriture; nous ne savons pas quand, ou, et par qui le manuscrit a été écrit; nous ne pouvons pas être certain du sujet en question [IMPE1980].*

190-§ Voilà sept siècles[132] que ce manuscrit demeure indécrypté. Il est présumé que le rédacteur soit Roger BACON (Hypothèse 1 et Hypothèse 3) mais au moins cinq personnes ont participé à sa rédaction constate le Capitaine CURRIER (Constat 37). Nous supposons qu'il peut être rédigé en plusieurs langues et que finalement il est fort probable que les rédacteurs, si l'hypothèse de CURRIER s'avère vraie, aient utilisé plusieurs méthodes d'encryptage dont une pourrait être basée sur la sténographie. En somme, il est difficile de trouver le bon chemin qui mène à la résolution de cette problématique vieille de quatre cents à sept cents ans. Nous conduirons notre étude en tentant d'éviter les inductions qui associent : spécificité linguistique et traits remarqués dans le manuscrit.

191-§ Nous commencerons par nous intéresser aux caractéristiques multigraphiques[133] des séquences de lettres du manuscrit puis nous étudierons ses mots dans leurs fréquences et leurs diversités.

[132] Au plus sept siècles et au moins quatre siècles.

[133] De même que pour les « n-transpositions », nous appelons une représentation « multigraphiques » un ensemble de « graphes » (lettres, symboles, signes) qui apparaît sous diverses formes.

•

NOUS ÉTUDIERONS les éléments simples avant d'en venir aux structures complexes dont l'origine est la combinatoire des éléments simples.

> *Il grava, modela, soupesa et permuta les vingt-deux lettres fondamentales et forma avec elles toute la création et tout ce qu'il y à former pour le futur [...]. Il plaça les vingt-deux lettres fondamentales sur une roue comme si c'étaient des murailles [...]. De quelle façon les combina-t-il et les permuta-t-il ? Aleph avec tous les Aleph, Bêt avec tous les Bêt [...] et il se trouve que toute créature et toute chose dite provient d'un Nom unique [...]. Deux pierres bâtissent deux maisons, trois pierres bâtissent six maisons, quatre pierres bâtissent vingt-quatre maisons, cinq pierres bâtissent cinq vingt maisons, sept pierres bâtissent cinq mille quarante maisons. A partir de ce moment, va, et pense à ce que la bouche ne peut pas dire et l'oreille ne peut ouïr [ECO1994].*

192-§ La combinaison des éléments simples crée des structures complexes. La transcription du manuscrit en séquence de lettres montre qu'il existe plusieurs alphabets possibles qui sont à la base de la connaissance que nous avons de ce langage.

Quelles méthodes allons-nous employer pour mettre en exergue les indices qui nous permettront de déduire les procédés d'encryptage ?

193-§ Nous utilisons les calculs statistiques et probabilistes à différents niveaux de combinaisons de lettres. Nous commencerons par étudier le texte comme une suite de lettres prises une à une ; cette approche est dite monogrammique[134] et montre le comportement de chacune des lettres du manuscrit. Puis, au fur et à mesure, nous étudions des combinaisons plus importantes de lettres avec les outils de calculs de couples et de triplets de lettres que nous abordons selon différents angles de la dépendance et de l'indépendance *n-grammique* Markovienne[135] ainsi que de la mesure d'ordre de Claude SHANNON.

Transcription du manuscrit

---

[134] Une seule lettre.

[135] Les chaînes de MARKOV sont utilisées dans de nombreuses disciplines. Dans le domaine du langage l'équipe *Rank Xerox Research Center RXRC* de Grenoble utilise les travaux de MARKOV pour extraire des probabilités de réalisation de vocables afin d'analyser automatiquement le langage. Pour nous, notre approche markovienne consiste à montrer les cas rares et les cas systématiques.

194-§ Le cryptologue travaille sur des séquences d'images, de sons ou de symboles. Pour obtenir ces suites, il est nécessaire de connaître ou d'établir la limite qui sépare chacun des signes. Vous remarquez que dans les « phrases » du manuscrit (Figure 1, Figure 2, Figure 3, page 47), chaque lettre est distincte des autres car séparée des autres par un intervalle suffisamment large pour ne pas être confondu avec l'espace qui sépare chaque lettre d'un vocable. Puis, un retour à la ligne est effectué pour signaler un autre paragraphe. Toutes ces indications font que la séquence de lettres est décomposable en monades. Seulement la transformation de l'information continue en information discrète est réalisable selon des processus différents[136] qui donneront autant de versions de transcriptions[137].

195-§ Les cryptologues W. F. FRIEDMAN et le Capitaine CURRIER ont discrétisé ce manuscrit ; seuls certains signes ne coïncident pas entre leurs deux versions. La phrase suivante, extraite d'un folio du manuscrit de Voynich, est discrétisée par deux séquences de symboles différentes.

[136] La reconnaissance optique des caractères a longtemps utilisé les principes de l'analyse de Fourrier pour laisser place maintenant à l'analyse par ondelettes (« Ondes et ondelettes » de Barbara BURKE HUBBARD aux éditions BELIN POUR LA SCIENCE). La discrétisation des rayonnements électromagnétiques est facilitée par l'étude de la variation du signal en fonction du temps. Mais il peut être extrêmement difficile de distinguer les unités alphabétiques dans le cas d'un manuscrit crypté. En fait, plus la source d'information est continue plus il est probable que la discrétisation soit source d'erreurs de transcription. En tous cas, il risque d'exister plusieurs interprétations de discrétisation pour un unique message non discret.

[137]

ASCII	2	4	8	9	+	A	E	I	O	P	Q	S	J	L	C
FROGGY															
EVA	2	4	8	9	+	A	E	I	O	P	Q	S	J	L	C
CURRIER															

Version CURRIER

HTO**K** SOE 4ODOE 4OR OEAM O**H**G8**8** 2OK GPTG GPAIK-

Version FRIEDMAN

HTO***** SOE 4ODOE 4OR OEAM O**P**G8**K** 2OK GPTG GPAIK-

196-§ Cette phrase est interprétable de six façons différentes[138] dès l'étape de discrétisation . Notons surtout que la séquence manuscrite est ici présentée dans une version extrêmement lisible et que dans la pratique les caractères sont moins facilement dissociables comme vous pouvez le constater dans la Figure 2.

197-§ Nous avons vu que ce que CURRIER considère être :  est une tache pour FRIEDMAN. De même, ce que FRIEDMAN considère être :  , est considéré par CURRIER comme étant . D'autres questions nous viennent à l'esprit dont l'une est ou commence le texte ? est-il écrit de haut en bas et de gauche à droite comme il est coutume de le faire dans l'écriture latine ? Le sens de l'écriture est-il défini de droite à gauche comme dans l'écriture Arabe ? ou bien est-elle à boustrophédon[139]? Qu'est-ce qui détermine les limites d'un paragraphe ?

198-§ Le manuscrit de Voynich est un exemple qui montre combien il est difficile de pratiquer une énumération exhaustive de signes manuscrits en symboles discrèts. FRIEDMAN et CURRIER se sont confrontés à cette problématique de la perception holistique. Ils ont obtenu deux séquences partiellement différentes du manuscrit de Voynich. Ces deux séquences de symboles reflétant leurs propres représentations logiques des signes à discrétiser.

Quelle est la fonction essentielle de cette transformation d'information ? Cette question peut paraître surprenante mais pourtant tenter d'y répondre montre de quelles façons nous procédons dans nos méthodes.

---

[138] Nombre factoriel de discrétisations différentes.

[139] Mode d'écriture archaïque qui consiste à écrire alternativement de gauche à droite et de droite à gauche. Littéralement en grec: comme va le bœuf (*bous*) quand il laboure le champ (*strophein*) (note 13).

199-§ Les cryptanalystes décomposent systématiquement des ensembles en sous ensembles puis ces mêmes sous ensembles en groupes, et ainsi de suite, jusqu'à aboutir à une monade. Or cette monade est une unité de dimension minimale qui fait sens. Pour le cryptanalyste, cette démarche de décomposition conduit à un découpage de l'information en unités atomiques que nous sommes à même de mieux manipuler mathématiquement. Cette unité atomique, que nous appelons ainsi pour montrer que ce qui apparaît indécomposable finit par se retrouver décomposé[140], prend la forme d'un symbole alphabétique.

Le cryptanalyste pratique alors cette discrétisation avec l'*a priori* que l'information étudiée est une information intelligible construite avec des règles déterministes et qu'alors l'alphabet est un ensemble composé d'unités appelées lettres.

200-§ Nous attendons, par exemple et en toute naïveté, et bien que la Conclusion 2 de TILTMAN rend incertaine cette supposition, que le manuscrit de Voynich soit une « information construite avec des règles déterministes ».

La discrétisation est donc la mise en adéquation entre une source continue et sa représentation discrète par l'induction qu'elle soit le produit d'un alphabet fini de symboles.

201-§ Le groupe[141] de FRIEDMAN a décelé trente-six caractères différents[142]. Quant au Capitaine CURRIER, il remarqua trente-neuf signes[143] distincts[144]. Les quatre autres transcriptions ont révélé les effectifs suivants :

[140] Le signe sténographique se transforme en phonème ou en morphème qui eux-mêmes sont à nouveau décomposables en lettres.

[141] Il existe deux groupes d'études, ici nous nous référons au plus récent (page 74).

[142] Dont trois sont : l'espace, la fin de ligne et la tache d'encre.

[143] La transcription de Courrier ne couvre pas tout le manuscrit ; la transcription que nous utilisons n'est donc pas pourvue de trente-neuf signes mais uniquement de vingt-six signes.

[144] Dont trois représentent : l'espace, la fin de ligne et la fin de paragraphe.

	Caractères	Signes du formatage[145]
TILTMAN	17	0
IMPÉRIO	31	5
VOYNICH Study Group[146]	29	3
KRISCHER	43	4

Tableau 1 Variations de la perception des signes en fonction des différents transcripteurs.

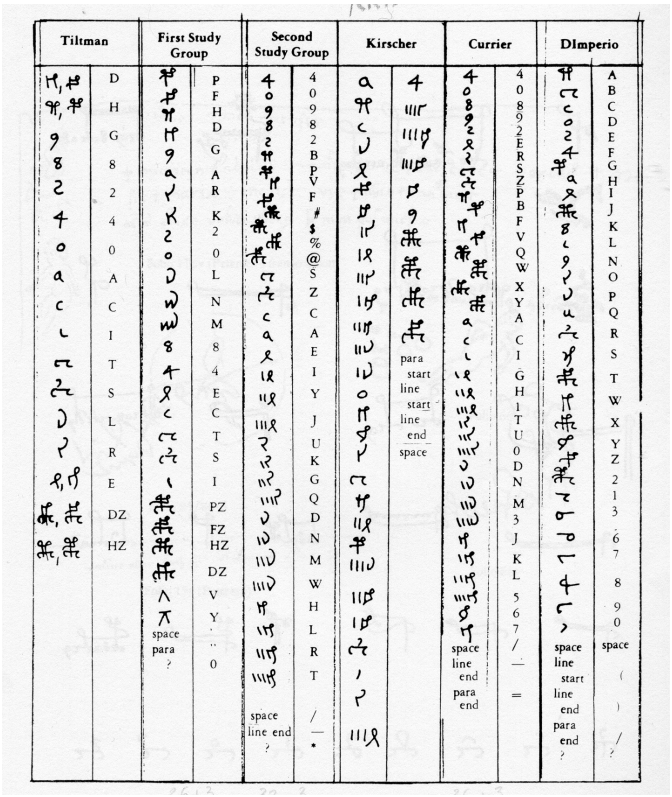


Tableau 2 Variations des transcriptions des symboles en lettres (Source : Maria D'IMPÉRIO page 97).

202-§ Nous remarquons que TILTMAN ne découvre que dix-sept lettres. Tandis que KRISCHER, FRIEDMAN et IMPÉRIO en découvrent plus du double[147].

[145] Caractères espaces, fin de ligne, fin de paragraphe, intersection avec un dessin, tache d'encre.

[146] Premier groupe de travail dirigé par FRIEDMAN (page 73). Dans notre étude nous disposons de trente lettres et du symbole espace : soit un maximum de trente et un caractères pour la version FRIEDMAN.

[147] Ce point est important car nous verrons que ceci montre un découpage particulier du manuscrit.

Utilisons les probabilités

203-§ En cryptanalyse, la notion de probabilité est abordée de façon simple. La définition que nous donnons d'une probabilité est celle apportée par Solomon KULLBACK [KULL1977]. Il dit:

> *La probabilité qu'un événement se produise est le ratio du nombre de cas favorables au nombre des cas possibles, tous les cas ayant les mêmes chances de se produire.*

204-§ Si la probabilité d'un événement est p alors la probabilité qu'il n'apparaisse pas est q, de telle façon que $p+q=1$.

> **En cryptanalyse, nous distinguons la notion de probabilité de celle de *« statistical probability »* qui dit qu'en pratique nous ne connaissons que les événements empiriques de présence des symboles contenus dans le message transmis.**

205-§ Nous ne possédons qu'une vision réduite au message communiqué par rapport à l'ensemble des messages pouvant être échangés. Pour cela, pour connaître les probabilités d'occurrence de chaque lettre d'un alphabet, il est nécessaire d'étudier une quantité importante de textes:

> *Pour trouver les probabilités d'occurrences de chacune des lettres de l'alphabet, il est nécessaire d'examiner une quantité importante de texte.*

206-§ La méthode empirique doit nous conduire à circonscrire les probabilités de chaque lettre d'un alphabet. La fréquence absolue se substitue alors à la notion de probabilité.

> **Il est remarquable que les termes « probabilité, fréquence, occurrence » soient utilisés avec une signification très proche et non rigoureuse[148] au sens mathématique.**

207-§ Toutefois, leurs représentations demeureront fidèles à ce qu'elles expriment, ainsi la probabilité est toujours comprise entre zéro et l'unité tandis que la fréquence s'exprimera entre zéro et cent et une occurrence sera un nombre entier positif.

208-§ Il existe deux utilisations possibles des probabilités. Nous considérons que des événements apparaissent indépendamment ou non. La différence entre ces deux cas est simple.

209-§ PREMIÈRE OPTIQUE. La probabilité d'apparition d'une lettre *OU* d'une autre lettre est

[148] La confusion entre probabilité et fréquence est nocive dans la méthodologie cryptanalytique. Nous verrons à la page 174 que l'amalgame conduit à une erreur d'analyse de l'indice de coïncidence.

la somme des probabilités respectives de ces lettres. Dans la langue anglaise les voyelles ont pour probabilité *Pa, Pe, Pi, Po, Pu, Py,* le reste des lettres étant des consonnes, la probabilité d'obtenir soit une voyelle *OU* une consonne est la somme des probabilités respectives des voyelles et des consonnes c'est-à-dire 1 : vous êtes donc certains de tirer une voyelle ou une consonne. La probabilité d'obtenir les voyelles *a OU e* est $P(a|e)=Pa+Pe$. La probabilité[149] d'obtenir une voyelle est $P(V)=Pa+Pe+Pi+Po+Pu+Py$ le reste étant des consonnes $P(C)=1-Pa-Pe-Pi-Po-Pu-Py$: votre certitude s'amenuise en une possibilité.

210-§ DEUXIÈME OPTIQUE. Par contre, si vous vous demandez qu'elle est la probabilité de réussir le tirage d'une lettre *e ET* d'une lettre *a* alors il vous faut multiplier la probabilité de chacune de ces deux lettres $P(a,e)=Pa.Pe$. La probabilité de choisir aléatoirement deux voyelles dans un texte de langue anglaise est $P(V).P(V)$ soit approximativement 0.16 , puisque $P(V)\approx 0.4$: il est donc plus incertain de réussir ce tirage que celui de la PREMIÈRE OPTIQUE.

Utilisons les statistiques

211-§ Par méthode statistique nous entendons

> *Le traitement mathématique de l'observation de données en accord avec les lois fondamentales des probabilités.*

212-§ Une variable statistique est une variable qui peut prendre un nombre fini ou infini de valeurs de telle façon que la somme des probabilités de cette variable soit égale à l'unité. Une statistique est le calcul d'un nombre obtenu à partir de l'observation de données. Le calcul d'une moyenne utilise des données[150]. La moyenne peut être pondérée par un coefficient tout comme celle de la quantité de mouvement de plusieurs éléments[151]. Il est d'usage de noter $\bar{x}$ le symbole représentant la moyenne, il est lu: « x barre ».

[149] En cryptanalyse, les probabilités ne sont pas déterministes et leur étude repose sur une approche empiriste. Dans des textes français, il est commun d'obtenir une somme des probabilités de voyelles de $p(e)+p(a)+p(i)+p(u)+p(y)+p(o)=0,446551$, et une somme des probabilités de consonnes de $q(c)=1-p(v)=1-0,446551=0,55345$.

[150] Si Pierre, Paul et Jacques ont respectivement 12, 13 et 14 ans alors l'âge moyen de ces trois jeunes gens est (12+13+14)/3=13 ans.

[151] Cas des mouvements différents des planètes de masses différentes de notre système solaire.

$$\bar{x} = \frac{\sum_{i=1}^{i=n} w_i \times x_i}{\sum_{i=1}^{i=n} w_i}$$

Equation 1 Moyenne statistique pondérée.

213-§ La formule se simplifie si tous les coefficients de pondération son égaux à l'unité[152], alors $\sum_{i=1}^{i=n} \omega_i$ devient égal à n et $\bar{x}$ devient:

$$\bar{x} = \frac{\sum_{i=1}^{i=n} x_i}{n}$$

Equation 2 Moyenne statistique.

214-§ Toutefois, il convient d'indiquer que le calcul de la moyenne est assez sensible aux valeurs *anormalement* petites ou grandes et peut devenir alors un mauvais indice[153] pour le cryptologue [LEGR1994].

215-§ Le *Mode* d'une distribution est la valeur la plus importante. Elle est une caractéristique importante en cryptologie car il est le seul paramètre utilisable pour les données qualitatives. C'est la recherche du Mode d'une distribution d'occurrences de lettre qui permet de résoudre un texte crypté par monosubstitution. Ce fut la première approche que FRIEDMAN adopta pour l'étude du manuscrit. Il présuma que le manuscrit de Voynich était une simple monosubstitution de lettres. L'indice qui lui faisait penser à cela était que le document devait être du treizième siècle. Fait assuré par une lettre manuscrite qui l'accompagnait. Or , à cette époque médiévale, les procédés d'encryptage n'étaient pas algébriquement compliqués. C'est pourquoi, sa première démarche fut d'associer le mode statistique avec la lettre la plus représentative de chaque langue écrite du treizième siècle. Mais aucune de ces langues : Grecque, Arabe, Latine, Anglaise et Allemande, ne révélait le texte clair.

152 Cas de deux corps de même masse circulant dans la même direction.

153 Cas d'une pluie de météorites dans laquelle une météorite anormalement grosse se dissimulerait ; si l'on calcule la moyenne de l'ensemble alors le gros météore risque de passer inaperçu et dans ce cas le calcul de la moyenne comporte une erreur de jugement.

216-§ Maintenant que nous savons calculer une moyenne statistique et en déterminer son mode, nous déterminons la variation des écarts des données par rapport à cette moyenne. Nous l'appelons *« Variance »*, nous la notons:

$$s^2 = \frac{\sum_{i=1}^{i=n} \left(x_i - \bar{x} \right)^2}{n}$$

Equation 3 Variance.

217-§ La variance est l'écart-type exprimé au carré, elle est homogène au carré de x. Si x est exprimée en mètre alors la variance sera exprimée en mètre carré [LEGR1994]. L'écart conserve l'unité de x et est la racine carré de la variance.

$$s = \sqrt{\frac{\sum_{i=1}^{i=n} \left(x_i - \bar{x} \right)^2}{n}}$$

Equation 4 Ecart-type.

218-§ Il est indispensable de remarquer qu'une étude qui n'indiquerait que la moyenne sans l'écart-type ne serait pas valable [LEGR1994].

Cette équation est utile lorsque nous devons connaître le groupe de lettres qui se distinguent par leurs occurrences. Les lettres les plus fréquentes d'une distribution appartiennent au premier[154] écart-type[155].

[154] En pratique, nous différencions trois types de groupes de fréquences.

[155] Dans les monosubstitutions la distribution des statistiques est conservée. L'écart-type de la distribution statistique du cryptogramme reste égal à celui d'un texte clair. Cependant, à l'écart-type considéré correspondra une série de lettres différentes de celle d'une distribution de référence. Comment retrouver le message clair ? Nous déterminons le Mode de la distribution qui correspond logiquement à celui de la lettre E de la langue Française. Nous calculons l'écart entre la position de la lettre E (si l'origine est A = 0 alors E =4) et la lettre correspondante au Mode. Nous appliquons cet écart sur l'ensemble du cryptogramme et nous trouvons le texte clair. Nous pouvons, pour confirmer ce calcul, calculer la moyenne pondérée de la distribution statistique du cryptogramme et la comparer avec la moyenne pondérée de référence.

Indices laissés par les monographies

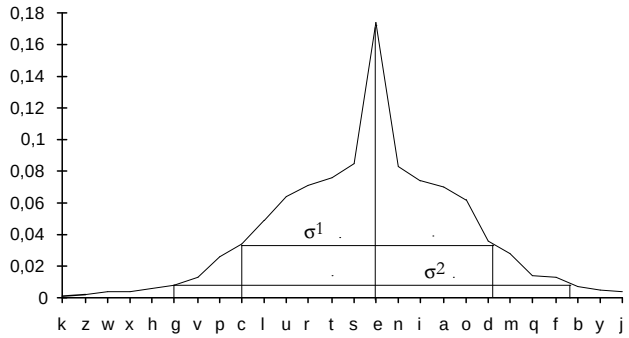
219-§ La distribution statistique montre globalement les caractéristiques d'un document. Nous apprécions son étendue et son élargissement. Le mathématicien « cryptologue » se fie aux caractères mathématiques de la courbe obtenue. Il utilisera par exemple : les calculs de moyennes et d'écart-type. Il recherchera le mode de la distribution peut-être utilisera-t-il les interquartiles. Il pourra aussi caractériser la distribution par les coefficients de Pearson comme nous l'avions fait pour un essai de caractérisation des textes génétiques [CASA1994].

220-§ Dans tous les cas, la représentation graphique est une méthode pratique pour le cryptologue qui fait confiance à l'intuition et la perception de la forme.

> **SINKOV avait cette qualité qui lui permettait à partir d'un document de retrouver un mot probable sans pour autant être capable de comprendre immédiatement le document étudié** [HODG1988]**.**

221-§ Nous allons regarder quelques représentations graphiques de documents afin de comprendre la relation qui existe entre l'approche statistique et la perception que nous pourrions appeler tantôt « déduction » tantôt « induction ».

222-§ Les statistiques d'un texte montrent les proportions d'utilisation de chaque lettre et de chaque mot. La représentation de ce type de distribution permet d'évaluer la nature du langage qui a servi à la rédaction du cryptogramme. Il est courant par exemple



Distribution Gaussienne avec point d'exception des statistiques monogrammiques de la langue française.

Calcul de σ1 : σ1 = écart-type premier = 0,039176 avec N éléments = 26 et X_{moyen} = 0,03842577. L'intervalle constitué par σ1 comporte 11 lettres : D L R N S E A I T U O. Il reste N2 éléments tels que N2 = 26 - $N_{\sigma 1}$, soit N2 = 26 - 11 = 15.

Calcul de σ2 : σ2 = écart-type second = 0,010551 avec N2 éléments = 15 et X_{moyen} = 0,011297. L'intervalle constitué par σ2 comporte 7 lettres : F V M C P Q G

d'associer un mode statistique de dix-sept pour-cent à la langue française car elle est la seule langue à disposer d'une lettre aussi fréquemment employée.

223-§ Cependant, les statistiques littéraires sont différentes des statistiques d'un langage de programmation. La spécificité d'un langage influence les statistiques d'un texte. Non seulement il existe des distinctions entre langues naturelles mais encore chacune de ces langues voit ses statistiques varier en fonction du contexte et de l'indexicalité [ETHN1986]. Il est donc parfois difficile de pouvoir faire la différence linguistique entre plusieurs cryptogrammes.

En effet, le cryptogramme est représentatif non seulement de son langage de rédaction mais aussi du procédé d'encryptage qui lui a été appliqué.

224-§ Mais il serait faux de croire que les langues naturelles sont suffisamment différentes pour pouvoir les distinguer aisément à travers le masque du chiffrement. Il existe des intersections entre langages qui sont de réels problèmes pour le cryptanalyse. Bien que la langue anglaise diffère de la langue française, il n'en est pas moins vrai qu'elles partagent des vocables communs. Or, nous constatons, dans tous les ouvrages de cryptologie, que la connaissance de la langue est un *a priori* indispensable, et que, si vous ne connaissez pas la langue, il vous faut utiliser la formule qui permet de la découvrir. Soit, nous savons que son application est limitée à quelques exceptions. Mais ceci ne nous surprend pas puisqu'au XIV^{ème} siècle QALQASHANDI faisait déjà remarquer que,

> *bien que le principe fondamental soit de connaître le langage de rédaction, il fallait bien constater que les statistiques des lettres du Coran étaient souvent différentes de celles des autres textes.*

Nous nous demandons si effectivement le cryptanalyste est en mesure de travailler indépendamment de la connaissance de ces valeurs référencées ?

225-§ Nous voyons que cela est rarement le cas. BARKER montre que la cryptanalyse d'une double transpositions passe avant tout par la reconstruction du texte clair avant même celle des clés de transpositions[156]. La reconnaissance anagrammatique pourrait

[156] Les lettres du message clair sont substituées à leur numéro de colonne correspondante. Cette chaîne de numéro est indexée de un à la dimension du texte. Puis nous classons les numéros d'indexation par ordre croissant des numéros de colonne. Ainsi si le texte apparaît sous la forme 4 3 6 1 2 5 alors l'indexation donne le rapport suivant

N°colonne	4	3	6	1	2	5
Indexation	1	2	3	4	5	6
Classement	4	5	2	1	6	3

le classement correspondant sera la suite 4 5 2 1 6 3.

montrer, qu'en ce cas, la *gestalt* précède l'analyse. Nous retrouvons ce fait dans la détection du motif de DREYFUS dans le télégramme de PANIZZARDI (page 211). Il se résume à l'expression de GAUSS rapportée par WATZLAWICK :

> *Je connais déjà la solution, il me reste maintenant à découvrir comment j'y suis parvenu,*

226-§ et qu'alors présumant du vocable, il devient possible de reconstruire le procédé d'encryptage. La connaissance *a priori* de la langue se montre alors incontournable. Toutefois, dans les méthodes spécifiques du décryptement, nous constatons que le calcul de la longueur de la clé de polysubstitutions peut être effectué sans connaissance *a priori* de la langue, et en cela, la méthode de KASISKI est très intéressante. La méthode[157] de SALTON et DAMASHEK [SALT1991] est de même remarquable puisqu'elle catégorise les textes entre eux uniquement à partir de leurs n-grammes.

Position	p1	p2	p3	p4	p5	p6
Classement	4	5	2	1	6	3

Nous calculons la différence $P_{i+1} - P_i$ pour chaque P_i et nous obtenons une suite de nombres positifs et négatifs. Dans cette séquence nous recherchons le motif le plus grand et redondant. A chaque motif correspond une séquence de numéro de colonne. La différence mathématique entre ces séquences de numéro de colonne indique la dimension de la première clé de transposition. Nous retrouvons ici quelques similitudes avec le motif de *DREYFUS* (page 213). Pour retrouver la deuxième clé de transposition, nous faisons remarquer que la première colonne de la deuxième clé est composée des premières lettres du cryptogramme. Nous recherchons la colonne de la première grille de transposition qui contient la première lettre (sous sa forme indexée) du cryptogramme. Cette colonne est alors la première ligne de la deuxième grille de transposition. La largeur de cette grille sera déterminée par la coïncidence entre deux lettres identiques ayant le même numéro d'indexation. Nous répétons l'opération pour les autres lignes et colonnes qui livrent de plus en plus d'intersections. Les deux grilles étant complétées il est possible de lire les deux combinaisons de clé.

[157] La première étape consiste à calculer la fréquence de chaque n-gramme distinct. Si un document m a pour J le nombre de n-grammes distincts et m_i l'occurrences du n^{ème}-gramme i alors de n^{ème} Vecteur x_i est

$$x_i = \frac{m_i}{\sum_{j=1}^{J} m_j}$$

Si un autre document n a pour n^{ème} Vecteur le vecteur y_i alors le cosinus de l'angle entre ces deux textes est le produit de la somme normalisée

$$cos(q_{mn}) = \frac{\sum_{j=1}^{J} x_{mj} \times y_{nj}}{\sqrt{\sum_{j=1}^{J} x_{mj}^2 \sum_{j=1}^{J} y_{nj}^2}}$$

Nous observons pourtant que l'indépendance de l'analyse par rapport au langage est occasionnelle.

227-§ Il faut avouer que les méthodes sont foncièrement liées à la notion de contexte linguistique. Par exemple, nous considérons que l'efficacité de la méthode de sélection des cas favorables, par l'indice de coïncidence de FRIEDMAN, est dépendante de la bonne adéquation des valeurs statistiques de référence avec les valeurs probables du cryptogramme étudié.

228-§ Même si depuis les travaux de MARKOV, sur les chaînes linguistiques, nous disposons d'une meilleure approche analytique, il n'en demeure pas moins vrai que le mauvais choix des statistiques de référence conduit à l'impossible reconstruction du texte clair. Le cryptanalyste est toujours sur cette corde raide, qui le place entre la tentation de l'induction, lui permettant d'avancer dans son analyse, et la pratique du Commandant BAZERIES, nous rapporte Fletcher PRATT, qui consiste à élaborer une méthode spécifique pour chaque cryptogramme. En fait, le choix de l'induction est valable pour de petits procédés d'encryptage comme celui de Jules CÉSAR[158]. Pourtant déjà une simple monosubstitution par alphabet aléatoire rend la résolution complexe.

Ces simples équations statistiques nous permettent déjà d'apprécier les premières mesures statiques[159] des deux versions du manuscrit de Voynich.

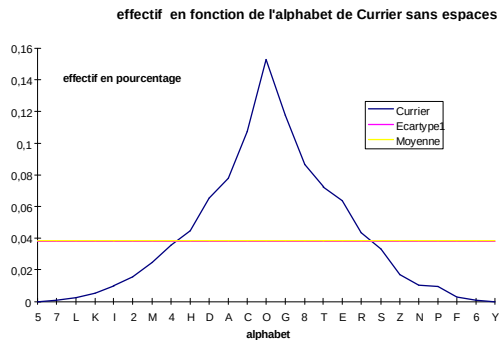
229-§ Nous calculons les statistiques monogrammiques, la moyenne des effectifs et l'écart-type leur correspondant. Nous allons donc découvrir si une lettre est caractéristique d'une distribution ; est-ce que le mode de la distribution permet de soupçonner un système d'encryptage particulier ?

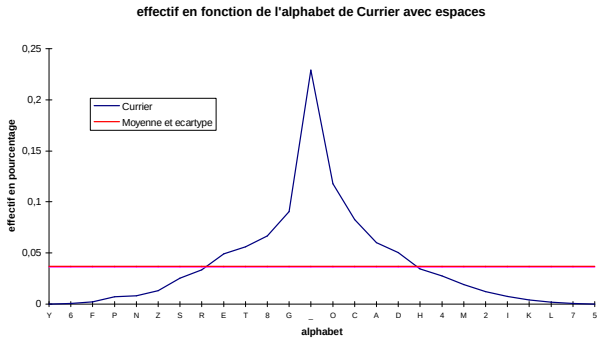
---

158 Jules CÉSAR écrivait à CICÉRON en remplaçant chaque lettre claire par celle située trois rangs plus loin dans l'alphabet. Ainsi, la phrase *Alea jacta est* est cryptée *Dohd mdfwdhvw*. Par la suite, CÉSAR voyant son amitié pour CICÉRON s'amenuiser, préféra utiliser un messager de confiance pour transmettre ses messages plutôt qu'un chiffre lisible potentiellement décryptable par ses ennemis [CESA1964] De nos jours, tout alphabet de substitution obtenu par décalage de l'alphabet normal est appelé *« alphabet de Jules CÉSAR »,* même si le décalage est différent de trois [KAHN1980]. Le texte crypté obtenu est incompréhensible mais deux calculs statistiques vont révéler la fragilité de la méthode.

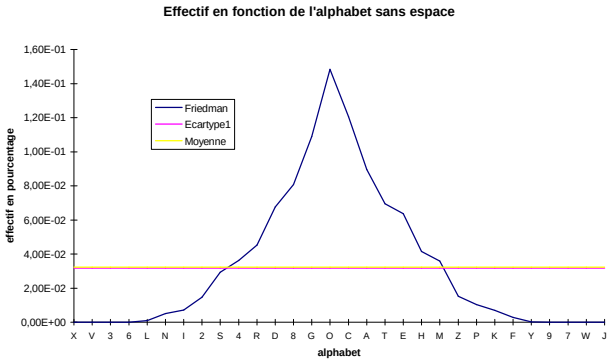
Chaque lettre claire est cryptée par simple bijection. A une lettre claire correspond une lettre cryptée: *lettre claire ↔ lettre cryptée*. L'une correspond à l'autre et *vice versa*, il y a conservation des statistiques d'une distribution normale, la lettre cryptée se substituant à la lettre claire. Si un texte comporte la lettre E et que celle-ci se trouve substituée par la lettre N alors N sera présente à la hauteur de 0,1732 fois la taille du texte et ainsi de suite pour les autres lettres. Les lettres cryptées du groupe décrit par le premier écart-type sont les lettres claires du groupe du premier écart-type d'une distribution statistique classique.

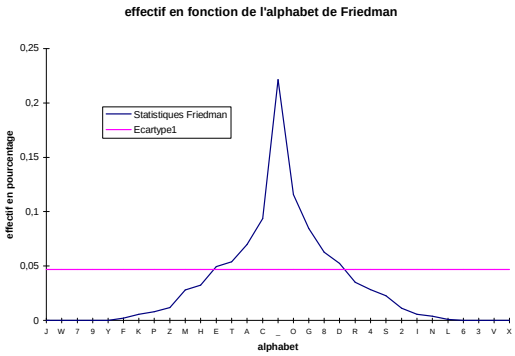
159 Cf. Annexe, page 367.





230-§ Dans le cas de la transcription de CURRIER, le mode statistique des effectifs en fonction de l'alphabet de CURRIER sans espace est occupé par la lettre **[O]** et le premier écart-type donne le groupe des lettres les plus fréquentes[160] **[C, G, A, 8, D, T, H, E, R, O].** Dans la version de FRIEDMAN, le mode est identique à celui de CURRIER mais la distribution est suffisamment répartie différemment pour donner un premier groupe[161] plus grand **[G, C, 8, A, D, E, R, H, 4, M, O].** Le reste de l'intersection[162] de ces deux groupes donne les lettres **[4, M]**qui sont statistiquement limitrophes à la version de CURRIER.





231-§ Par contre, lorsque nous considérons les alphabets pourvus du caractère espace alors nous constatons que le premier groupe[163] est composé des lettres **[C, O, A, G, T, 8, E, D]** dont l'espace représente le mode. Les deux groupes sont identiques ; nous concluons donc que

---

[160] ᶜ ᵍ ᵃ ⁸ ᵗᵗ ᶜᵣ ᵠᵠ ˣ ʔ ᵒ

[161] ᵍ ᶜ ⁸ ᵃ ᵗᵗ ˣ ʔ ᵠᵠ ᵠʷ ᵒ

[162] ᵠʷ

[163] ᶜ ᵒ ᵃ ᵍ ᶜᵣ ⁸ ˣ ᵗᵗ

Conclusion 4 Les versions monographiques de FRIEDMAN et de CURRIER correspondent lorsqu'elles sont prises avec les caractères espaces.

232-§ L'approche monographique par les statistiques est remarquablement déconcertante. L'*a priori* que BACON est l'auteur du manuscrit (Hypothèse 3 et Hypothèse 1) et que l'alphabet sténographique utilisé était connu de lui (Constat 3 et Hypothèse 4) laissaient penser que le manuscrit datait du treizième siècle.

Constat 20 La répartition statistique « normale » du caractère espace dans le texte indique que l'opération de cryptage n'intervient que sur les mots.

233-§ et comme le Constat 8 de FEELY dit que les statistiques[164] monogrammiques du latin sont très proches de celles du manuscrit alors nous pourrions conclure que l'approche monographique par les statistiques nous dit que le manuscrit est issu d'un procédé d'encryptage basé sur la monosubstitution alphabétique (Note 155). Le test *Phi*[165] [CALL1985a] ne contredit pas ces observations et accentuerait l'idée que le manuscrit est bien issu d'une substitution monoalphabétique. De plus, la forme de la distribution est adéquate à l'hypothèse de la monosubstitution et que son rejet s'envisage quand

> *L'absence de crête marquée dans une distribution de fréquence indique qu'une forme complexe de substitution est utilisée. L'apparence d'une courbe plate est un des critères de rejet de l'hypothèse de la substitution monoalphabétique [CALL1985a].*

234-§ Pourtant, NEWBOLD n'avait pu résoudre cette monosubstitution et avait envisagé l'hypothèse qu'il existât des procédés successifs que la bribe « MULTAS PORTAS » sembla indiquer. Mais comme aucune analyse monographique et anagrammatique (Conclusion 1) n'aboutit à une solution :

---

164 Effectifs des lettres et représentation du premier groupe.

165 Le *Phi* test est noté **Φ**. Initialement, il était destiné aux cryptogrammes de petites dimensions (moins de 200 caractères). Le principe repose sur une distinction entre, une mesure observée Φ_o, une mesure théorique Φ_p et une mesure équiprobable Φ_r. Quand la mesure observée tend à être la mesure théorique, et se détache de la mesure équiprobable, alors le cryptogramme est sensé être issu d'un encryptage monoalphabétique ; sinon, le procédé utilisé est plus complexe. Cette méthode est très emprunte de l'idée de référence dont la conclusion est dépendante de la mesure théorique Φ_p et de la mesure équiprobable Φ_r. Or, la mesure théorique est une induction et la mesure équiprobable repose sur le constat qu'il existe un nombre clairement défini de lettres dans l'alphabet théorique ce qui exclut les systèmes à représentations multiples et les intersections de langages.

Conclusion 5 Il faut nous rendre à l'évidence que l'étude statistique monographique est insuffisante.

235-§ Pour cette raison, nous élargissons notre étude à des graphes de plusieurs lettres que nous appelons *n-graphes* ou *n-grammes*. Nous passons de l'étude monogrammique à l'étude digrammique qui débouchera sur une étude Markovienne des couples de lettres que nous plaçons en parallèle à leurs incidences sur la mesure d'ordre de SHANNON.

Approche multigraphiques

236-§ Dans la pratique d'analyse de texte, nous dissocions chaque mot en voyelles et en consonnes[166]. Le passage du monogramme au digramme, du digramme au trigramme puis du n-gramme au (n+1)-grammes, montre qu'il existe une transition d'états que l'on désigne par probabilité de transition.

237-§ Nous distinguons deux états, l'état initial et l'état final. L'obtention de l'état final est conditionné par l'état initial. Au début, l'état monogrammique d'un texte est l'alphabet initial. Quand nous étudions les lettres qui succèdent à chacune des lettres de l'alphabet nous cherchons l'existence d'un ensemble de règles distinguant le texte étudié d'une séquence aléatoire de lettres. Initialement, les monogrammes du texte ne montrent pas la structure du texte mais celle-ci apparaît quand nous étudions les transitions de groupes de lettres de plus en plus grands. Finalement, nous aboutissons à une représentation aristotélicienne des transitions de lettres. L'arbre obtenu est la forme construite —peut être unique— du texte étudié [MARK&PETR1981].

238-§ Si l'on approfondit l'arbre décrivant les chaînes de MARKOV. On constate que certaines branches sont finies. Il existe des filiations d'alternances de voyelles et de consonnes pour lesquelles l'obtention de suite de lettres est probante.

[166] Pour les langues non sémitiques.

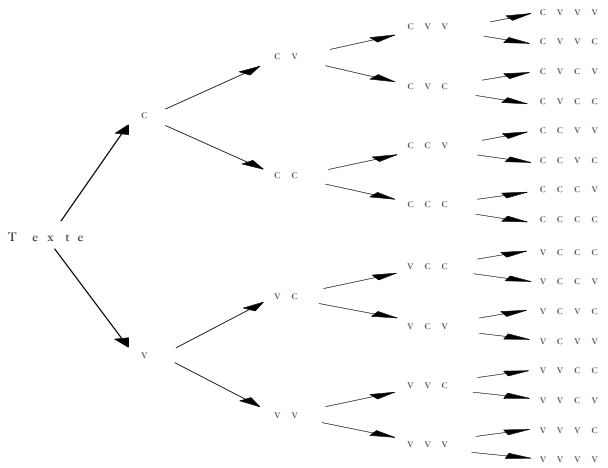


Figure 8 Arbre markovien. Alternance Voyelle Consonne.

239-§ D'un point de vue théorique chacune des probabilités est différente de zéro mais dans chaque langue il existe des combinaisons impossibles de lettres. La profondeur de l'arbre markovien est donc inégale selon les branches du fait même que certaines probabilités convergent vers zéro.

De ce fait, il existe des propositions uniques propres à chaque langage, la distribution des statistiques de présences monogrammiques, digrammiques, ou n-grammiques, est dépendante[167] de la langue prise dans son contexte d'expression.

240-§ Les présences de lettres sont différentes selon les époques et les genres littéraires. FEELY constatait que le latin employé par R. BACON était différent, plus condensé, et plus abrégé que le latin classique (page 68). La langue française[168] n'échappe pas à ce constat, le manuscrit de Voynich non plus. La probabilité monogrammique est insuffisante pour montrer une structure de combinaison de lettres remarquables. Jusqu'à présent l'approche monogrammique n'a pas permis de distinguer les mots de VOYNICH de leurs anagrammes. Pourtant, nous concevons comme évident que l'ordre des lettres se lie étroitement à la compréhension et qu'il nous faut rechercher

167 Les différences se trouvant parfois déjà dans la dimension des alphabets. Nous pensons à la langue Russe dont l'alphabet comporte trente-trois lettres contre vingt-six en français.

168 En premier lieu, la langue Française se trahit par la forte prépondérance de sa lettre *« E »* qui a une fréquence double de sa deuxième lettre *« A »*. Ses voyelles sont au nombre de six mais elles occupent plus des deux cinquièmes du texte. La lettre *« E »* est présente dans la plupart des couples fréquents de lettres. Le bigramme ***« QU »*** est le seul bigramme formé d'une lettre rare et d'une lettre fréquente qui soit lui-même fréquent. Les bigrammes fréquents formés de deux lettres identiques sont dans l'ordre, *« EE », « LL », « TT », « NN », « MM », « RR », « PP », « FF », « CC »*. Le seul bigramme formé de voyelles identiques est *« EE »*. Les trigrammes fréquents sont des terminaisons « *ENT », « AIT », « ANT »,* ou de petits mots, *« LES », « QUE », « DES », « EST »*.

des structures plus conséquentes de lettres si l'on veut cerner l'architecture du manuscrit.

241-§ TILTMAN avait pour idée que le manuscrit était écrit à partir d'un langage synthétique primitif (Hypothèse 9); et lorsqu'il étudia le procédé de Cave BECK, il fit remarquer[169] que : *Cave BECK ajoute la lettre « s » ou le chiffre « 8 » pour signifier que le mot codé est sous sa forme plurielle.* et qu'alors il serait opportun d'étudier les aspects digraphiques et trigraphiques des lettres du manuscrit.

Indépendance digrammique

242-§ La première approche qui permet d'établir quelques différences entre les anagrammes —et de se distinguer d'une approche monogrammique— consiste à calculer les probabilités des couples de lettres. Le principe est de découper un texte[170] de deux lettres en deux lettres. Puis de calculer[171] la proportion de chaque couple différent de lettres par rapport au nombre total de couples rencontrés.

243-§ Nous obtenons un ensemble de valeurs comprises entre zéro et un pour l'ensemble des couples de lettres ((A, A), (Z, Z)) pour la langue française, ((A, A), (Я, Я)) pour la langue russe et ((ⲋ, ⲋ), (ⳍ, ⳍ)) pour le manuscrit[172]. Les probabilités des digrammes contenus dans le manuscrit montrent[173] qu'il existe des cas impossibles d'associations de lettres[174] comme il en existe aussi dans les langues naturelles.

244-§ Nous remarquons que l'étude digrammique sans dépendance nous permet de distinguer une chaîne de lettres formant un mot d'une chaîne comportant les mêmes lettres mais mises en désordre. Cette méthode est donc plus acceptable que l'approche monographique. Cette recherche de dénombrement des digrammes avec indépendance doit nous permettre de comparer ce que nous remarquons de

---

169 Constat 13, page 81.

170 Le texte de *n* caractères contiendra *n-n modulo 2* couples de lettres.

171 Considérons l'ensemble des couples *(x2n-2, x2n-1)* de lettres *(x0, x1, x2,..., x2n-1)* d'un texte. Les digrammes satisfont les deux probabilités : 1) La probabilité d'obtenir la lettre *x2n-2* et la lettre *x2n-1* lettre, le couple *(x2n-2, x2n-1)* est ce qu'on appelle un digramme, si α est l'alphabet alors $P(x2n\text{-}2, x2n\text{-}1) \geq 0$, telle que, $0 \leq (x2n\text{-}2, x2n\text{-}1) < \alpha$. 2) Si l'on considère l'ensemble des arrangements possibles des couples de lettres *(x2n-2, x2n-1)*, la somme des probabilités est : P(x0, x1) +...+ P(xn, xn+1) est 1, $\sum_{0 \leq x2n-2}^{x2n-1 \leq \alpha} p(x_{2n-2}, x2_{n-1}) = 1$.

172 Alphabet de trente lettres (Tableau 2 page 103, page 99 & Tableau 14—Tableau 16, page 394).

173 Pour des raisons de lisibilité les probabilités des Tableau 14 à celles du Tableau 16 sont à diviser par 10 000 (page 394).

174 L'ordre alphabétique est indépendant de tout ordre alphabétique interne au manuscrit.

particulier dans la présence des digrammes du manuscrit et ceux que nous trouvons dans des textes non cryptés. Les digrammes pris un à un et sans considérer leurs liens immédiats avec les autres digrammes procède de la même méthode d'analyse des monosubstitutions ; mais ici, nous considérons la substitution comme digraphique[175] ; deux lettres claires sont remplacées par deux autres lettres (Note 99).

Hypothèse 13 Le manuscrit est le résultat d'une substitution digraphique.

245-§ Si nous devons comparer les digrammes du manuscrit avec les digrammes des textes de langue naturelle alors nous devons constater un fait de première importance : l'alphabet de symboles du manuscrit est plus grand que tout autre alphabet connu[176]. La combinatoire des symboles, pris deux à deux, est donc plus grande dans le manuscrit que dans les autres textes. Nous nous attendons alors à une distribution plus continue dans le manuscrit que dans un texte « classique ».

246-§ Nous considérons dans un premier temps que les digrammes sont formés indépendamment de tout caractère espace ; les couples de lettres « à cheval » entre deux mots deviennent possibles, nous obtenons la Figure 9.

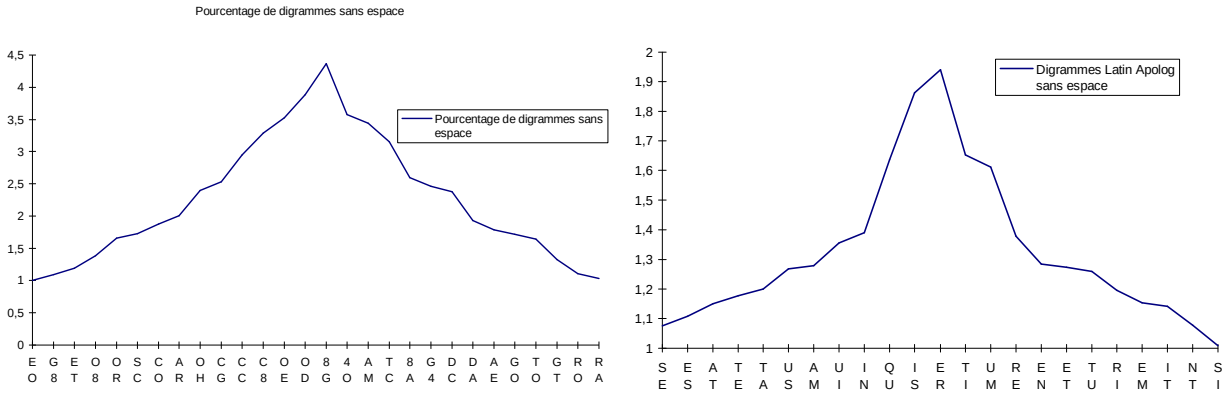


Figure 9 (à gauche) Digrammes sans espace de MS408.

[175] Le système PLAYFAIR a été inventé par Charles WHEASTONE qui le fit accepter par Lord PLAYFAIR. Le système sera utilisé pendant la première guerre Mondiale et pendant la guerre des Boers de 1902. La méthode de substitution digrammique substitue deux lettres par deux autres lettres. A partir d'une grille identique à celle de POLYBE, aux dimensions 5 lignes sur 5 colonnes, on place les lettres de l'alphabet crypté. Le texte clair est découpé en digrammes. On prend le premier digramme du texte, on compare chacune de ses deux lettres avec les lettres de la grille ; puis selon des règles déterminées d'avances on prend pour digramme crypté le couple de lettres complétant le rectangle dont les deux lettres claires forment deux des extrémités.

[176] A l'exception de l'alphabet Russe.

Figure 10 (à droite) Digrammes sans espace du texte latin
Apologia Apuleii (APOLOG.TXT).

La Figure 9 montre que

> **Constat 21 Il existe de nombreux digrammes très fréquents, [OE], [OD], [8G], [4O], bien que le couple [8G] soit le plus fréquent ; il ne dépasse les suivants que d'un pour-cent.**

247-§ La Figure 9 (**[OE, OD, 8G, 4O]**)[177] s'apparente[178] à la Figure 10 (QU, IS, ER, TI) qui représente la distribution des digrammes sans espace du latin.

> **Constat 22 La distribution des digrammes sans espace —de haute-fréquences— du manuscrit est proche de la distribution des digrammes —de haute-fréquences— sans espace du latin.**

248-§ La Figure 10 montre que les digrammes les plus fréquents sont associés entre eux pour former des mots qui sont eux-mêmes très courants. En langue anglaise, le cône principal est formé par les couples de lettres : IN, HE, TH, ER (Figure 11).

[177] ox, of, 89, 4o.

[178] Compte tenu de la différence de diversité digrammique : l'alphabet de Voynich peut engendrer 30^2=900 digrammes différents contre 22^2=484 pour le latin. Par contre, l'aspect de la courbe (Figure 9) tend à être celui d'une courbe plate qui signifie que l'encryptage du manuscrit est probablement complexe [CALL1985a].

Hypothèse 14 Nous en déduisons[179] que les couples, [OE], [OD], [8G], [40] , sont à la base de l'élaboration du vocabulaire de ms408.

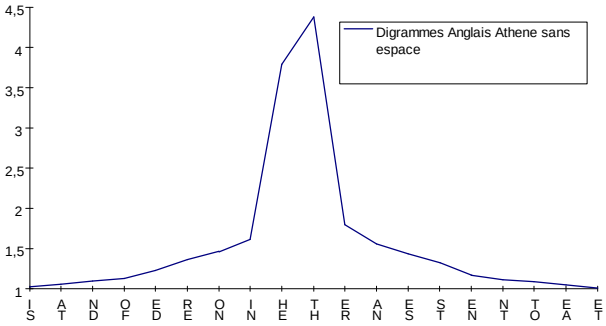


Figure 11 (à gauche) Digrammes sans espace d'un texte Anglais.

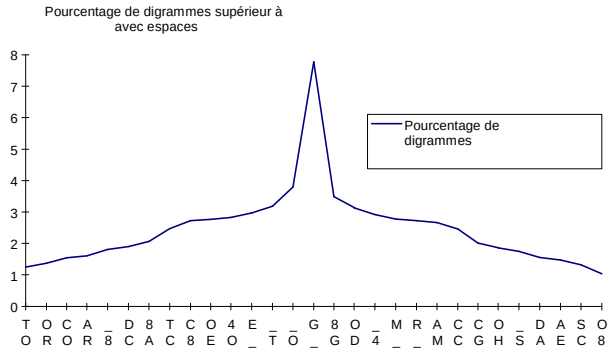


Figure 12 (à droite) Digrammes avec espace de MS408.

249-§ Maintenant, nous considérons tous les couples de lettres avec et sans espace. Les digrammes de lettres entre mots ne sont plus possibles et deviennent des couples de lettres avec espace : les proportions de digrammes sont donc modifiées par la disparition de ces couples de lettres et altérées aussi par l'émergence de nouveaux couples auparavant entrecoupés d'un espacement.

250-§ La Figure 9 et la Figure 10 se transforment en Figure 12 et Figure 13. Les apparences sont similaires ; elles sont caractérisées par deux « pics ».

Constat 23 Le mode « M_ » des digrammes du latin avec espaces est moins accentué et cinq couples de lettres constituent le cône majeur de la distribution (T_, S_, M_, E_, ER).

Par contre,

[179] Il est notable qu'en réalité leur nombre doit être plus proche de huit que de quatre si l'on tient compte de la différence de diversité des digrammes, du langage de Voynich, du latin et des autres langages moins pourvus en lettres alphabétiques.

Constat 24 Le mode [G_] des digrammes avec espace du manuscrit est très isolé des autres ; seulement[180] trois couples forment le cône majeur de la distribution, [_O], [G_], [8G].

251-§ Le Constat 23 fait remarquer que la diversité des digrammes est proche du mode de la distribution et qu'à l'occasion le digramme « M_ » pourrait être destitué par l'un de ces cinq digrammes.

252-§ Le Constat 24 s'oppose à toute alternative ; le couple **[G_]** agit en despote sur le manuscrit comme la lettre « E » le fait sur les monogrammes de la langue française.

253-§ Pour résumer notre approche d'indépendance digrammique ; nous dirons que

Constat 25 Le digramme [G_] est exceptionnellement représenté et ne permet pas à d'autres digrammes de se substituer à lui.

Par conséquent, nous nous demandons si la lettre **[G]** est une lettre non nulle.

Hypothèse 15 Le Constat 25 suggère que la lettre [G] du manuscrit est une lettre nulle.

254-§ L'idée que le manuscrit soit pensé en latin et écrit grâce à une substitution digraphique n'est pas suffisante compte tenu du Constat 25 et de la dimension de l'alphabet de symboles de VOYNICH ; et surtout, compte tenu du manque de similitude entre les deux cônes —de la Figure 12 et de la Figure 13— que décrivent les Constat 23 et Constat 24.

255-§ Seule subsiste la correspondance des deux cônes de la Figure 9 et de la Figure 10 mais qui n'affirme aucune hypothèse sinon celle que si le manuscrit de Voynich est issu d'une substitution digraphique alors OE, OD, 8G, 40 sont les digrammes des mots les plus fréquents et qu'alors le décryptage[181] est évident.

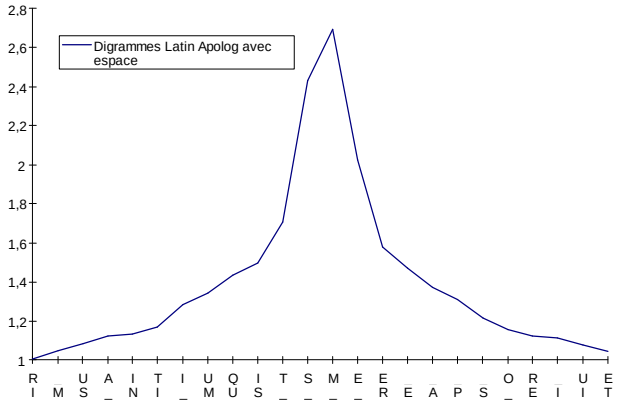
---

[180] Nous nous attendions à ce que le cône principal soit formé par un nombre équivalent de digramme que nous retrouvons dans le latin. Apparemment, le comportement des lettres de Voynich face au caractère « espace » est différent du comportement des lettres anglaises et latines. Cette marque spécifique nous dévoile un trait du manuscrit.

[181] Quand deux distributions ont la même forme, la même amplitude : les deux courbes sont juxtaposables et montrent que la méthode PLAYFAIR —substitution digraphique— a les mêmes fragilités qu'un alphabet aléatoire.

Dans le cas d'une substitution digraphique, on ne raisonne plus une analyse en terme de statistiques monogrammiques mais en terme de statistiques digrammiques ; ainsi peu nous importe de savoir si la lettre E est présente à 17 % ou non mais il nous importe de connaître quel digramme est le plus fréquent.

256-§ Nous ne disons pas qu'il existe une quelconque ressemblance entre le manuscrit et la langue anglaise; cependant, la comparaison trinitaire *concordance-contrariété-différence* est intéressante dans notre cas.



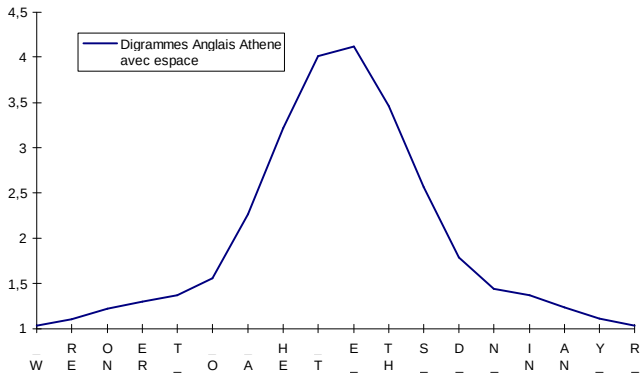


Figure 13 (à gauche) Digrammes avec espace du texte latin APOLOG.TXT (page 353).

Figure 14 (à droite) Digrammes avec espace de *Athene* (ATHENE.TXT) en Anglais.

257-§ La Figure 12 et la Figure 14 devraient, comme la Figure 9 et la Figure 11, être soit concordantes soit différentes ; *a priori*, elles sont différentes, mais en y regardant mieux, nous constatons qu'elles sont contrariées : la Figure 12 s'apparente à la Figure 11 et la Figure 9 s'apparente à la Figure 14. Les digrammes avec espaces du manuscrit montrent quelques familiarités avec les digrammes sans espaces du texte anglais et aussi que les digrammes sans espaces du manuscrit montrent des similitudes avec les digrammes avec espaces du texte anglais ; cette inversion soumet l'hypothèse que

---

Par exemple, dans la langue Française, on constate, d'après la distribution normale des digrammes d'un texte référence, que le plus fréquent de tous est ES. Nous devons donc rechercher le digramme crypté qui se distingue et nous considérons que son signifiant n'est pas le couple de lettres qui le compose mais qu'il s'agit en fait de ES.

Dans un cas pratique, il n'existe pas obligatoirement une distinction flagrante du mode par rapport aux digrammes suivants ; cependant, il y a un ensemble de digramme de Haute Fréquence (premier groupe) dans lequel nous trouvons l'équivalent clair du digramme crypté.

On doit se rendre à l'évidence que selon le genre littéraire certains digrammes peuvent ne pas se comporter normalement. C'est pourquoi il est important de rappeler que plus les statistiques linguistiques sont adaptées au genre "littéraire" et plus les éléments cryptés sont dissociables les uns des autres.

Les analyses précédentes (note 155) sur la reconstruction d'un message monosubstitué sont parfaitement applicables au cas de la méthode PLAYFAIR. On retrouve les mêmes caractéristiques d'ensembles tel qu'il existe un groupe de HF (haute fréquence), un groupe de FM (fréquence moyenne) et un groupe de FB (fréquence basse).

Hypothèse 16 Si la langue pensée dans le manuscrit est Anglaise alors le caractère espace n'est pas celui qui se montre comme évident.

258-§ De toute évidence ce que nous approchons et tentons de définir, comme étant : « ressemblant, similaire, différent », est l'expression d'une difficulté à trouver des analogies digrammiques sérieuses. Peut-être simplement parce que la diversité des langages ne nous permet pas d'exhumer les contours et les lignes séparatrices qui les délimitent. En fait, nous voyons essentiellement que les lettres de VOYNICH ne s'accordent pas parfaitement avec les caractères espaces. Notre étude d'indépendance digrammique est encore insuffisante.

259-§ A présent, nous allons considérer les digrammes du manuscrit comme étant successivement dépendants. Nous nous référons alors au travaux de MARKOV sur les transitions d'états et nous considérons le manuscrit comme une séquence de lettres cémentées les unes après les autres.

Dépendance digrammique

260-§ Posons que *x0, x1, x2* et *x3*, soient des lettres ; pour que la chaîne formée par la conjonction entre *p(x0, x1)* et *p(x2, x3)* puisse être indéniablement vraie dans son domaine de probabilité, il est nécessaire d'établir le lien entre *p(x0, x1)* et *p(x2, x3) ;* ce lien est la transition d'un état à un autre dont *n* dépend de *n-1*. C'est cette relation que MARKOV développe dans l'*étude des chaînes linguistiques du roman russe en vers d'A.S. Puskin : « Evgenij Onegin »* [MARK&PETR1981]. On peut donc définir un texte clair comme étant une génération de lettres par chaîne Markovienne avec une matrice de transition.

Nous construisons cette matrice[182] en déterminant l'abscisse comme étant l'état final de la transition et l'ordonnée comme l'état initial de la transition.

261-§ La probabilité de transition de  en  notée *p(/)* dit que l'événement est conditionné par l'événement . Le calcul de cette probabilité est le nombre de fois que le digramme apparaît divisé par le nombre de digrammes commençant par la lettre . Nous notons cette transition :

[182] Les matrices sont regroupées en annexe à partir de la page 394.

$$p(\text{ol} / \text{qo}) = \frac{\sum(\text{qo}, \text{ol})}{\sum(\text{qo})}$$

Equation 5 Transition d'état Markovien.

262-§ Le manuscrit n'utilise pas toutes les combinaisons de transitions de lettres[183] théoriquement disponibles. Le calcul des transitions d'états digrammiques nous apprend que toutes les transitions ne sont pas réalisables (Tableau 15) ; dans les deux cas ou le caractère espace, est, ou, n'est pas, considéré dans le calcul de la transition, le symbole ol ne paraît jamais après le symbole qo. Le digramme qol est impossible[184] dans le langage de VOYNICH.

> **Constat 26 Sur un ensemble de neuf cents combinaisons possibles de digrammes sans espace, il existe quatre cent cinquante et un digrammes impossibles.**
>
> **Constat 27 Sur un ensemble de neuf cent soixante[185] combinaisons possibles de digrammes avec espace, il existe cinq cent trente-deux digrammes impossibles.**

263-§ Les impossibilités de constructions digrammiques indiquent les limites de la construction du vocabulaire ; soit parce que l'auteur du manuscrit n'a pas eu besoin de ces mots qui n'apparaissent pas dans notre approche empiriste, soit parce qu'il existe une ou des impossibilités techniques (Code alphanumérique de KIRCHER, page 193) ne permettant pas de faire se suivre certains symboles.

> **Hypothèse 17 S'il est vrai que des transitions d'états sont absolument impossibles alors il doit exister une ou des (Conclusion 2) syntaxes[186] qui régissent les associations de symboles en mots.**

264-§ Les transitions avec espaces (Tableau 14) nous apprennent qu'un mot ne commence jamais[187] par les symboles **[J]**, Λ, **[W]**, **[x]**[188] et **[Z]**[189]. De même, un mot ne finit jamais par les symboles **[3]**, **[6]**, **[J]**, Λ[190], et **[X]**.

---

[183] Hormis le caractère espace.

[184] En nous basant sur les résultats uniques de notre approche empirique.

[185] 960 car le caractère espace ne peut se succéder à lui-même.

[186] Nous rejoignons le sentiment de CURRIER qui estimait —sans pouvoir le démontrer— que la ligne gouvernait la formation des mots.

Constat 28 Quand il s'agit de la transcription de FRIEDMAN alors cinq symboles, [J], Λ, [W], [x], [Z], ne commencent jamais un mot ; cinq symboles ne finissent jamais un mot [3], [6], [J], Λ, [X].

265-§ Le Constat 28 induit que trois symboles ne sont jamais situés au début et en fin de mot.

Constat 29 [J], Λ et [X] ne sont jamais utilisés[191] pour commencer ou finir un vocable.

266-§ En fait, le comportement de certaines lettres du Constat 28 n'est pas aussi intéressant qu'on aurait pu l'espérer.

- Le symbole Λ apparaît deux fois dans notre texte pour la simple raison qu'il se confond avec un symbole 𝔞 mal rédigé ou inversement un symbole 𝔞 que l'on confond avec un symbole Λ mal écrit.

- Le symbole **[Z]** est en fait celui qui pose le plus de problème[192] puisqu'il est le complémentaire de quatre digrammes, **[DZ]**, **[FZ]**, **[HZ]**, **[PZ]**, que l'on reconnaît graphiquement par les « majuscules »  ,  ,  ,  .

267-§ Le dernier point que nous avons abordé est perturbant pour l 'analyste qui se confronte non seulement à son propre raisonnement mais aussi à la logique de chacun des transcripteurs. Cette lettre **[Z]** peut ou peut ne pas être considérée

---

187 Notre démarche est inversée à celle de CURRIER qui recherchait les cas fréquents plutôt que les cas isolés : ceci n'est pas une critique mais une façon complémentaire de procéder.

188 Signe entre la croix et la bavure (tache).

189 Fait partie d'un digramme qui dans le manuscrit prend la forme d'une lettre « majuscule ».

190 Cette lettre Λ est confondue avec la lettre 𝔞.

191 Si l'on devait faire une analogie entre le Constat 29 et un cas que nous connaissons dans la langue française, nous dirions que **[J],** Λ et **[X]** sont des symboles ni numériques ni alphabétiques mais séparateurs de mots comme le « trait d'union » qui ne commence ni ne finit jamais un mot. **[J],** Λ, et **[X]** ont une position de pivot qui partage le mot en deux parties.

192 Le codage des alphabets est variables suivant l'analyste qui a discrètisé (Page 103). Les multiples versions de transcriptions monographiques conjuguées à une transcription bigraphique sont des freins à notre étude car nous nous demandons à chaque fois de quel alphabet il s'agit et si la lettre que nous étudions est ou n'est pas couplée avec une autre lettre.

comme indépendante ; nous imaginons en effet la possibilité que  , , , , soient des assemblages de monogrammes. Outres les problèmes de hiérarchisation[193] il demeure la difficulté d'analyser un texte panaché de monogrammes et de digrammes : lorsqu'il s'agit d'un cryptogramme le cas est naturel mais il ne l'est pas quand la complexité du cryptogramme est accentuée par une faute de méthode de transcription.

268-§ La transcription de CURRIER montre deux cas particulièrement intéressants. En premier lieu les mots ne commencent jamais par la lettre **[z]** —logique puisqu'elle est couplée— ni par la lettre **[q]**[194] et ni par la lettre **[M]**. De même, les lettres **[5]**, **[q]**, **[x]** ne clôturent jamais un mot du manuscrit, précisons cela :

- La lettre **[q]** est un ornement graphique sans fonctionnalité apparente si ce n'est de lier deux parties d'un mot ou de créer un pont entre-deux mots[195]. En tous cas la liaison se fait entre les parties internes des mots. Toutefois d'autres symboles sont reliés de la même sorte mais ils ne sont pas codifiés par cette lettre **[q]**.

- La lettre **[M]** a pour habitude de ne jamais ouvrir un mot ou une phrase par contre elle se réserve le droit de les fermer quasiment systématiquement lorsqu'elle y figure. Sa probabilité ou sa capacité à terminer « mots et phrases » est de 0,945. Cette probabilité de transition sur un espace est édifiante.

> **Constat 30 La lettre [M] appelle presque systématiquement la fin d'un mot, d'une phrase ou d'un paragraphe.**

269-§ A présent, nous continuons d'étudier les transitions d'états mais avec des groupes de trois lettres.

Transition trigrammique

270-§ L'étude trigraphique du manuscrit doit mettre en évidence les cas particuliers qu'on doit considérer comme des traits caractéristiques supposés être significatifs d'une construction linguistique particulière.

---

193 admet les codes DZ et ZD, admet FZ et ZF, admet HZ et ZH, admet PZ et ZP.

194 Signe particulier qui ne possède pas de fonte graphique.

195 Folio 56r1, « très jolie calligraphie » entre les deux premiers mots de la première ligne (voir aussi le folio 100r1, première ligne et sixième mot) et le phénomène se reproduit dans le folio 99v à la ligne 8 mais il n'est pas signalé dans la transcription.

271-§ Nous pratiquons deux axes de recherche. Nous recherchons les trigrammes uniques[196] ainsi que ceux qui ne constituent ni le début et ni la fin d'un mot. Nous considérons les deux aspects des symboles « majuscules » de composition digrammique.

272-§ PREMIER ASPECT FRIEDMAN. Nous découvrons vingt-trois trigrammes[197] qui sont placés systématiquement dans un mot sans qu'ils en constituent le début ni même la terminaison. Parmi ceux-ci nous révélons deux groupes : le premier groupe[198] contient huit trigrammes dont la première lettre est **[C]** ; le deuxième groupe[199] est dominé par huit trigrammes qui commencent par la lettre **[Z]**.

273-§ Nous ne répondons pas encore à la question : pourquoi autant de ces trigrammes commencent par une même lettre **[Z]** ou **[C]** ? Mais nous remarquons qu'elles n'occupent pas la même place dans les mots : le **[Z]** est six fois à la seconde place[200] des mots et deux fois à la troisième place ; de même, le **[C]** est présent une seule fois à la deuxième position, quatre fois à la troisième place, trois fois à la quatrième place[201] et deux fois à la cinquième place.

Constat 31 Les trigrammes internes aux mots sont rares et commencent fréquemment par la lettre [C] ou [Z].

Constat 32 Les lettres [C] et [Z] ne sont pas placées identiquement dans les mots : le [Z] intervient dès la deuxième place tandis que le [C] intervient particulièrement à partir de la troisième place.

274-§ Le Constat 32 nous indique que la diversité ne se fait pas en deuxième position du mot et que la redondance se place essentiellement en troisième et quatrième position

196 Leurs probabilités de transition trigrammique sont égales à un.

197 Cf. Annexe, page 403.

198 C9A, CG4, CGS, CGT, CIC, CII, CKC, CMA

199 Z2H, ZAA, ZAT, ZCI, ZCS, ZFZ, ZG4, ZGS.

200 Trigrammes de la version FRIEDMAN avec les symboles composés comprenant la lettre Z.

Trigramme	C9A	CG4	CGS	CGT	CIC	CII	CKC	CMA
Position	3	2	5	4, 3	3	3, 5	4	4

Trigramme	Z2H	ZAA	ZAT	ZCI	ZCS	ZFZ	ZG4	ZGS
Position	2	2	2	3	2	3	2	2

201 Le total fait neuf trigrammes car il existe deux trigrammes identiques ce qui implique une diversité de huit trigrammes.

des mots.

275-§ DEUXIÈME ASPECT FRIEDMAN. Ce second angle de vue métamorphose les couples de lettres DZ, FZ, HZ, PZ, en uniques lettres  , , et . La condensation de ces symboles implique une modification des mots dans leurs compositions et leurs dimensions. Les trigrammes ne sont plus répartis dans deux principaux groupes ; un seul groupe[202] réunit quatorze trigrammes[203] commençant par la lettre **[C]** : les triplets de première lettre **[Z]** ont disparu.

276-§ PREMIER ASPECT CURRIER. Cette version fournit trois groupes[204] de trigrammes. Le premier groupe[205] se compose de quatre trigrammes commençant par la lettre **[R]**. Le deuxième groupe[206] est un peu plus diversifié et chaque triplet débute par la lettre **[Z]**. Finalement, le troisième groupe[207] —encore un peu plus diversifié— s'initie avec la lettre **[I]**.

Constat 33 En complément du Constat 32, les lettres [I] et [R] participent à la césure des mots.

---

[202] Trigrammes de la version FRIEDMAN avec les symboles composés réduits à un code.

Trigramme	C9A	CG4	CGS	CGT	CIC	CII	CKC	CMA	CWC	CWT	CXC	CXS	CXT	CZ8
Position×Nombre	3	2	5	3, 4	3	3, 5	4	4	2×4	2	2×21, 3×6, 4, 6	2	3	3, 4

Les trigrammes internes aux mots se placent aux positions 2, 3, 4, 5, 6 avec une prédominance de la position 2 (29 fois) puis 11 fois à la position 3 ; 5 fois à la position 4 ; 2 fois à la cinquième position et une seule fois à la position 6 du mot.

[203] Nombre de trigrammes diversifiés.

[204] Trigrammes avec symboles composés de Z.

Trigramme	R2I	R5S	RCI	RPC
Position	5	3	8	4

Trigramme	Z8T	ZAT	ZCI	ZGT	ZOA
Position×Nombre	3	2	2	2	2×7

Trigramme	IKH	ILC	ILD	ILO	ILT	IOA
Position×Nombre	3	2	3×3, 4×5	3, 6	5	4

[205] R2I R5S RCI RPC

[206] Z8T ZAT ZCI ZGT ZOA

[207] IKH ILC ILD ILO ILT IOA

277-§ DEUXIÈME ASPECT CURRIER. Dans ce cas le groupe des trigrammes débutant par la lettre **[Z]** est inéxistant mais ici il n'y a pas d'augmentation « compensatrice » des deux autres groupes de trigrammes[208].

Conclusion 6 Les positions 2, 3 et 4 des vocables sont des positions d'équilibres dépendantes des symboles [C] , [I] , [R].

278-§ Le Constat 31 conforte l'idée de TILTMAN, selon le Constat 12, la deuxième partie du code de Cave BECK commence avec la lettre « s » ou « t », et, il est extrêmement étrange que nous détections des groupes principaux —qui vont deux à deux— dont leurs premières lettres sont **[Z]**, **[C]** , **[I]** , **[R]**.

Pouvons-nous conclure que « s » et « t » soient parmi nos quatre lettres ? Certes non, mais nous devons référencer ce constat:

Constat 34 Le Constat 12 et le Constat 31 coïncident.

279-§ Si l'on associe la Conclusion 6 au Constat 34 alors nous avons de fortes présomptions que le manuscrit soit familier à un système de langue parfaite.

280-§ Pour conclure l'étude des lettres du manuscrit nous allons explorer une deuxième façon de faire qui repose sur la théorie de l'information. Ce dernier chapitre sera un angle supplémentaire de vision sur le comportement des lettres du manuscrit.

Mesures de la désorganisation des lettres

281-§ Nous utilisons la *théorie de SHANNON* pour évaluer le niveau de désorganisation des lettres du manuscrit par rapport à un tirage équiprobable.

282-§ Cette théorie de l'information introduite en 1949 par Claude SHANNON est incontournable en cryptographie [SEBE1989]. En fait,

tous les systèmes modernes de communications s'appuient sur cette théorie,

[208] Trigrammes de la version CURRIER avec les symboles composés réduits à une seule lettre.

Trigramme	IKH	ILC	ILD	ILO	ILT	IOA
Position×Nombre	3	5	3×2, 4×6	3, 6	5	4

Trigramme	R2I	R5S	RCI	RPC
Position×Nombre	5	2	8	4

cependant cette méthode ne s'applique pas à tous les cas de la cryptanalyse ; le terme « moderne » s'accommodant mal avec l'âge de notre manuscrit. Toutefois, cette théorie repose sur un principe fort qui consiste à dissocier une information en deux composantes principales. La première est celle qui quantifie et mesure sans considérer le contenu de l'information. La deuxième composante est la signification de l'information transmise.

283-§ Dans son aspect « quantifiable », selon SHANNON, le minimum à apprendre d'un événement est sa survenue. Dans la théorie de l'information, on ne tient pas compte de la signification de la donnée survenue, on dit que:

> *l'information apportée par un événement est d'autant plus grande que sa probabilité de survenue est faible ;*

ce qui signifie que la seule valeur significative d'une donnée est sa probabilité d'apparition et que dans un système Emetteur—Récepteur, la rareté de la survenue caractérise la distribution informationnelle [CASA1994].

284-§ La richesse informationnelle apportée par une probabilité faible s'explique aussi par la notion de codification des données. Ainsi, dans une transmission, avec ou sans compression, les données se voient attribuer un code ; selon la présence statistique des données il convient d'attribuer des codes de petites tailles pour les cas de fortes redondances et au contraire de codifier les cas rares par des codes de tailles plus importantes [SHAN1949b]. C'est précisément le cas en télégraphie

> *..en télégraphie, le symbole le plus court, un point, a été choisi pour la lettre anglaise la plus fréquente, 'e', tandis que les lettres peu fréquentes sont représentées par des séquences plus longues de points et de traits.*

285-§ Aussi, dans le cadre d'une transmission, on se pose la question, à savoir:

> *Quelle est la quantité d'information contenue dans le message à transmettre ?*

286-§ SHANNON exprime les variations entre probabilités par la somme de logarithmes, des probabilités individuelles, pondérés par les mêmes probabilités ; la formule[209] est la suivante:

[209] La relation entre bases est $\log b(a) \times \log a(b) = 1$.

$$H(A) = -\sum_{i=1}^{i=n} p_i \times log(p_i)$$

Equation 6 Entropie, formule de SHANNON.

ce qui signifie qu'une probabilité non égale à un demi, dans un système binaire, est inférieure à la moyenne dont l'effectif est de deux. Ceci revient à évaluer les probabilités événementielles par rapport à la moyenne. Ce procédé ne prend pas en compte l'ordre[210] des éléments dans la séquence,

> *elle ne caractérise qu'un groupe de symboles statistiquement homogène [ATLA1992]. On dit que l'émission de suites de symboles par la source doit constituer un processus stochastique stationnaire et ergotique [KINC1957].*

287-§ En fait, l'entropie[211] $H(\ )$ est en général considérée comme exprimant l'état de désordre d'un système physique. D'une façon plus précise, on peut dire que l'entropie mesure le manque d'information sur la véritable structure du système [ATLA1992].

Densité diacritique

288-§ En cryptanalyse, nous l'appliquons pour comparer les densités diacritiques des langues. Si nous étudions la fréquence des espacements dans la langue anglaise et la langue française nous remarquons que $H_{anglais}$ et $H_{français}$ sont différents[212] : la densité diacritique de la langue anglaise est de 4,0755 et celle de la langue française est de 3,9568 ce qui montre que le français est plus disparate[213] que l'anglais. La fonction H() de SHANNON ne se limite pas à la simple étude monogrammique d'une distribution de lettres. Elle permet de calculer aussi la densité diacritique d'une langue d'après les digrammes qui la composent, nous parlons alors de *h2* qui est d'après les transitions

---

[210] Toutefois l'application de l'Equation 6 sur des probabilités de transitions Markoviennes ouvre la voie d'une considération de l'ordre des éléments étudiés.

[211] L'information est une quantité abstraite mesurable dont la valeur ne dépend pas de ce sur quoi porte l'information : sa valeur H() dépend des probabilités associées avec ces formes de réalisation mais en aucune façon de leurs causes ou de leurs conséquences ; indépendance des événements, la probabilité d'une catégorie est déterminée si celles de toutes les autres le sont ; H() est continue, car une petite variation de p(i) entraîne une petite variation de $-p_i \times \log_2(p_i)$; elle est additive, si deux messages sont indépendants alors $H(x,y) = H(x) + H(y)$.

[212] H() étant la somme des probabilités des lettres de la langue écrite plus le caractère espacé multipliées par le logarithme inverse de la probabilité.

[213] Disparate : manque d'égalité entre les probabilités.

Markoviennes :

$$h_{2(\,Message)} = \sum_{i=1}^{i=Dim\ \mathrm{Alphabet}} \frac{p(lettre_{i+1}, lettre_i)}{p(lettre_i)} \times \log_2 \frac{p(lettre_i)}{p(lettre_{i+1}, lettre_i)}.$$

289-§ Si nous nous intéressons à la densité diacritique des n-grammes d'un texte alors la fonction sera h_n. En cryptanalyse, les fonctions *h()* de SHANNON sont utilisées pour comparer les cryptogrammes avec des textes référencés. Si un texte crypté inconnu a des densités diacritiques *h1*, *h2*, ..., h_x et qu'un texte crypté par une méthode connue possède les mêmes caractéristiques de densité alors il est fort probable que le texte inconnu soit crypté selon la même méthode que le texte servant de référence.

Entropie embarrassante

290-§ William Ralph BENNET fut le premier à appliquer le concept d'entropie à l'étude du manuscrit de Voynich. Dans *Scientific and Engineering Problem Solving with the Computer*, paru en 1976, BENNET nous indique, que le langage Polynésien possède une entropie de second ordre de même nature, bien que l'entropie *h2* de MS408 soit tout de même plus élevée [BENN1976].

> **Toutefois, la comparaison ne peut aller plus loin puisque nous nous heurtons au fait que la Polynésie Française et Anglo-saxonne ne furent découvertes que tardivement[214] à la fin du dix-huitième siècle. De ce fait, la corrélation entre ces deux langages n'est que théorique.**

291-§ Les entropies du second ordre sont parmi les caractéristiques les plus embarrassantes. La différence entre les entropies du premier et second ordre, *h1-h2*, est identique à la différence entre les entropies absolues du premier et second ordre, *H1-H2*. Selon Dennis J. STALLINGS [STAL1998],

[214] James COOK découvre Hawaii en 1778.

Hypothèse 18 Le comportement de *h2* montre qu'il est peu probable qu'il s'agisse d'un langage naturel et que seul un système verbeux[215] (prolixe), ou plusieurs caractères cryptés codent pour un seul caractère clair, pourrait expliquer la redondance décrite par *h2*.

292-§ La dimension du cryptogramme est très supérieure au message dissimulé dans le cas d'un chiffrement avec verbosité.

Les proportions sont comparables à celles obtenues dans l'*Ave Maria* du célèbre Abbé TRITHÈME.

293-§ La particularité d'un système verbeux est de produire des mots de grandes dimensions. L 'étude sur la diversité et la fréquence des vocables montre en fait le phénomène inverse.

La répétition, bien que *h2* énonce l'impossibilité d'un langage naturel, ne peut-elle être un phénomène naturel ?

294-§ De nombreux textes montrent que la répétition peut être démonstratrice d'un genre littéraire particulier comme ces deux textes[216] allemands et latins.

Allemand (ancien)

eiris sazun idisi
suma hapt heptidun

5

suma clubodun
insprinc haptbandun
phol ende uuodan
du uuart demo balderes uolon
thu biguol en sinthgunt

[215] A titre d'exemple on considère les vingt-six lettres d'un alphabet et à chacune de ses lettres on associe le numéro de son rang ; la lettre *Z* est codée par le code *26* et la lettre *A* est codée par le code *1*. Le groupe de mots, *« MANUSCRIT DE VOYNICH »,* se trouve codé par la séquence, *13.1.14.21.19.3.18.9.20. 4.5. 22.15.25.14.9.3.8.* Il est intéressant de constater que si l'on désire que les codes soient parfaitement distincts alors il faut préciser que les nombres inférieurs à *10* doivent être précédés d'un code particulier comme le chiffre *0* que nous avons déjà présenté comme un symbole de Voynich hypothétiquement nul. La séquence devient *130114211903180920 0405 22152514090308*, et on constate que le chiffre *0* occupe *9/36* du groupe de mots —soit 25%. Cependant la conséquence évidente est un doublement de la dimension des mots : « phénomène que nous ne constatons pas dans le manuscrit ».

[216] Le premier texte est une incantation magique écrite en ancien allemand et le second texte est écrit en latin.

thu biguol en friia
thu biguol en uuodan
sose benrenki
sose lidirenki
ben zi bena
lid zi geliden
sazun her duoder
suma heri lezidun
umbi cuoniouuidi
inuar uigandun
uuorun zi holza
sin uuoz birenkit
sunna era suister
uolla era suister
so he uuola conda
sose bluotrenki
bluot zi bluoda
sose gelimida sin

Latin

Gaudeamus Igitur
Gaudeamus igitur,
Iuvenes dum sumus;
Post iucundam iuventutem,
Post molestam senectutem
Nos habebit humus,
Nos habebit humus.
Ubi sunt, qui ante nos
In mundo fuere?
Vadite ad superos,
Transite ad inferos,
Ubi iam fuere,
Ubi iam fuere.
Vita nostra brevis est,
Brevi finietur;
Venit mors velociter,
Rapit nos atrociter;
Nemini parcetur,
Nemini parcetur.
Vivat academia,
Vivant professores,
Vivat membrum quod libet,
Vivant membra quae libet;
Semper sint in flore,
Semper sint in flore.
Vivat et respublica
Et qui illam regit,
Vivat nostra civitas,
Maecenatum caritas,
Quae nos hic protegit.
Vivat omnes virgines,
Faciles, formosae,
Vivant et mulieres,
Tenerae, amabiles,
Bonae, laboriosae.
Pereat tristitia,
Pereant osores,
Pereat diabolus
Quivis antiburschius,
Atque irrisores.

295-§ Tous deux contribuent à nous faire penser que la répétition peut être en fait non pas le résultat d'un procédé d'encryptage mais simplement la résultante d'une structure particulière d'énonciation.

Il est remarquable que la diversité des genres littéraires est d'une telle profusion que plus nous recherchons une référence textuelle et plus nous en découvrons d'autres.

296-§ Nous recherchons ce point de référence, sur lequel nous puissions faire basculer l'énigme du manuscrit vers sa ou ses solutions, ce point d'appui qu'Archimède demanda pour soulever la terre. Nous sommes toujours en quête de ce point de référence. Dans cette démarche, Dennis STALLINGS réunit des portions de textes issus de l'époque médiévale et il calcule leurs entropies.

Texte[217]	*h1*	*h2*	*h1-h2*
Book of Mormon - 1 Nephi	4.033	3.090	0.942
Book of Mormon - Alma	4.041	3.109	0.931
Book of Mormon - Ether	4.009	3.029	0.980
King James Bible - Genesis	3.969	3.020	0.949
King James Bible -Joshua	4.012	3.029	0.983
King James Bible -Acts	4.041	3.137	0.904
Francis BACON's Essays, Part 1	4.048	3.220	0.827
Francis BACON's Essays, Part 2	4.042	3.214	0.828
Francis BACON's Essays, Part 3	4.066	3.229	0.837

Tableau 3 Entropies *h1*, *h2* et *h1-h2*, Source EVMT (Dennis J. STALLINGS)[218].

En fait, remarque-t-il, l'entropie *h1-h2* demeure toujours inférieure de moitié à celle du manuscrit. Comment expliquer cette « embarrassante » caractéristique *h2* ?

Type of VOYNICH Text	Transcription Alphabet	# ch.	File Size	h0	*h1*	*h2*	*h1-h2*
Herbal-A	CURRIER	33	9804	5.044	3.792	2.313	1.479
Herbal-A	FSG	24	10074	4.585	3.801	2.286	1.515
Herbal-A	EVA	21	12218	4.392	3.802	1.990	1.812
Herbal-A	Frogguy	21	13479	4.392	3.826	1.882	1.945
Herbal-B	CURRIER	34	13858	5.087	3.796	2.267	1.529
Herbal-B	FSG	24	14203	4.585	3.804	2.244	1.560
Herbal-B	EVA	21	16061	4.392	3.859	2.081	1.778
Herbal-B	Frogguy	21	17909	4.392	3.846	1.949	1.897

Tableau 4 Entropies *h1*, *h2* et *h1-h2* du manuscrit de Voynich, Source EVMT (Dennis J. STALLINGS).

297-§ Gabriel LANDINI apporte un début de réponse. Il étudie la nouvelle classique *Les contes de Genji* qu'il adapte en deux types de notations : *Romaji*[219] et *Kana*[220], afin que son programme informatique MONKEY[221] puisse calculer les différents ordres de l'entropie. Il observe que le japonais écrit en Kana a une entropie *h2* supérieure à celle du japonais écrit en Romaji. *Les contes de Genji* écrit en Kana apparaissent très proches du manuscrit de Voynich si nous nous réfèrons à l'unique soustraction *h1-h2*. Cependant, une soustraction exprime une variation dépendante de la grandeur de *h1* et *h2* mais uniquement relative à l'écart qui sépare *h1* de *h2*. En fait, les valeurs *h0*, *h1* et *h2* du Kana, sont bien différentes des valeurs *h0*, *h1* et *h2* du manuscrit de Voynich. Par contre, le japonais Romaji est opposé au japonais Kana. Les deux premières valeurs de l'entropie sont voisines de celles du manuscrit mais la troisième et dernière

[217] Alphabet de vingt-sept lettres

[218] Compte-rendu du 27 avril 1998.

[219] Notation des phonèmes avec les lettres latines.

[220] Notation des syllabes.

[221] Premier programme informatique adapté au manuscrit pour l'étude des entropies.

valeur est plus élevée.

Conclusion 7 Les différences, entre le Kana et le Romaji, sont que la notation syllabique est génératrice de redondances trop inégales, tandis que, la notation phonémique est moins disparate.

298-§ Il en découle une hypothèse qui énonce que

Hypothèse 19 Ces écritures cryptées sont des notations phonétiques.

299-§ Le dernier outil usuel est *l'unicity distance*. Elle dit combien de lettres doivent être découvertes pour « casser le code » par une analyse des fréquences. Sa formulation[222] fait intervenir le logarithme des permutations de lettres de l'alphabet[223] et la différence *D*, appelée redondance[224], entre le logarithme $log_2(Dimension\ alphabet)$ et l'entropie estimée[225] du langage.

$$N = \frac{h(k)}{D} = \frac{h(k)}{R - r} = \frac{h(k)}{\log_2(\text{Dimension Alphabet}) - \sum_{i=1}^{i=\text{Dimension Alphabet}} p_i \times \log_2\left(\frac{1}{p_i}\right)}$$

300-§ **Seulement, nous comprenons aussi que si *D* est inconnue alors *N* est indéterminable.**

301-§ Nous tirons l'enseignement que la connaissance *a priori* de la langue est indispensable pour pratiquer ces calculs. Or, bien qu'il soit vrai, que dans la cryptologie militaire il

---

[222] Cette formule permet d'évaluer la sécurité d'une méthode d'encryptage. Quand N est petit cela signifie qu'un nombre minimal N de lettres est suffisant pour décrypter le message. Mais lorsque N est grand alors il est nécessaire de découvrir un grand nombre de lettres pour obtenir le texte clair. Par exemple, fait remarquer Jennifer SEBERRY à la page 66 de son livre [SEBE1989], une substitution par alphabet de n lettres donne $n!$ permutations possibles. Et si la langue probable de rédaction est l'anglais alors, $N = \frac{h(k)}{D} = \frac{log26!}{D}$, comme D de l'anglais est 3,2 : alors N devient $N = \frac{log26!}{3,2} = 27,6$; il est nécessaire de rendre clair vingt-sept à vingt-huit lettres pour être sûr de décrypter le message. Tandis que pour une opération de chiffrement par arithmétique modulaire seulement $N = \frac{log26}{3,2} = 1,5$ lettre soit entre une et deux lettres sont suffisantes.

[223] Si l'alphabet est désordonné alors $h(k)=log_2(n!)$, si l'alphabet est décalé alors $h(k)=log_2(n)$.

[224] En anglais « Redoundance ».

[225] En anglais « Rate of language ».

soit courant que le cryptanalyste sache d'où provient le message, qu'il connaisse aussi la méthode d'encryptage employée et la nature des informations transmises, souligne Wayne G. BARKER :

> *il doit être compris que, dans le monde réel de la cryptanalyse, il est rare que le cryptanalyste approche la solution d'un système d'encryptage complètement en "aveugle" et que le cryptanalyste aura généralement une bonne idée de qui utilise le système [BARK1995],*

il faut se rendre compte que dans le cas d'un problème avec minimum d'information ces outils deviennent inefficaces.

302-§ Pour autant, le groupe de cryptanalystes de l'European VOYNICH Manuscript Translation Project EVMT [LAND1997] conclut que

> **Conclusion 8 La fonction h() révèle que le manuscrit de Voynich ne peut pas être issu d'une monosubstitution alphabétique de langue Indo-européenne avec ou sans transposition.**

303-§ Ce résultat n'excluant pas le fait que cette monosubstitution soit à groupes codiques ou phonétiques, ou bien qu'il y ait alternance des procédés d'encryptage. Donc, toutes les hypothèses demeurent possibles. Rappelons-nous que l'outil fournit un résultat qui n'est pas une méthode. L'outil est simplement une unité qui ne prend sens que si elle est incluse dans un système constructif. Les outils de la théorie de l'information, selon SHANNON, ne sont pas particulièrement efficaces en cryptanalyse non militaire. Elle nécessite, en effet, trop d'*a priori* sur la nature et le contexte rédactionnel du cryptogramme.

C'est un fait : la distance qui sépare tout texte crypté de son message clair est représentative de la difficulté que nous avons à lire le texte crypté en temps réel ; mais comment mesurer une distance entre deux entités dont l'une est inconnue et l'autre hypothétique.

304-§ La monosubstitution de CÉSAR ne distancie pas le texte monosubstitué de son « clair ». Ils sont tous deux identiques dans l'ordonnancement des séquences de phrases, de mots et de lettres. L'*unicity distance* de SHANNON exprime la difficulté de l'analyse qui croît en fonction de *h(k)* et dépend directement des arrangements possibles des éléments —des mots, des lettres, des entités— de départ. Notre difficulté à lire cette monosubstitution de CÉSAR tient du fait unique que le système de représentation est décalé. Ce qui apparaît n'est pas ce qui est. Nous retrouvons ce décalage [KAHN1980] dans les *Saintes Ecritures*[226] où la forme *Sheshak* remplace le

[226] Ancien Testament, livre de Jérémie, Chapitre 25, verset 26 :

nom de *Babel*[227]. La substitution s'effectue symétriquement[228] par rapport à l'alphabet hébraïque. La première lettre de cet alphabet est substituée par sa dernière lettre, puis la deuxième est substituée par l'avant dernière. Il est fait de même pour les autres lettres. Ainsi, si nous appliquons ce principe au vocable BABEL, sous sa forme sémitique BBL alors , le B est remplacé par la lettre *Shin,* notée SH, et le L est substitué par la lettre *Kaph,* notée K, « *Babel* est donc *Sheshak* ».

305-§ Bien que la substitution symétrique soit remarquable, il n'en est pas moins vrai que la substitution du vocable BABEL par SHESHAK, soit une source d'interrogations ; non pas sur la méthode algébrique pour obtenir SHESHAK mais sur la signification de cette opération.

306-§ C'est pourquoi, il est nécessaire de situer la théorie de SHANNON dans son contexte de deuxième moitié de vingtième siècle ou le tout calcul algébrique a imprégné l 'ensemble des méthodes cryptographiques[229] de ces cinquante dernières années.

Tous les rois du nord, proches et lointains, chacun à son tour, et tous les royaumes de la terre, qui sont sur la surface du sol ; et le roi de Shéshak boira après eux.

et Chapitre 51, verset 41 :

Comment ! Shéshak est prise, elle est conquise la splendeur de toute la terre ! comment ! Babylone est devenue un lieu désolé, parmi les nations !

[227] Babylone.

[228] Le principe de substitution est appelé *Athash*. Ce mot est le diminutif de quatre lettres de l'alphabet hébreux : *Aleph, Tan, Beth, Shin.*

[229] L'essor des calculateurs a imposé un système de formalisation algorithmique des procédés cryptographiques. L'utilisation de procédés algébriques est donc logique pour leur analyse.

Seulement, le manuscrit que nous sommes en train d 'étudier est d'une autre époque. Il vient d'un temps[230] où la méthode scientifique se construisait.

307-§ Pour autant, les mesures statistiques, probabilistes et entropiques, nous ont permis d'appréhender de nouvelles connaissances sur les structures n-grammiques et sur la nature « probable » du manuscrit. Maintenant, nous allons étudier les mots du manuscrit dans leur diversité, leurs fréquences et leurs capacités à contenir les preuves de leur propre encryptage grâce, entre autres, aux méthodes de KASISKI, KERCKHOFFS et FRIEDMAN; puis nous placerons nos découvertes par rapport à la langue synthétique de LULLE et de KIRCHER afin d'estimer si l'intuition de TILTMAN (Hypothèse 9 & Constat 13) est juste.

[230] La datation du manuscrit est établie entre le treizième et le seizième siècle.

•

> *Dieu, ayant fait l'homme pour être une créature sociable, lui a non seulement inspiré le désir et l'a mis dans la nécessité de vivre avec ceux de son espèce, mais lui a donné aussi la faculté de parler, qui devait être le grand instrument et le lieu commun de cette société. C'est de cela que viennent les mots, qui servent à représenter, et même à expliquer les idées [LEIB1690].*

LES MOTS que nous trouvons dans le manuscrit de Voynich doivent nécessairement être sensés pour ceux à qui ils s'adressent. L'individu qui partage cette culture est placé dans une communication symétrique [RUES&BATE1988] par rapport au langage du manuscrit ; état dans lequel nous ne sommes pas. Cependant, les mots sont opérables comme n'importe quelle séquence de lettres et en vertu de cela nous tirons des enseignements quant à leur diversité et quant à leurs façons de se répéter.

Diversités et fréquences des mots du manuscrit

308-§ La redondance et la diversité des vocables sont relatives à la pratique d'un langage. La diversité décrit la pluralité de notre monde et la redondance rassure notre mémoire que ce que nous observons avec habitude est nommé pareillement.

Explications empiriques

309-§ Peu de choses se disent quand le nombre de vocables est petit, et inversement, un nombre infini de vocables ne peut être atteint par la connaissance puisque nous sommes nous-mêmes limités.

> *Quoiqu'il n'existe que des choses particulières, la plus grande partie des mots ne laisse point d'être des termes généraux, parce qu'il est impossible que chaque chose particulière puisse avoir un nom particulier et distinct, outre qu'il faudrait une mémoire prodigieuse pour cela [LEIB1690].*

310-§ Aussi entre ces deux extrêmes se situe l'adéquation que nous faisons entre la nécessité de connaître suffisamment de vocables pour nous exprimer et l'effort que nous devons produire pour rechercher les termes adéquats à une communication symétrique.

311-§ La première mesure de cette attitude fut introduite par George Kingsley ZIPF et elle repose sur un constat empirique et non théorique. Elle constitue une estimation de l'utilisation d'un vocabulaire et fut affinée par Benoît MANDELBROT qui considéra

nécessaire l'introduction, dans cette équation, du facteur individuel.

312-§ Cette tendance, décelée par Kingsley ZIPF, montre en pratique que le numéro de rang par ordre d'utilisation des vocables est fonction de la fréquence d'utilisation de ces vocables. Cette loi dit que nous aurons plus de facilité à nous exprimer avec des mots courants qu'avec des mots rarement usités. Ce dernier point est essentiel en cryptanalyse puisqu'il induit qu'il est plus probable que certains vocables apparaissent tandis que d'autres seront absents du discours.

313-§ Force est de constater que chaque individu est issu d'un environnement particulier. L'appartenance à cet environnement —ou groupe social— pousse l'individu à réutiliser les pratiques de ce groupe afin de pouvoir communiquer, symétriquement dirait Jurgen RUESCH, avec l'ensemble des membres de son assemblée. Seulement chaque groupe se constitue parce qu'un centre d'intérêt est commun. Nous attendons d'un groupe un discours adéquat avec le sujet qui réunit ses membres. Les vocables les plus utilisés seront spécifiques à ce cadre de communication. Ainsi dans la communication militaire anglophone, il est souvent question de *« to commanding general »,* ou de, *« to signal officer », « stop », « query »*, ou bien de *« artillery »,* nous dit le cryptanalyste W. G. BARKER. Les mots sont alors représentatifs des groupes culturels.

> **Non seulement la langue implique l'utilisation de mots particuliers mais encore le groupe social montre ses signes distinctifs. Pourtant les distinctions ne sont pas toujours nettes et parfois il n'est pas évident de distinguer une langue d'une autre quand elles sont cryptées.**

314-§ La loi de ZIPF puise dans la constatation que l'emploi d'un mot dans un texte est inversement proportionnel à son rang. Le mot qui occupe la dixième place dans une liste ordonnée décroissante sera un centième de fois aussi fréquent que le mot le plus courant de cette liste [ZIPF1935].

$$\frac{i(r,k)}{k} = \frac{1}{10r} \quad \begin{cases} k \text{ est l'ensemble de tous les mots du discours.} \\ r \text{ est le rang dans le classement décroissant des fréquences.} \\ i \text{ est le nombre d'occurences d'un vocable.} \end{cases}$$

Equation 7 Première approximation de la loi de ZIPF.

315-§ Mais ce constat est empirique et ne s'applique pas à toutes les langues dit Benoît MANDELBROT, et qu'alors, il convient d'utiliser la loi dite de *ZIPF-MANDELBROT* [MAND1997].

316-§ George Kingsley ZIPF a rattaché sa loi au principe de moindre effort. L'être humain, selon ZIPF, choisit ses mots de telle façon qu'il puisse minimiser une certaine dépense en fonction du message qu'il doit émettre. L'homme est inscrit dans ses propres

limites physiologiques. Sa vitesse maximale[231] de parole, que nous pourrions évaluer en mots par heure, est déterminée physiquement par ses organes vocaux bien avant sa vitesse maximale[232] « cérébrale » de lecture [AFL1998]. PIERCE montre qu'il existe un lien qui associe un temps de parole (t) aux mots choisis dans la liste des mots les plus usuels pour l'orateur [PIER1966]. Il écrit cette relation par une expression mathématique simple : $p(r) = 2^{-ct_r}$. Ceci signifie, d'après cette expression, que plus les mots sont longs à parler t_r et moins ils sont utilisés $p(r)$. Toutefois, les travaux de MANDELBROT, HOWES et RIESZ montrent que la vitesse de lecture est limitée par le mot « reconnaissance » et non pas par le mot « émission » [PIER1966]. Pour une même signification un mot long peut tout aussi bien être plus utilisé qu'un mot court, c'est le cas du mot russe « poème » qui se dit plus fréquemment СТИХОТВОРЕНИЕ que СТИХ.

317-§ Au regard du quantitatif la fréquence relative des catégories grammaticales est stable bien que variant d'un individu à l'autre ou d'un texte à un autre texte. C'est ainsi qu'en français les mots outils (articles, pronoms, conjonctions, prépositions) représentent 50% de n'importe quel texte, l'autre moitié étant constituée par les mots pleins (substantifs, verbes, adjectifs, adverbes).

On peut noter que dans un dictionnaire cette proportion est tout autre, les mots outils ne représentant que 0,5% du lexique total.

Constat 35 Aussi, l'absence des mots outils dans un texte implique la réduction de moitié du nombre de ses mots.

318-§ Or ce fait doit nous interpeller car dans le cas d'un langage synthétique il y a une réelle réduction de la diversité des vocables et surtout il y a une réduction des mots outils.

Fréquences de mots

319-§ Le calcul de fréquence n'a pas d'autre utilité que d'autoriser l'analogie avec des événements déjà rencontrés[233]. Le calcul se rapporte aux vocables du texte et non aux

[231] De l'ordre de 10 000 mots par heure.

[232] Pouvant dépasser 50 000 mots par heure.

[233] Constitution de lexique suivant François TERS :

> *Choisir un certain nombre de textes variés d'au moins 2 000 mots chacun, pris dans toutes les branches du savoir (journaux, romans, théâtre, arts, sciences, etc.); en faire un relevé lexicologique complet en notant le nombre d'apparitions de chaque mot (vocable), c'est-à-dire sa fréquence; classer ensuite tout le vocabulaire recensé par ordre de fréquence décroissante, en tenant compte de la dispersion des mots (nombre de sources qui les contiennent). S'arrêter à une fréquence minimum, qui diffère selon l'importance du matériel dépouillé et le but utilitaire qu'on s'est fixé, c'est obtenir un vocabulaire de base ou vocabulaire fondamental» [TERS1968].*

mots du texte ; le *vocabulaire* est l'ensemble des vocables représentés un nombre quelconque de fois dans le texte considéré, le vocable étant lui une unité de lexique[234] et le mot est une unité de texte; on a lu un mot dans le texte, mais c'est un vocable qu'on trouvera dans le dictionnaire [MULL1968] ; la proportion de chacun constituera un indice de disparité, parmi ses congénères, par rapport à d'autres textes et reflète un contexte linguistique qui se trouve décrit par l'ensemble ou un sous-ensemble de lexique.

320-§ La *notion de répartition* [BEAU1986] montre alors que la présence des vocables n'est pas constante dans des textes différents et que d'une

> *façon générale, les listes de fréquence ne donnent guère les mots concrets.*

321-§ Il est nécessaire de distinguer[235] les mots fréquents des mots *disponibles* [TERS1968] qui sont usuels et utiles mais peu fréquents. En fait, nous utilisons plus de mots que nécessaire pour nous comprendre. La fréquence a pour rôle une meilleure mémorisation à long terme ceci expliquant la grande proportion de redondances et de mots «vides» que nous représentons par un simple graphique extrait des travaux de Pierre GUIRAUD.

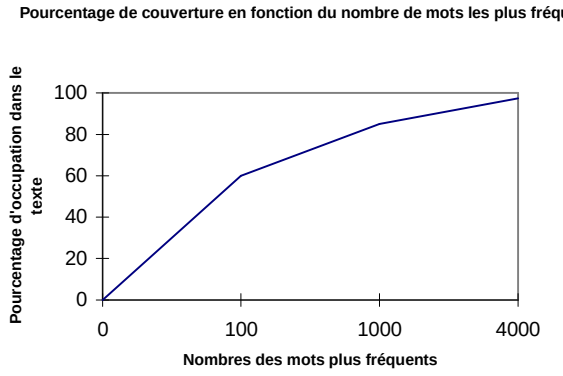


Tableau 5 Pourcentage de couverture d'un texte en fonction de la fréquence des mots.

234

> *Le vocabulaire s'oppose alors à lexique qui comprend les vocables que le locuteur utilise et ceux, virtuels, qu'il pourrait utiliser mais qu'il garde en mémoire [BEAU1986].*

235 La richesse sémantique d'un mot plein apporte plus de dynamique à la cryptanalyse d'un cryptogramme qu'un mot usuel même si celui-ci est très fréquent. Notre manuscrit revêt les deux : ses mots sont diversifiés et ils sont fréquents.

322-§ Il apparaît évident alors que la notion *statistique de fréquence* est à utiliser avec prudence. Le *mode statistique* d'une distribution ne révèle pas systématiquement le sujet discuté dans un texte. Les mots « vides » c'est-à-dire ceux qui ne changent pas l'intelligibilité du message occupent *« la moitié du nombre total des mots de tout texte... »* [GUIR1963] or un mot important[236] comme le vocable « CHEVRE » de « La chèvre de M. Seguin » peut ne pas faire parti des mots fréquents, nous rapporte Edmond BEAUME, bien que ce dernier soit des plus « important » pour cette histoire.

323-§ Nous comprenons ainsi pourquoi

> *Seul le vocabulaire disponible suscite un intérêt supérieur au vocabulaire de fréquence.*

324-§ Nous n'écartons pas *de facto* les éléments d'analyses mathématiques ; toutefois, nous nous limitons dans leur usage à la simple mise en évidence de caractéristiques simples souvent inductives. D'un autre coté, nous devons penser que la mathématique limite l'étude des cryptogrammes par le fait même qu'elle peut être à la source de fausses inductions et n'oublions pas que le calcul procède essentiellement d'une perte d'information [LEVY1987]. Ainsi, nous conservons en mémoire que la rareté d'un événement est riche en information et ceci n'est pas sans nous rappeler la théorie de Claude SHANNON qui montre que plus la probabilité d'un événement est faible et plus cet événement est porteur d'information [SHAN1949a].

325-§ Notre science se situe justement sur cette fragile position de l'interprétation du « quoi doit être utilisé » et de « quoi doit être abandonné » pour mener à bien une déduction qui aboutisse à un résultat satisfaisant. Un de ces pièges de la suffisance est montré par l'affaire DREYFUS (page 211). Ce qui est inutilisé par une science devient très utile pour une autre science, c'est précisément le cas de la *redondance* qui n'est pas utile en *« Théorie de l'information »* car elle la considère comme

> *un excédent relatif de signes par rapport au nombre minimal qui aurait été nécessaire pour envoyer la même quantité d'originalité...[MOLE1971].*

326-§ Pourtant, la redondance est indispensable dans notre communication naturelle et humaine car elle permet de

> *régler la quantité d'information transmise... Si le message est trop dense, il passe mal, la compréhension devient mauvaise [BEAU1986]*

---

[236] Sur ce point il doit être laissé une totale liberté de choix. Quel est le mot le plus important ? Pour Pierre GUIRAUD le vocable « chèvre » est le plus significatif de l'histoire de « La chèvre de M. Seguin ». Pourtant ce vocable pourrait être changé en un vocable d'être vivant aussi vulnérable face au loup. Le vocable « chèvre » de « La chèvre de M. Seguin » n'est donc pas important si l'on considère la morale de la fable.

327-§ c'est pourquoi Abraham MOLES écrit que

> *la redondance est en fait, un facteur essentiel de l'intelligibilité des textes; c'est pourquoi elle apparaît comme une grandeur aussi importante que l'information dans la communication interindividuelle.*

328-§ Nous devons ainsi trouver le chemin qui se situe entre ces deux tendances que sont la profusion et la rareté.

Récupération par la cryptanalyse

329-§ Un des aspects de la cryptologie est l'étude des fréquences des mots et des vocables. Le cryptologue recherche des caractéristiques[237] qui permettent d'orienter ses recherches. Dans la langue écrite nous utilisons des mots de dimension n-grammique plus souvent que d'autres[238]. Dans un texte de langue anglaise il est courant d'utiliser des mots de quatre lettres et très rare d'en utiliser de plus de quinze lettres. Le tableau de ci-dessous décrit ces variations d'utilisation en fonction de la dimension des mots de ce texte anglais.

Nombre de lettres par mot	nombre de mots	nombre de lettres	Nombre de lettres par mot	nombre de mots	nombre de lettres
x_i	f_i	$x_i \times f_i$	x_i	f_i	$x_i \times f_i$
1	390	390	10	288	2 880
2	1 028	2 056	11	163	1 793
3	1 369	4 107	12	86	1 032
4	**1 745**	6 980	13	25	325
5	1 457	**7 285**	14	23	322
6	1 169	**7 014**	15	4	60
7	1 039	**7 273**		10 000	51 708
8	735	5 880			
9	479	4 311			

Tableau 6 Dimensions des mots en fonction de leur présence [KULL1977].

330-§ L'étude des vocables nous renseigne sur la diversité des mots d'un texte. La première approximation de ZIPF entre dans ce cas de figure. Pourtant, pour PIERCE cette première « loi » est insuffisante pour distinguer et caractériser les langages.

---

[237] Régularité de la distribution des fréquences des mots ; dimensions des vocables les plus utilisés ; recherche des mots les plus grands et les plus petits ; études de la diversité des vocables.

[238] QALQASHANDI était un cryptanalyste arabe du quatorzième siècle, il faisait remarquer que les fréquences des lettres des messages écrits étaient souvent différentes de celles du Coran. Dans les années « trente », ZIPF montrait notre tendance à utiliser notre vocabulaire avec économie.

> *La loi de ZIPF donne des courbes qui indiquent que sa loi est très valable pour le gothique... passablement valable pour le yiddish... encore moins pour le norvégien et à nouveau moins pour le chinois.*

331-§ La loi peut s'appliquer pour certaines langues mais ne peut être généralisée à toutes bien qu'il ressorte globalement une indication commune qu'est le *principe de moindre effort*.

332-§ Dans le cadre de l'étude du manuscrit de Voynich, Gabriel LANDINI utilise les deux lois de ZIPF, dont la première et la plus connue[239] s'effectue par la méthode suivante :

> *Les signes d'un texte sont triés par leurs fréquences décroissantes et un numéro de rang est assigné à chacun d'eux. Pour les signes de même fréquence, leur arrangement est arbitraire.*

333-§ Le manuscrit est particulier[240]. Il contient des mots de fréquences inhabituelles[241] si nous les comparons avec les langues européennes comme le français, l'anglais (Tableau 6) et le latin. LANDINI compare les résultats de cette première approximation appliquée au manuscrit de Voynich[242] avec sept textes[243] de langue anglaise. Parmi ces textes seuls trois[244] ont un comportement « analogue » au manuscrit. Cette analogie montrerait que le manuscrit se présente sous une forme non cryptée ; pourtant, nous ne pouvons pas ignorer les différences de fréquences des mots et des vocables qui opposent radicalement ces trois textes au manuscrit de Voynich.

---

[239] La représentation graphique de cette première loi se fait en traçant les coordonnées des logarithmes des fréquences en fonction des rangs occupés par ces vocables. La loi est alors représentée approximativement par une droite inclinée à $-\pi/4$.

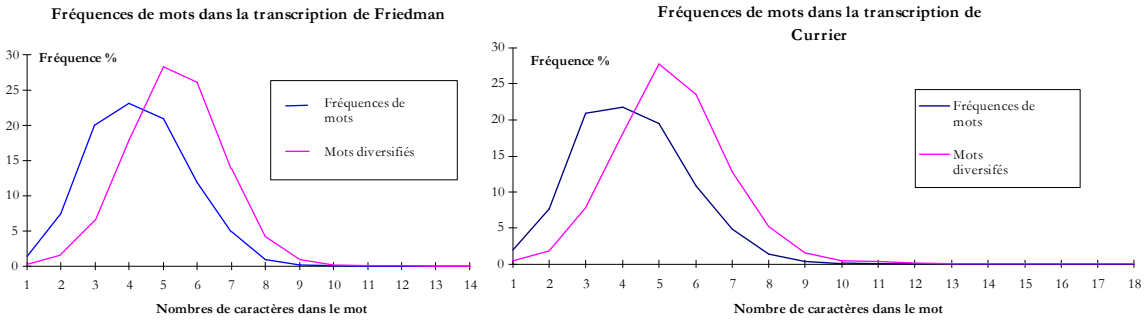
[240] Pour une langue particulière il existe une représentation graphique particulière de la loi de ZIPF. En comparant cette courbe avec celles obtenues à partir des cryptogrammes il doit être possible de constater des similitudes ou des incompatibilités.

[241] Près de sept fois supérieure à la distribution « normale » de la langue anglaise.

[242] Selon les quatre versions de transcription du manuscrit : Fsg.new, Voynich.now, Langage A et Langage B de CURRIER.

[243] *Alice in wonderland, Through the looking-glass, Emma, Frankeinstein, The Republic, Reason discourse, Roget's thesaurus.*

[244] *Alice in wonderland, Through the looking-glass, Reason discourse.*



334-§ Nous constatons que le manuscrit est constitué essentiellement par des mots de quatre lettres[245]. La transcription de CURRIER fournit deux mots[246] de grandes dimensions qui sont détachés des autres mots par l'absence de mots de quatorze et quinze lettres. Tandis que la transcription de FRIEDMAN donne une suite « homogène » de mots allant de une à treize lettres[247].

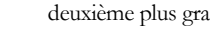
La deuxième loi de ZIPF que LANDINI utilise est appelée *« number-frequency »*.

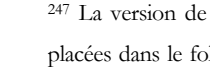
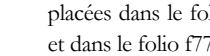
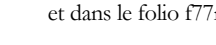
> *Cette règle montre la variation de la fréquence d'un vocable en fonction du nombre de vocables ayant la même fréquence.*
>
> **Constat 36 Il y a plus de vocables diversifiés dans les vocables très redondants que dans les vocables peu redondants.**

335-§ La diversification est donc liée à la redondance. Ces mots diversifiés ont alors une importance particulière proche de ce que nous appelons un « mot plein ». La relation de ce constat avec l'hypothèse de TILTMAN est apparente mais pas évidente. En effet, le deuxième fait remarquable concerne la diversité des vocables. Nous découvrons une proportion double de vocables de cinq lettres. Habituellement, nous nous attendons à ce que les vocables les plus présents aient une dimension minimale[248] de six lettres.

---

[245] Par habitudes nous nous attendons plutôt à ce que les mots de deux ou trois lettres soient les plus fréquents : à titre d'exemple, nous citons les mots: *who, an, to, be*, en anglais, et, *le, la, une, est,* en français.

[246] Le plus grand vocable  est composé de dix-huit lettres et on le trouve au folio f6v1. Le deuxième plus grand vocable  est composé de seize lettres et on le trouve au folio f41r10.

[247] La version de FRIEDMAN contient les plus grands mots suivants :  —treize lettres placées dans le folio f42v7,  et  —douze lettres placées dans le folio f10r1 et dans le folio f77r11. Voir annexe page 409.

[248] Nous observons ce phénomène empiriquement dans la langue anglaise —cas de l'expérience de G. LANDINI— mais ceci est à relativiser par rapport à l'ignorance que nous avons —et tenons pour certaine— du texte manuscrit sous-jacent.

336-§ Dans les deux cas, les mots de quatre lettres et la pluralité des mots de cinq lettres sont très bien représentés, tandis que les autres vocables apparaissent délaissés.

> **Hypothèse 20 Nous présumons que les mots ont subi des altérations qui annihilent leurs caractéristiques suffisamment remarquables pour qu'elles soient ressenties comme dangereuses pour l'intégrité du secret.**

337-§ La première altération imaginable est la neutralisation des petits mots par l'ajout d'au moins une lettre nulle. Les mots de deux ou trois lettres se transforment en mot de trois ou quatre lettres. Nous confortons cette première idée par le fait que cette opération implique une augmentation par addition du nombre des mots de quatre lettres déjà présents à leur état naturel et des nouveaux mots de quatre lettres crées par l'ajout de deux ou trois lettres.

338-§ La deuxième idée qui s'inspire du même raisonnement est que les mots diversifiés, que nous attendons par habitude, sont des mots de dimensions compris entre six et huit lettres.

> **Hypothèse 21 Nous neutralisons ces mots par leur césure en deux parties. Un mot facilement repérable, car très présent, est transformé en deux mots plus difficilement détectables.**

339-§ Les conséquences de cette dernière opération sont que les fréquences des mots diversifiés de grandes dimensions décroissent très rapidement par le système simple des *vases communicants* [LAND1997]. Nous induisons que, le quasi doublement de la fréquence des mots[249], tout comme la neutralisation des petits mots par ajout de lettres nulles réduit leurs fréquences et augmentent les effectifs en mots de trois et quatre lettres.

340-§ Nos deux hypothèses, Hypothèse 20 et Hypothèse 21, s'ajustent à la logique des graphes que G. LANDINI obtient dans son compte-rendu du 1er novembre 1997. Cependant, nous sommes conscients que ce cheminement d'hypothèses est construit à partir d'*a priori* discutables et que l'aboutissement à une conclusion serait une erreur de méthode. Prospectons d'autres façons de faire et intéressons-nous aux cycles des lettres et des mots du manuscrit.

[249] Zone délimitée par les mots de trois, quatre et cinq lettres (page 409).

•

LES LETTRES et les mots, parfois les propositions, sont redondants. Ce comportement naturel s'accentue lorsqu'une méthode d'encryptage par clé de polysubstitutions est utilisée simplement parce que cette clé est de dimension très inférieure[250] à celle du cryptogramme. Nous allons rechercher si une telle clé existe. Nous utilisons trois méthodes différentes et inventées par KASISKI, FRIEDMAN et KERCKHOFFS. Mais aussi, la recherche d'une périodicité nous conduit à calculer des écarts entre signes et elle met en valeur des discontinuités dans le vocabulaire du manuscrit. La méthode de KERCKHOFFS révèle qu'il existe au moins une lettre inhabituelle voire artificielle; nous sommes alors tentés de chercher des corrélations avec les langues synthétiques de LULLE et KIRCHER dont leurs structures font intervenir « artifice mnémotechnique » et « cercles concentriques ».

Méthode de KASISKI

341-§ Friedrich W. KASISKI était un officier au 33ème régiment d'infanterie de Prusse Occidentale. Pendant ses loisirs il s'intéressa à la cryptologie et publia en 1863 un livre fondamental pour la résolution des polysubstitutions [KAHN1980].

342-§ Dans « Die Geheimschriften und die Dechiffrierkunst » —que nous traduisons par « Les chiffres et l'art du décryptage »— KASISKI offre la solution générale pour le décryptement des polysubstitutions à clés périodiques. Il remarqua que

> *lorsque deux polygrammes identiques du clair sont semblablement placés par rapport à la clé, ils donnent dans le cryptogramme des polygrammes identiques [KAHN1980].*

343-§ Finalement, KASISKI[251] se désintéressa de la question et devint anthropologue de la préhistoire. Le fait rapporté est révélateur de la personnalité du cryptanalyste.

> **Il est curieux que leurs parcours de formation ainsi que leurs travaux ne sont pas guidés par une science mais qu'ils sont très souvent pris d'un intérêt pour l'autoformation et l'étude transversale des sciences.**

---

[250] Exception de la clé à vers littéral qui peut être de dimension égale à celle du cryptogramme. Toutefois, ses redondances internes se transforment en indices si elles sont en phase avec les redondances des lettres du texte.

[251] Devenu Commandant.

344-§ Quelle est sa méthodologie ? Que nous enseigne cette façon de faire lorsque nous l'appliquons sur notre manuscrit ? De quelle manière empruntons-nous et interprétons-nous à nouveau la méthode de KASISKI ? Ces trois questions sont les trois interrogations que nous proposons de développer.

Détection des redondances

345-§ Les langues sont redondantes, dans la mesure ou elles emploient plus de caractères, de mots et de phrases, que nécessaire [SHAN1949b]. Les caractères apparaissent non aléatoirement dans un texte clair. Leurs dispositions sont imposées par des règles de grammaire et d'orthographe. C'est ce qui permet aux personnes de communiquer ou bien à des machines d'échanger des données et à un globule blanc de reconnaître l'élément étranger d'un congénère.

Quand un texte clair est régi par des règles[252] rigoureuses et que le chiffrement repose sur une méthodologie bien précise alors le texte crypté comportera les traits caractéristiques du texte clair.

346-§ Nous constatons que la synchronisation, entre deux éléments distincts et tous les deux reliés par une méthodologie d'encryptage, conduit à un troisième élément qui rend compte de cette synchronisation. C'est précisément ce que KASISKI a mis en exergue ; les redondances de groupes de lettres présentes dans le texte crypté sont liées aux redondances de la clé d'encryptage.

347-§ Mais constater une variation ne signifie pas que cette variation est la valeur de la longueur de la clé d'encryptage. Nous représentons l'ensemble de ces cas par la formule:

$$L_{clé} = \left[\frac{Ecart}{i} \right]_{i=1}^{i=Ecart-1} \quad \begin{cases} L_{clé}\ Longueur\ possible\ de\ la\ clé\ de\ chiffrement \\ Ecart\ entre\ les\ redondances\ de\ n\text{-}grammes \\ i\ Diviseurs\ indiquants\ les\ multiples\ possibles \end{cases}$$

Equation 8 Formulation de la méthode de KASISKI.

348-§ Elle signifie que la variation entre deux positions, formant une redondance, est un multiple de la longueur de la clé. L'étude des variations d'écarts d'un texte crypté montre un ensemble de valeurs vraies et un ensemble de valeurs fausses et indépendantes de la synchronisation des redondances des lettres du texte sous-jacent

[252] Le format de la messagerie militaire est particulièrement sensible à des attaques cryptanalytiques puisque tous — APAVIA, ACP127, BIR... CIR— sont rigoureusement structurés et codifiés.

d'avec les lettres de la clé.

349-§ Le choix du n-gramme le plus significatif est essentiel pour réduire le nombre de calculs de clé au stricte minimum. Nous pourrions considérer que les groupes de deux lettres sont suffisants pour révéler la dimension de la clé ; mais cela est faux, ils sont les plus fréquents[253] et par conséquent ils sont générateurs de nombreuses fausses pistes[254].

350-§ Dans le cas contraire, si nous ne tenons pas compte des grands et rares groupes de lettres alors il n'est pas certain que les redondances de mêmes vocables soient révélatrices de la synchronisation. Le n-gramme le plus favorable est celui qui offre suffisamment de clés possibles par rapport à sa dimension.

Elimination des impossibilités

351-§ Nous déterminerons la longueur de la clé Lc en considérant en priorité les écarts de redondances, des 3-grammes, puis des 2-grammes ; les monogrammes ne révélant rien de certain. Sur un ensemble de résultats, il existe des possibilités de non véracité. Nous éliminons les cas improbables en calculant le ratio de l'Equation 8. Nous constatons que nous obtenons deux sortes de résultats. La première série est l'ensemble des nombres rationnels, et, la deuxième série est l'ensemble des nombres entiers, seul le deuxième cas est probable car il n'existe pas, à notre connaissance, de clé dans l'ensemble mathématique des rationnels. Parmi la deuxième série, il existe des nombres entiers qui ne représentent pas un multiple de Lc, nous pensons à l'unité[255] ou aux valeurs isolées[256] peu représentées. Seules les valeurs de fortes fréquences sont fortement probables.

352-§ En établissant la liste quantitative des « Cas possibles » nous déterminons l'ensemble des valeurs possibles de la clé.

Existe-t-il une période d'encryptage détectable

353-§ Nous appliquons cette méthode aux deux versions du manuscrit de Voynich et nous nous confrontons à l'incapacité d'extraire une dimension probable. En effet, les redondances de n-grammes montrent une « infinité » de cas possibles.

354-§ La première cause est la longueur du manuscrit qui offre une grande variété de

[253] En théorie, si l'alphabet contient n éléments alors il existe n^2 digrammes possibles.

[254] La synchronisation du texte avec les lettres de la clé se trouve dissimulée du fait même de leur très grande diversité.

[255] Une polysubstitution avec une clé d'une seule lettre est ni plus ni moins qu'une monosubstitution.

[256] Ces valeurs ne partagent pas de multiplicateurs communs avec d'autres résultats possibles.

combinaisons de lettres. Cependant, les n-grammes de grandes tailles devraient révéler la présence d'une période de substitution. Seulement, il n'existe pas de différence remarquable entre les périodes détectées dans le manuscrit et les périodes naturelles[257] des textes classiques. Il est imaginable que le manuscrit ne soit pas un unique cryptogramme ; il serait alors un assemblage de cryptogrammes. Cette idée est probable ; pour autant, le test *Chi* [CALL1985c] est difficilement applicable pour deux raisons fondamentales :

- Nous n'avons pas la possibilité de délimiter[258] physiquement —si ce n'est avec un certain aléa basé sur l'intuition— les différents cryptogrammes du manuscrit.

- Dans le cas où notre intuition est juste nous ne pourrions pas prouver[259] que des cryptogrammes, utilisant tout ou partie des symboles mis à leur disposition, soient issus d'un même procédé cryptographique.

355-§ Nous allons donc pratiquer une étude de surface, en recherchant les modulations internes, par le calcul des écarts entre les mots identiques, folio par folio. Nous recherchons une certaine cohérence interne en considérant que la totalité de ce manuscrit est la concrétisation d'une seule expression.

Nous employons la méthode de KASISKI que nous adaptons à notre pratique.

356-§ Nous ne calculons plus la dimension probable de la clé puisque nous n'en avons pas précédemment trouvées. Nous mesurons simplement le ratio[260] entre la somme des écarts entre mots identiques et le nombre de lettres contenus dans un folio.

$$R_{folio} = \frac{\sum n_{écart}}{N_{folio}}$$

Equation 9 Ratio des écarts entre mots.

[257] Tous les textes de langue naturelle sont redondants. Les périodes détectées ne sont pourtant pas l'expression d'un système d'encryptage par polysubstitutions.

[258] Le test Chi, noté χ, fait intervenir les effectifs des symboles des textes qui sont comparés. Un mauvais discernement des cryptogrammes conduirait à une modification des effectifs et à une erreur dans les comparaisons.

[259] Le test Chi est sensible et inadéquat dans le cas ou les cryptogrammes sont écrits avec des alphabets modulables. Un cryptogramme de petite dimension n'utilise pas toutes des lettres que l'alphabet de base lui propose. Cette tendance s'accentue fortement lorsque l'alphabet, mis à disposition, est construit d'après un procédé d'encryptage à représentations multiples.

[260] Le ratio tend vers zéro quand le texte est diversifié, et inversement, le ratio tend vers l'unité quand le texte contient des vocables redondants.

357-§ Nous nous attendons à ce que chaque folio soit à peu près pourvu du même ratio[261]. Mais le manuscrit est composite. Les folios ne sont pas tous identiques. Il apparaît comme évident que le manuscrit est constitué de textes de natures[262] différentes.

> **Constat 37 CURRIER décrivait les cinq parties du manuscrit en faisant remarquer qu'elles n'étaient pas toutes écrites de la même façon. Il constatait l'existence de deux langages statistiquement différents appelées *Hand A* et *Hand B*. Il remarquait aussi cinq à huit types d'écritures.**

1- Ces deux formes *A* et *B* figurent ensembles dans l'*Herbier* et la *Pharmacie*. Seule l'écriture *Hand A* semble être présente dans la section *Astrologie*. La partie traitant de *Biologie* est le produit d'une seule « personne » qui utilisa l'écriture *Hand B*. La cinquième partie est une suite de petits paragraphes. Elle dénote un ordonnancement d'étapes nécessaires à la bonne préparation d'un acte final comme ce à quoi sert une recette. Les folios de cette section *Recette* sont rédigés avec une écriture[263] qui synthétise à la fois *Hand A* et *Hand B* [CURR1976].

2- Notre approche par le calcul d'un ratio exprimé pour chaque folio montre que les sections : *Astrologie*, *Herbier*, *Pharmacie*, sont distinctes des deux autres sections *Biologie* et *Recette*.

3- Nous pourrions considérer, comme CURRIER, que les différences sont « entièrement » liées aux sections, mais nous ne sommes pas du même avis. Notre étude faite « page après page » montre que des folios d'une section se distinguent des groupes de pages auxquels ils appartiennent.

4- D'une façon générale, nous sommes d'accord avec CURRIER lorsqu'il dit que la section *Herbier* est faite d'un bloc bien qu'elle soit écrite avec deux langages distincts.

5- De même, la seconde section *Astrologie* est faite d'une seule pièce.

6- La section *Biologie* est écrite selon un système opposé à la section *Herbier*. Par contre, la section *Biologie* est le produit d'un seul langage.

---

[261] Nous évaluons le ratio par rapport à la zone définie par l'intervalle « *moyenne* moins *écart-type* » et « *moyenne* plus *écart-type* ».

[262] Ce que nous appelons « nature » n'est pas uniquement délimité par le thème développé dans chaque texte. Nous considérons à la fois le thème discuté et le procédé d'encryptage. Les textes qui développent le même thème sont considérés de natures différentes si leur encryptage est différent.

[263] Cf. Annexe, Alphabet par folio, page 397.

7- La section *Pharmacie* est plus chaotique que la section *Astrologie*. Les pages sont distinctes, parfois proches de celles de l'*Herbier*[264], parfois proches des folios de la section *Astrologie*[265].

358-§ Finalement, nous apprécions l'évolution des sections au fur et à mesure de l'avancement des écritures dans le manuscrit (Figure 15).

Les évolutions

359-§ L'*Herbier* est écrit avec les deux types d'écriture A et B. Les vingt-cinq premiers folios sont de la main A, puis les vingt-cinq suivants sont mixés de A et de B. Le procédé d'encryptage apparaît « constant » (Figure 15) sur l'ensemble de ces cent douze pages que nous appelons *Nature 1*.

360-§ La section *Astrologie* se distingue de l'*Herbier* parce que seul le type A d'écriture est présent. La troisième section est écrite avec une main B par un seul scribe prétend CURRIER. Nous constatons en effet que cette section consacrée à la *Biologie* est uniformément constante[266], elle est issue d'un procédé autre que l'*Astrologie* et l'*Herbier* mais elle s'approche de la partie traitant de la « *Recette* ». La section *Biologie* est d'une deuxième nature que nous appelons *Nature 2*.

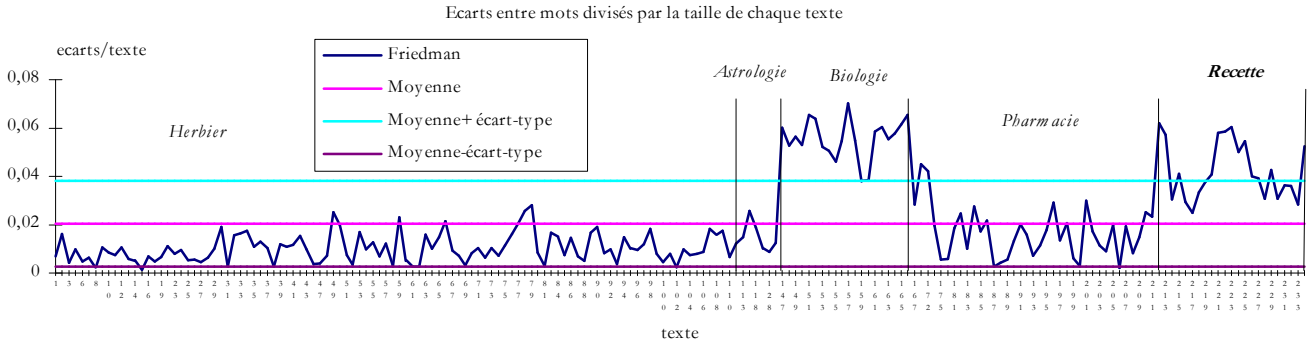


Figure 15 Variations des écarts entre mots en fonction des folios du manuscrit.

361-§ La quatrième section est « chaotique ». Elle débute par des écrits de type B mais de natures parfois proches de l'*Herbier* et parfois proches des sections *Biologie* et *Recette*. CURRIER cite le segment de pages 167–173 qu'il estime être rédigé avec le langage B. Pour nous, seules les pages 169 et 172 sont différentes.

---

[264] Pages 214, 216-219, 228, 230-233.

[265] Pages 212-213, 215, 220-227, 229, 234.

[266] Les valeurs d'écarts (Figure 15) sont supérieures à la somme de la moyenne et de l'écart-type.

362-§ La dernière section *Recette* apparaît comme un aboutissement —une conclusion— dont l'écriture est une hybridation des deux genres *Hand A et Hand B*.

Herbier	*Astrologie*	*Biologie*	*Pharmacie*	*Recette*
1 à 112	113 à 146	147 à 166	167 à 211	212 à 234
Hand A et B Nature 1	*Hand A* Nature 1	*Hand B* Nature 2	*Hand B* Nature 1 167–168, 170–171, 173 *Hand A* Nature 1 174–211 Nature 2 169, 172	*Hand (A +B)* Nature 1 214, 216–219, 228, 230–233 Nature 2 212–213, 215, 220–227, 229, 234

Tableau 7 Variations des écritures et des natures et des écarts entre mots.

Maria D'IMPÉRIO a listé les figures présentes dans le manuscrit en fonction des numéros de folio. Trouvons-nous quelques corrélations entre les emplacements des figures et les groupements que nous avons mis en exergue dans la Figure 15 ?

363-§ Le Tableau 7 montre schématiquement que le manuscrit n'est pas uniforme. La *nature 1* de la partie *Herbier* est adéquate au type de dessins qu'elle contient.

364-§ La partie *Astrologie* est comme la partie de l'*Herbier* et elle est de *nature 1* mais elle contient des dessins astrologiques[267], cosmologiques, et quelques rares dessins de « plantes ».

365-§ La partie *Biologie* est d'une deuxième nature et ses dessins sont ceux d'humains.

366-§ La partie *Pharmacie* est écrite avec les deux langages A et B ; les n*atures 1* et *2* sont aussi présentes[268]. Les pages 167–168 comportent des figures humaines mais les pages 170–171, 173, sont dédiées à la cosmologie et aux réseaux de rosettes.

367-§ Les pages 174–211 sont mixées de dessins de plantes et de représentations pharmaceutiques du type « récipients à herbes » ; elles sont écrites avec la même main *Hand B* que les pages 170–171, 173, mais elles ne contiennent pas les mêmes genres de dessins. Le fait est identique à la page 169, elle est ornée de dessins humains, elle est pourtant écrite d'une main *Hand A* qui n'est pas celle des pages 167–168. La page 172 nous fait répéter ce que nous avons dit de la page 169. Les dessins qui figurent sur la page 172 sont ceux d'étoiles mais les types d'écritures sont différents des pages

[267] Rosettes.

[268] Nous ne concluons pas que les types d'écritures conditionnent la nature des écrits. En effet, Dans la première partie, la *nature 1* est présente dans les deux types d'écriture A et B.

170–171, 173.

368-§ Nous affirmons que

> **Conclusion 9 Le manuscrit n'est pas un manuscrit crypté avec un seul procédé. La complexité se construit à partir d'une section. Quand les sections se suivent, le « procédé » évolue vers l'hybridation de deux langages[269], initialement distincts dans l'*Herbier*, en un seul langage de rédaction pour la section *Recette*.**

369-§ Nous constatons aussi que

> **Constat 38 La *nature* des écrits n'est pas dépendante du type d'écriture A ou B. De même, la *nature* des écrits n'est pas en relation avec la nature des dessins qui leurs sont juxtaposés.**

370-§ La Conclusion 9 et le Constat 38, que nous venons de formuler, nous poussent à énoncer l'hypothèse que

> **Hypothèse 22 La nature des écrits est révélatrice d'une grande variation de la méthode « d'encryptage ».**

Méthode de KERCKHOFFS

371-§ Parce que le nombre de cryptogramme est excessivement important en temps de guerre, il devient difficile de pratiquer une cryptanalyse par la méthode de KASISKI quand les chiffreurs utilisent des clés d'encryptage du type « vers littéral ». Auguste KERCKHOFFS[270] proposa

> *de ne rechercher la longueur de la clef que lorsqu'il est possible de l'obtenir assez rapidement [PRAT1940].*

372-§ Dans le cas contraire, il préconise de réunir les cryptogrammes supposés être cryptés par la même clef et de comparer ces cryptogrammes comme Wayne BARKER le fait sur les doubles transpositions[271] [BARK1995]. Nous allons donc opposer les folios du

---

[269] CURRIER considère qu'il existe au moins deux types d'écritures parce que statistiquement différentes. Si nous étudions le manuscrit, page après page, alors nous remarquons qu'il existe six *modes statistiques* différents (Constat 43, Constat 44 et Annexe page 397).

[270] Jean Guillaume Hubert Victor François Alexandre Auguste KERCKHOFFS Von Niervenhof. Directeur de l'Académie Internationale de volapük. Il écrit en 1883 « la cryptographie militaire ».

[271] Cf. Note 156 page 110.

manuscrit bien que nous savons, depuis notre étude par la méthode KASISKI qu'il soit quasiment certain que le manuscrit n'est pas le produit d'un chiffrement par polysubstitutions. Pourtant, l'intérêt de la méthode KERCKHOFFS est de mettre en opposition les séquences de lettres de cryptogrammes et de repérer si certaines parties correspondent et de spéculer ainsi sur une éventuelle « clé de substitutions »[272].

373-§ Nous considérons, à titre d'expérience, que chacune des pages du manuscrit est le fruit d'un procédé d'encryptage unique. Nous plaçons la première page sur la ligne numéro une, puis la deuxième page sur la ligne numéro deux et ainsi de suite jusqu'à la dernière[273] page du manuscrit. Notre façon de faire peut être comparée au test *Kappa*[274] [CALL1985c].

Constat 39 Le seul point remarquable que nous faisons apparaître est la prédominance de la lettre [o] qui s'intercale avec une agaçante véhémence.

374-§ Nous voyons bien que le rôle de la lettre **[o]** est de grande importance. Chacun[275] des premiers mots des pages 72 à 74 est d'une même et unique dimension de cinq lettres. Le deuxième mot qui succède à chacun de ces trois mots a pour deuxième lettre **[o].** Le fait est identique[276] pour les pages 45 à 50. Le premier mot des pages 45–50 a six lettres et le symbole **[o]** occupe la neuvième place.

---

[272] La représentation multiple n'utilise pas de clé mais la périodicité de cette substitution est remarquable.

[273] La dernière page est la page 234.

[274] Le test Kappa, noté κ, s'emploie quand la clé de polysubstitution est très longue. Les lettres des cryptogrammes sont supposées être cryptées par le même procédé et la même clé et elles sont comparées d'après leurs positions respectives. Cette approche est très inspirée de la méthode KERCKHOFFS mais elle implique —comme dans le cas du test *Chi*— que les cryptogrammes soient parfaitement synchronisés ; si ce n'est pas le cas, alors, il est indispensable de trouver le décalage qui les sépare afin qu'il soit possible d'aboutir à une solution [CALL1985c]. Nous nous demandons ce qu'on doit entendre par « aboutir à une solution » dans le cas du manuscrit de Voynich ?

[275] Le symbole dièse # indique le caractère espace (version FRIEDMAN),

vp045	P	O	R	O	R	G	#	T	O	R	#	O	P	T	A	R	#	S	C	#	T	C	O	E	#
vp046	H	T	O	8	A	R	#	T	O	F	Z	G	#	O	P	O	K	#	S	O	8	#	T	P	Z
vp047	F	T	O	E	8	G	#	2	O	S	G	#	8	A	M	#	D	Z	G	#	S	O	8	G	#
vp048	P	O	C	C	A	M	#	4	O	D	G	#	S	G	#	8	A	M	#	4	O	P	T	C	G
vp049	P	S	C	O	D	G	#	O	8	A	I	I	R	#	4	O	G	#	O	F	2	C	O	8	#
vp050	P	T	C	8	A	R	#	4	O	8	A	R	G	#	8	R	N	#	P	T	C	C	H	G	#

vp072	H	S	O	8	G	#	4	O	H	Z	G	#	4	O	H	O	E	8	G	#	T	O	P	8	A
vp073	H	O	E	O	R	#	T	O	D	Z	G	#	O	D	G	#	T	O	M	#	O	D	S	O	E
vp074	O	D	T	O	P	#	T	O	E	#	S	O	H	O	E	#	O	H	C	O	E	#	O	D	C

[276] Hormis le deuxième mot de la page 49 qui n'a qu'une seule lettre **[o]**.

375-§ Le comportement de cette lettre est aussi observable dans la transcription de CURRIER. La lettre **[O]** occupe la neuvième[277] place entre la page 9 et la page 13.

> **Constat 40 L'aptitude de la lettre [O] à occuper certaines positions est suffisamment occurrente pour ne pas être considérée comme une coïncidence fortuite.**

376-§ Nous allons voir à présent comment calculer cette coïncidence à travers la méthode de FRIEDMAN.

Méthode FRIEDMAN

377-§ William Frederick FRIEDMAN est né en Russie en 1891. Après que sa famille eut immigré aux Etats-Unis. Il étudia la génétique à l'université de Cornell. Il fut engagé en 1915 par George FABYAN pour « améliorer les semences et le cheptel de sa ferme ». Un des laboratoires de cet homme fortuné se consacrait à rechercher les indices permettant de dire que les oeuvres de SHAKESPEARE étaient celles de Francis BACON. C'est en préparant des agrandissements photographiques de ces oeuvres que FRIEDMAN fut attiré, ainsi que celle qui deviendra sa femme, par la cryptanalyse. David KAHN souligne que

> *c'est encore un des paradoxes de l'histoire de cette science que l'intérêt de deux cryptologues de premier plan ait été éveillé par une thèse erronée, contre laquelle ils allaient lutter toute leur vie,*

378-§ comme si l'impossibilité renforçait leur ténacité. Par la suite, la guerre éclata en Europe et ils furent sollicités par l'armée comme cryptologues. FRIEDMAN assura entre autre la formation des officiers à la cryptologie. A son propos, David KAHN conclut :

---

[277] Neuvième caractère à partir de la gauche de la ligne. Le caractère séparateur de mots (l'espace) est considéré comme un caractère à part entière (version CURRIER)

vp009	D	T	O	8	G	#	F	T	**O**	G	#	T	D	O	G	#	O	A	M	#	O	A	R
vp010	D	**O**	T	C	O	R	#	T	**O**	R	#	G	H	T	C	G	#	P	S	O	8	#	T
vp011	P	**O**	A	R	#	G	#	S	**O**	E	#	T	O	E	O	R	#	P	Z	O	E	#	T
vp012	D	**O**	A	R	G	2	A	R	**O**	C	C	C	T	C	C	D	A	R	#	4	O	A	8
vp013	F	T	O	8	A	M	#	S	**O**	P	T	C	G	#	4	D	O	#	S	C	G	#	4

> *FRIEDMAN a prospecté le domaine cryptologique plus largement et plus profondément que quiconque... créa une terminologie rationnelle... En définitive, la puissante organisation cryptologique américaine, telle qu'elle existe de nos jours, avec ses milliers d'employés et son vaste réseau de stations, est née du petit bureau que FRIEDMAN créa de toutes pièces au sein du ministère de la Guerre.*

Indice de coïncidence

379-§ La notion de «Nombre de Coïncidence» fut introduite en 1920 [FRIE1922]. Elle est d'une certaine façon la poursuite du travail de KASISKI sur la détection des redondances de polygrammes. Seulement, son domaine s'étend à la mise en évidence de familiarités entre les cryptogrammes. En cela, l'indice de coïncidence est utile pour répondre aux questions : « est-ce que le cryptogramme est issu d'un encryptage monoalphabétique ? », et, « quelle est la dimension de l'alphabet le plus probable ? », ou, « est-ce que les cryptogrammes que nous étudions sont issus d'un même procédé d'encryptage ? », certains s'accordent[278] même à dire qu'il est en fonction direct avec la valeur numérique de la longueur de la clé d'encryptage. En fait, l'indice de coïncidence résume un rapport entre ce que nous observons dans un cryptogramme et ce à quoi nous aurions dû nous attendre dans le cas d'un désordre « parfait ». FRIEDMAN analyse —dans sa méthode— un chiffre de VOGEL en trois étapes.

> *La solution du problème se trouve grâce à trois étapes ; la détermination de la longueur de la période, la reconstruction de la clé numérique, puis finalement la reconstruction des alphabets chiffrants.*

380-§ La première consiste à déterminer la longueur de la période d'encryptage qui jusqu'à présent reposait sur la méthode de KASISKI:

> *...si il existe des répétitions dans le texte clair avec des intervalles constants[279] alors nous les retrouverons dans le texte crypté...*

381-§ A l'instar de KERCKHOFFS il considère qu'elle est impuissante dans certain cas. En étudiant une cryptanalyse possible du disque de VOGEL[280], il constate:

---

[278] Nous lançons là un « pavé dans la mare ». Les méthodes cryptanalytiques développées par FRIEDMAN, CALLIMAHOS, KULLBACK ne se résume pas à un simple calcul algébrique qui met en relation directe les occurrences de lettres d'un cryptogramme en fonction d'une période d'encryptage. Leurs pratiques est méthodologiques et font appel à deux suppositions essentielles : la nature du langage utilisé dans le texte sous-jacent ainsi que la longueur probable —approximative— de la clé d'encryptage. Leurs méthodologies reposent systématiquement sur la recherche de coïncidences internes ou externes des lettres des cryptogrammes ; artefact que nous retrouvons dans le test de la moyenne de *Phi [CALL1985c]* et le test *Chi* (comparaison de cryptogrammes).

[279] Ou multiple d'un nombre commun.

[280] Procédé d'encryptage utilisant un système de cinq disques concentriques.

> *...dans un cryptogramme contenant plusieurs alphabets en un seul, les répétitions de trigraphes et de polygraphes seront naturellement moins fréquents sauf pour un message très long.*

382-§ En ce sens que la méthode de KASISKI vue précédemment est insuffisante dans le cas d'encryptages successifs par différents alphabets.

383-§ Dans leur ouvrage *Cryptography, an introduction to computer security*, J. SEBERRY et J. PIEPRZYK donnent l'ordre des étapes comme suit : il faut avant tout calculer la valeur de l'indice de coïncidence du texte étudié. La comparaison de cette valeur avec une table —donnant l'indice en fonction de la période— permet d'apprécier la longueur de la clé d'encryptage. Dans une troisième étape, ils recherchent les diviseurs communs entiers et découpent le texte principal en fonction du plus petit diviseur commun. Maintenant, ils disposent d'un ensemble de textes classés par ordre décroissant d'indice de coïncidence. Finalement, ils assument l'induction qui relie l'indice le plus élevé au sous texte révélant le plus d'information. Ainsi, pourraient-ils s'attendre à découvrir les lettres, « A » et « E », comme les lettres les plus occurrentes dans ce sous texte, et ce, pour la langue anglaise.

Critique

384-§ Le premier objet de la critique est la relation inductive entre le calcul de l'indice de coïncidence et la longueur de la clé d'encryptage. SEBERRY et PIEPRZYK réduisent le test *Chi* (notes 258–259) à un simple calcul d'échelle. Or, la force de la méthode du test *Chi* est de quantifier les coïncidences entre lettres selon la modulation[281] de la longueur de la clé d'encryptage que l'on a estimée —mais pas encore déterminée— par le calcul d'indice de coïncidence.

385-§ Le petit programme qu'ils proposent montre combien la relation entre l'indice de coïncidence et la période est sujette à des fluctuations[282] d'ordre contextuel.

En ce sens, ils fixent des valeurs comme constantes or qu'elles devraient être considérées comme des variables.

386-§ La *« Measure of Roughness »* est une de ces valeurs [SINK1968]. Sa valeur oscille entre la mesure théorique des probabilités équiprobables et la mesure d'une observation qui normalement est d'ordre contextuelle.

---

[281] La longueur de la clé est indéterminée. Le calcul d'indice de coïncidence permet d'avoir une estimation —ou une « fourchette » d'évaluation— de cette longueur après quoi le test *Chi* est appliqué pour chaque longueur de clé au voisinage de cette estimation.

[282] Ils mettent en relation un calcul purement mathématique avec une caractéristique non universelle de la langue.

$$MR = \sum_{i=0}^{i=n-1} \left(p_i - \frac{1}{n} \right)^2 \quad \text{avec} \quad \sum_{i=0}^{i=n-1} p_i = 1$$

Equation 10 Measure of Roughness d'après SINKOV.

387-§ Par exemple, un seul et unique événement a pour *MR* la valeur zéro ; une séquence dont chacune des lettres apparaît avec la même probabilité crée une *Measure of Roughness* nulle. Cette opération est intéressante puisqu'elle positionne une série d'événements par rapport à un tirage équiprobable. J. SEBERRY et J. PIEPRZYK fournissent alors le lien entre l'indice de coïncidence et la *« Measure of Roughness »*. Ils appellent cet indice *« The index expected »*, en ce sens l'indice attendu par rapport à des inductions[283] préalables.

$$Ic(exp) = \frac{\frac{1}{d} \times (N - d)}{N - 1} \times high + \frac{(d - 1) \times N}{d \times (N - 1)} \times low$$

Equation 11 Indice de coïncidence attendu.

388-§ La valeur obtenue pour la langue anglaise, $MRanglais_{(high)}$ est[284] de 0.066, reflète uniquement un cas particulier de cette langue anglaise;

c'est pourquoi il est nécessaire dans ce cas de connaître au préalable la langue de rédaction du message crypté.

389-§ La plus basse *MR* possible pour un alphabet de *n* lettres est $n \times \left(\frac{1}{n} \right)^2$. Admettons que l'alphabet de la langue anglaise comporte vingt-six lettres *(n=26)*. Nous obtenons $26 \times \left(\frac{1}{26} \right)^2$. La valeur minimale[285] $MRanglais_{(low)}$= 0,038. Finalement, pour un texte de 100 000 caractères, de langue anglaise et de période d'encryptage de longueur 10 caractères, ils obtiennent l'indice de coïncidence,

[283] Deux inductions se présentent : l'induction de langage exprimée par Mr_{high} repose sur la supposition des valeurs empiriques des probabilités et implicitement la dimension de l'alphabet utilisé dans le texte sous-jacent est supposée dans le calcul de Mr_{low}.

[284] D'après leurs propres sources statistiques.

[285] Valable pour tous les langages basés sur 26 lettres.

390-§

$$Ic(exp) = \frac{\frac{1}{10} \times (100000 - 10)}{100000 - 1} \times 0{,}066 + \frac{(10 - 1) \times 100000}{10 \times (100000 - 1)} \times 0{,}038 \text{ , } Ic(exp)=0{,}04079.$$

391-§ Vous pouvez tester cette équation pour des dimensions différentes de taille de texte, vous constaterez que l'indice de coïncidence varie peu. Tandis que MR_{low} influence grandement l'évaluation de cet indice. Comme cette opération est la première parmi d'autres qui elles-mêmes devront assumer d'autres inductions, nous ne pouvons qu'être prudent quant à l'interprétation de ce calcul. Dans le cas du manuscrit de Voynich, si nous considérons qu'il est rédigé dans l'une des huit langues suivantes : anglaise, française, allemande, italienne, romaji, portugaise, russe et espagnole, alors la longueur de la clé d'encryptage est inexistante[286].

> **Conclusion 10 Il n'existe pas de clé d'encryptage au sens ou nous l'entendons du seizième siècle à aujourd'hui et pour la langue, anglaise, française, allemande, italienne, romaji, portugaise, russe, espagnole et latine.**

392-§ En fait, le calcul d'indice de coïncidence montre un certain désordre parmi les fréquences des lettres constituant le texte crypté. C'est en termes de possibilités d'interprétation qu'il faut raisonner et non en induction mettant en relation l'indice de coïncidence à la longueur de la clé d'encryptage.

> **Le groupe de lettres qui montre un indice élevé sera plus facilement analysable qu'un groupe de lettres dont l'indice est petit.**

393-§ Il est à noter, en effet, que l'indice se calcule d'après des occurrences et non pas d'après des fréquences de lettres[287] comme cela est le cas dans la méthode de SEBERRY. De ce fait, un indice de coïncidence ne peut être négatif[288] puisque les occurrences d'un élément sont au moins égale à l'unité. Par contre, la différence entre

---

[286] La formule qui donne la période d'encryptage en fonction de la langue, de l'indice de coïncidence et de la taille du texte est $d = \frac{N(h - l)}{N(ic - l) + h - ic}$. La longueur de la clé d'encryptage varie entre 0,29 et 0,94 : autant dire qu'il n'existe pas de clé d'encryptage continue sur l'ensemble du manuscrit (page 385).

[287] La distinction est simple. L'occurrence d'un élément est la somme de ses répétitions, tandis que la fréquence est la somme des occurrences d'un élément divisée par la somme totale de toutes les occurrences rencontrées.

[288] L'indice de coïncidence est inférieur à zéro lorsqu'il est calculé par rapport au nombre de coïncidence qui lui peut être négatif (cas de la comparaison entre différents cryptogrammes).

la fréquence et l'unité est systématiquement inférieure ou égale à zéro.

Acceptabilité

394-§ Nous trouvons, dans l'ouvrage de SEBERRY, une définition qui exprime l'indice de coïncidence en fonction des fréquences de lettres. Or, il est évident qu'une fréquence est toujours inférieure ou égale à l'unité quand on déclare que la somme des fréquences est égale à l'unité [SEBE1989]. Les indices des langues européennes calculés par FRIEDMAN et KULLBACK montrent des valeurs[289] comprises entre 0,05 et 0,09.

Nous doutons de l 'exactitude[290] de la formulation faite par SEBERRY et PIEPRZYK et nous rappelons que l'originalité de l'indice de coïncidence est d'être une recherche du cas le plus favorable en coïncidence entre des événements. La notion de fréquence est délaissée pour l'agrégation d'analogies.

---

[289] Nous faisons remarquer que l'indice peut se calculer sans se référer à une pondération par l'effectif de l'alphabet ; ainsi la valeur de l'indice est diminué de ce facteur multiplicateur.

[290] Nous pensons que cette confusion se situe dans les deux approches possibles de l'indice de coïncidence. La première façon de faire repose sur la méthode d 'étude locale qui privilégie la recherche de coïncidences locales entre lettres ou groupes de lettres.

1. FRIEDMAN pratique cette méthode en calculant la différence entre les éléments —lettres, groupes de lettres— qui coïncident et les éléments qui ne coïncident pas. Cette soustraction est alors ramenée au *prorata* du nombre total de coïncidences rencontrées. Ainsi, si une lettre 'a' coïncide un certain nombre de fois avec un événement —nous notons cette coïncidence *Ka*— et qu'une autre lettre 'z' coïncide un certain nombre de fois avec ce même événement —nous notons ce nombre de coïncidence *Kz*— alors le nombre de coïncidence entre 'a' et 'z' est la soustraction de la coïncidence —entre 'a' et 'z'— et de la non coïncidence entre 'a' et 'z'. L'indice de coïncidence se détermine alors comme la division de cette soustraction par la totalité des coïncidences rencontrées. Dans ce cas il est possible d'obtenir un indice de coïncidence négatif.

2. La deuxième façon de faire est le calcul de *Kappa*. Cette variable est basée sur le concept de coïncidences [KULL1977]. La méthode de KULLBACK est pourtant différente pour trois raisons fondamentales.

   - Le test de *Kappa* s'exprime indépendamment de la non-coïncidence entre événements.
   - *Kappa* admet une valeur théorique et une valeur d'observation dont le rapport indique une distance entre ce qui est attendu et ce qui est observé : elle met en exergue le désordre des lettres d'un cryptogramme —relativement à l'induction du langage sous-jacent.
   - La troisième raison est certainement à l'origine de la confusion (page 84 de [KULL1977]). *Kappa* se calcule comme le rapport entre une valeur observée et une valeur théorique. La valeur observée —appelée **Φ**o— est liée aux occurrences des lettres présentes dans le cryptogramme ; cette valeur est donc un entier positif supérieur à l'unité. Or la décomposition de **Φ**o s'écrit *fi(fi-1)* qui prête à confusion avec la notion statistique de fréquence dont la valeur est comprise entre 0 et 100.

L'indice de coïncidence est compris entre (-1) et (1) tandis que *Kappa* —issu de cette même notion de coïncidence— est compris entre 0 et 1. Dans le cas ou *Kappa* est calculé par rapport à la *Measure of roughness(Mr)* alors *Kappa* est compris entre 0 et 1/*Mr*.

395-§ La formule de l'indice de coïncidence faite par FRIEDMAN est la suivante:

$$Kappa(ic) = \frac{\sum_{i=1}^{i=Dim\ alphabet} \frac{fi(fi-1)}{n}}{\frac{N(N-1)}{n}} \quad avec\ fi \geq 1$$

Equation 12 Indice de coïncidence.

Avec fi l'occurrence de la lettre de rang i dans l'alphabet, n le n-gramme considéré et N le nombre de lettres du texte étudié.

396-§ Cette formule révèle quatre états interprétables. Quand toutes les valeurs des fi sont basses, on constate que *kappa* a tendance à converger vers zéro. C'est le cas d'une période d'encryptage très grande[291]. Lorsqu'un texte est non crypté, ou crypté avec la conservation des statistiques naturelles, on remarque que *kappa* tend vers la valeur de *kappa* de la langue de rédaction[292]. Quand la valeur de *kappa* est comprise entre les deux cas précédents. La valeur de *kappa* est variable et inutilisable[293]. Lorsqu'une ou plusieurs lettres se distinguent quantitativement des autres, on peut remarquer que *kappa* est grand : on exploite alors les fortes présences de lettres[294]. En fait, *kappa* est

---

[291] Exemple de série, S=(a, a, a, a, a, a, a, a, a, a).

$$\text{Kappa(1 - gramme)} = \frac{1(1-1)+1(1-1)+\ldots+1(1-1)}{10(10-1)} = \frac{(1-1)}{10\times 9} = \frac{0}{90} = 0$$

[292] Exemple de série, S =(a, b, b, b, b, c, c, c, c, c)

$$\text{Kappa(1 - gramme)} = \frac{1(1-1)+4(4-1)+5(5-1)}{10(10-1)} = \frac{32}{90}$$

[293] Exemple de série, S= (x,y,z,a,a,b,b,c,c,c).

$$\text{Kappa(1 - gramme)} = \frac{1(1-1)+1(1-1)+1(1-1)+2(2-1)+2(2-1)+3(3-1)}{10(10-1)} = \frac{10}{90}$$

[294] Exemple de série, S =(a,b,c,e,e,e,e,e,e,e).

$$\text{Kappa(1 - gramme)} = \frac{1(1-1)+1(1-1)+1(1-1)+7(7-1)}{10(10-1)} = \frac{42}{90}$$

exploitable quand des occurrences se marginalisent par leurs grandes valeurs d'unités distinctes.

Détermination de la langue

397-§ Les travaux de FRIEDMAN et KULLBACK ont permis de relier le langage avec une échelle de valeurs sur laquelle les langues écrites sont hiérarchisées ; elle permet aux cryptanalystes de mesurer l'écart entre la référence et le cas qui se présente sous la forme d'un cryptogramme. Cette mesure doit révéler la nature du système d'encryptage quand la langue de rédaction du cryptogramme est connue. Cette mesure révèle la nature du langage quand le système d'encryptage est connu[295]. Il s'agit d'une équation à trois composantes[296] et deux inconnues[297].

398-§ Nous n'avons pas détecté de périodicité d'encryptage dans le manuscrit de Voynich. Nous estimons donc qu'il ne s'agit pas d'une polysubstitution comme nous en avons parlé précédemment (Conclusion 10). Nous calculons l'indice de coïncidence du manuscrit.

> **Constat 41 Nous trouvons un indice de coïncidence (kappa) de 0,0951 pour la transcription[298] de FRIEDMAN avec les espaces ; sans espaces, l'indice *kappa* diminue à 0,0842.**

399-§ Nous comparons l'indice calculé sans espace avec les indices de référence que KULLBACK présente à la page 83 de son traité sur les outils mathématiques utilisés en cryptanalyse [KULL1977]. Huit langues figurent sur son échelle. Celle qui a la valeur d'indice[299] la plus basse est la langue russe. La valeur la plus haute est tenue par la langue japonaise. Or, l'indice du manuscrit est en-dehors et supérieur à cette échelle[300].

---

295 Connu pouvant être étendu a présumé.

296 La référence, le langage du cryptogramme, le système d'encryptage.

297 La langue du cryptogramme et le système d'encryptage.

298 La transcription de CURRIER fournit des indices sensiblement identiques. Avec espaces, Kappa(ic)=0,0902. Sans les espaces, Kappa(ic)=0,0836.

299 Indice de coïncidence monographique.

300 Le russe est à 0,0529 et le japonais est à 0,0819.

Constat 42 Le japonais *romaji* est le langage dont l'indice de coïncidence est le plus proche[301] du manuscrit.

400-§ Comment expliquons-nous ce fait ? Nous savons que l'indice se calcule par la somme des occurrences ôtées de l'unité. Le comportement des occurrences est relatif à cette unité. Le schéma est simple,

plus les occurrences tendent vers cette unité et plus l'indice tend vers zéro.

401-§ Par conséquent, l'indice de coïncidence *Kappa* converge vers une valeur grande[302] quand *fi* est grande : c'est le cas lorsque une lettre est excessivement représentée par rapport aux autres lettres du cryptogramme.

402-§ Peut-on considérer que la représentation multiple soit à l'origine de ce fait ? *A priori* non[303], la substitution à représentations multiples partage les occurrences d'une lettre avec d'autres représentants. L'implication de cette méthode d'encryptage est alors une uniformisation[304] des fréquences de symboles. Par conséquent,

Hypothèse 23 Nous présumons que la forte présence de la lettre [0] est en partie responsable de l'élévation de l'indice de coïncidence.

403-§ Nous avons remarqué, auparavant, que le manuscrit n'était pas constitué d'une « nature » uniforme[305]. Or le calcul d'indice que nous avons fait, ci-dessus, est un calcul moyen sur l'ensemble du manuscrit. Autrement dit, les différentes parties peuvent se neutraliser mutuellement et ainsi fausser nos hypothèses. Pour cela, nous étudions la valeur de cet indice page par page.

---

[301] Voir aussi la Conclusion 7 sur l'opposition entre kana et romaji par STALLINGS et LANDINI.

[302] Au mieux si $fi = N$, alors $\frac{fi(fi-1)}{N(N-1)}$ devient $\frac{N(N-1)}{N(N-1)} = 1$.

[303] Cependant, une substitution à représentations multiples se dissimule par l'adjonction de lettres nulles à fortes occurrences. En ce cas, la réponse est positive.

- Les langages synthétiques sont construits d'après les règles fixées par le créateur et il n'est pas improbable que certains cas soient en adéquation avec l'hypothèse de TILTMAN et le Constat 42.

[304] En théorie 1/Alphabet. Si il existe vingt-six lettres dans l'alphabet alors la valeur équiprobable théorique est 1/26.

[305] Cf. Figure 15, page 164.

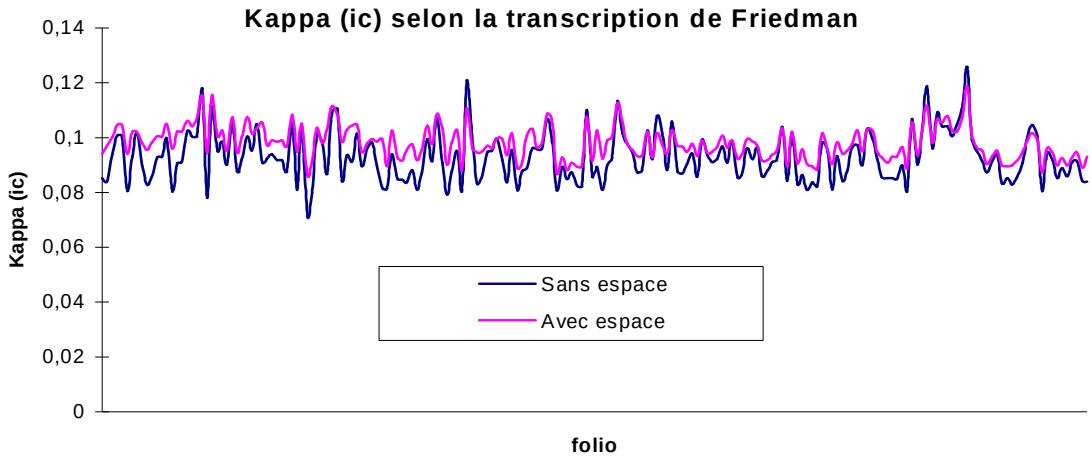


Figure 16 Indice de coïncidence en fonction des pages du manuscrit (valeurs en annexe page 386).

404-§ La répartition constante de l'indice de coïncidence[306], autour de sa moyenne[307], nous dévoile une constance dans la distribution des effectifs. Cependant, les écarts entre mêmes mots (page 164) ne confirment pas pleinement ce jugement. Ils nous disent que des pages du manuscrit sont bien plus disparates que d'autres. Le plus remarquable est que ces pages ne sont pas immédiatement placées au début du manuscrit et elles ne sont pas réparties uniformément tout au long du document, mais plutôt, elles se trouvent « groupées » à partir de la deuxième moitié, pour une quarantaine de pages, puis réapparaissent dans le dernier tiers de cette deuxième moitié.

405-§ Le manuscrit semble constitué de pages écrites avec une certaine constance[308] dans l'utilisation de l'alphabet[309]. Mais l'agencement des mots et des lettres modifient les valeurs d'écarts.

---

[306] Les écart-types de ces deux séquences sont respectivement (annexe page 386) pour le texte avec espaces et le texte sans espace : CURRIER(0,0109 ; 0,0074) et FRIEDMAN (0,0091 ; 0,0062). Les moyennes respectives sont CURRIER(0,0937 ; 0,0990) et FRIEDMAN (0,0929 ; 0,0981). Ces moyennes sont différentes de l'indice de coïncidence kappa que nous avons calculé sur l'ensemble du texte : en effet, la moyenne des indices de coïncidences de cryptogrammes différents n'est pas égale à l'indice de coïncidence calculé sur la sommes de ces cryptogrammes : la fonction de l'indice de coïncidence n'est pas additive.

[307] La zone est déterminée par deux bornes. La borne haute est la moyenne de l'indice plus la valeur de l'écart-type. La borne basse est la moyenne moins la valeur de l'écart-type.

[308] Constat de l'étude de l'indice de coïncidence.

[309] Nous ne disons pas qu'il existe un seul alphabet. A chaque page nous trouvons qu'un alphabet est utilisé d'une manière similaire à celui des autres pages.

Ainsi la modularité de l'indice provient essentiellement de la modification des positions des mots et non d'un changement de proportion de chaque lettre utilisée.

Est-ce totalement vrai ? Pour tenter d'y répondre nous étudions le manuscrit comme si il était un assemblage de textes écrits avec des alphabets différents d'encryptages.

Diversité des alphabets

406-§ Jusqu'à présent, nous avons considéré que l'alphabet de lettres était unique et constant sur l'ensemble du manuscrit.

Comme les indices sont peu fluctuants et que les écarts montrent de fortes variations alors il doit exister des modifications dans l'organisation[310] de l'alphabet.

407-§ Nous étudions les effectifs de lettres pour chaque page afin de détecter quelques variations[311].

Constat 43 Notre surprise est de constater la non uniformité des alphabets de chacune des pages.

408-§ Le plus grand des alphabets est celui de la page 91 du manuscrit ; il est constitué de vingt-trois lettres. Le plus petit alphabet est présent dans deux pages voisines : 204 et 207. Il contient dix lettres et le caractère[312] espace n'arrive qu'en seconde position. Nous pourrions croire que ce fait est exceptionnel : certes non, il se reproduit à la page 103, ou la lettre **[o]** est autant représentée que le caractère espace. Nous avons quelques difficultés à croire qu'une lettre puisse être autant représentée que cet inéluctable espace. Il nous faut nous rappeler l'expérience de décryptage du cunéiforme de Babylone (page 215) pour comprendre que l'absence de « vide » entre groupes de signes ne dit pas que ces groupes sont soudés les uns aux autres. Tout comme la présence d'un tel espace ne signifie pas *de facto* qu'il est le seul et unique représentant de sa condition.

---

310 C'est-à-dire que les lettres sont changées —substituées— dans leurs représentations graphiques mais elles sont inchangées —ou peu altérées— dans leurs fréquences.

311 Cf. Annexe, Alphabet par folio, page 397.

312 L'espace n'est pas comptabilisé dans l'alphabet en tant que lettre. Nous signalons quand même son rang car il est un indicateur essentiel. En effet, il n'est pas assuré que ce caractère soit réel. Sa fonction pourrait être celle d'une lettre nulle comme dans l'écriture de l'ancien Perse où l'espacement est représenté par un caractère oblique.

Dans ce manuscrit l'espace est honorablement représenté[313]. Toutefois, ce qui nous intrigue est l'équivalente représentativité de la lettre [O] de la page 103.

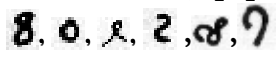
409-§ Somme toute, nous pourrions penser que toutes deux sont de la même nature. Mais alors, le symbole représenté par ces deux signes serait extraordinairement envahissant[314].

410-§ Est-ce que la lettre **[O]** est tout simplement la lettre d'un alphabet ? Nous en doutons. L'occurrence est trop importante[315] pour être l'expression d'une seule lettre cryptée : hormis le cas de la monosubstitution de CÉSAR[316] où si, tel avait été le cas, nous n'aurions eu aucun souci pour décrypter le manuscrit.

411-§ Puisqu'il est peu probable que la lettre **[O]** soit une lettre : que peut-elle être ? Cette question nous rappelle un système codique du XVI^{ème} siècle. Ce code de 1552 fut utilisé par le Connétable Duc de Montmorency et il est un exemple de substitution à représentation multiple. Son tableau de substitutions est décomposé en quatre parties. L'une d'entre elles est réservée à l'utilisation de signes nuls. L'insertion de ces signes dans le texte substitué permet de dérouter l'attaque du cryptologue. Leur simple présence modifie deux aspects essentiels du texte clair : en premier lieu, ces signes modifient les statistiques de chaques groupes de lettres, la deuxième modification porte sur la structure des mots. L'insertion d'un signe nul dans un mot implique une croissance de la dimension du mot (page 154). La recherche analogique, entre ce mot et un lexique, se complexifie au point de devenir parfois impossible quand le nombre de signes nuls utilisés est grand.

412-§ Or, si nous considérons chaque page du manuscrit comme unique alors nous remarquons qu'il existe à chaque fois une lettre excessivement représentée. Ces lettres sont dans le cas de CURRIER comme dans le cas de FRIEDMAN : **[O, G, C, T, A, 8].**

Constat 44 Six lettres : [O], [G], [C], [T], [A] et [8], jouent le rôle de modes statistiques dans les effectifs de lettres par folio.

Hypothèse 24 Existe-t-il une relation entre ces six lettres, [O], [G], [C], [T], [A], [8], et les six lettres 

313 Entre 17 et 25 %.

314 De l'ordre de 30 à 40 %.

315 Entre 11 et 21 %.

316 Les statistiques sont décalées mais conservées dans leur grandeur (note 158, page 112).

de l'hexagone du folio 69r ? Les lettres  et  : sont-elles l'Alpha et l'Oméga du Carré magique ?

413-§ Lorsqu'on examine la géométrie du le carré magique on découvre des formes comme la croix.

S	A	**T**	O	R
A	R	**E**	P	O
T	**E**	**N**	**E**	**T**
O	P	**E**	R	A
R	O	**T**	A	S

414-§ Cette croix partage le carré magique en 4 carrés de 4 lettres. On observe une symétrie parfaite à la lettre N qui est le centre du carré des croix TENET et SRRS×RPPR. Son caractère à la fois unitaire et centriste nous rappelle qu'il existe une graphologie qui donne un sens à ce carré. Le N est le point commun d'un ensemble de signifiants. La croix TENET est entourée des lettres A et O qui en Grec représentent l'alpha[317] et l'Oméga[318].

	A	T	O	
A		E		O
T	E	N	E	T
O		E		A
	O	T	A	

415-§ Et l'on ne peut ne pas penser au Dieu des chrétiens qui se définissait ainsi :

> *Je suis l'alpha et l'oméga dit le seigneur Dieu, celui qui est, et qui était, et qui vient, le tout-puissant*[319].

416-§ Ainsi à un commencement correspond une fin et inversement la fin correspond au commencement. On a la révélation cyclique d'un état à un autre. La croix est alors inscrite dans le cercle dont le N est le centre et TEN[320] le rayon. La symbolisation recherchée est le graphe suivant :

---

317 Première lettre de l'alphabet.

318 La dernière lettre.

319 Le Nouveau Testament, Apocalypse de St Jean, Prologue 1, dédicace aux sept Eglises d'Asie.

320 La Tène est un village de Suisse qui borde le lac de Neuchâtel. En 1858, on découvre des vestiges archéologiques d'habitat, de sépultures diverses. Incinération ou inhumation de chefs Celtes, ces sépultures sont dites "Tombes à char"(Les Celtes édition BOMPIANI 1991). Chez le peuple Celtes, la civilisation du 2ème âge de fer débute aux alentours de 450 av. J.-C. et elle comporte trois phases: la TÈNE I, la TÈNE II et la TÈNE III (de 120 av. J.-C. au premier siècle apr. J.-C.) marque l'opposition des Celtes face à l'empire Romain et autour des conquêtes Romaines.

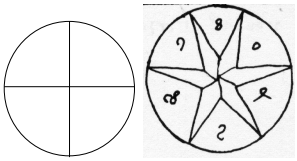


Figure 17 Le cercle du carré magique (à gauche) et l'hexagramme[321] du folio 69 (à droite).

417-§ La croix circonscrite au cercle signifit en cosmographie[322], la terre, les 4 éléments du cosmos[323] : Eau, Air, Feu, Terre. Ce que confirme la valeur 4 ogammique du N au centre de la figure. Au centre nous trouvons l'élément principal, le chiffre 4 des éléments de la terre et autour les 24 autres éléments qui font encore une fois référence à la doctrine chrétienne[324].

418-§ Le folio 69r présente des similitudes bien que la « roue » figurée soit hexagonale. Son *oméga* ꝏ est séparé de son *alpha* par un rayon de l'étoile hexagonale circonscrite à la roue ; le carré magique comporte deux rayons de moins et ses quatre branches contiennent le mot « TEN ». Le folio 69r n'est par pourvu de rayons étiquetés et le cycle est décrit par un commencement ꝟ suivi des lettres ꝛ, ꝺ, ꝯ, ꝺ et une fin ꝏ : « le serpent se mordant la queue », *Ouroboros* emblème[325] de l'alchimie [AROM1996].

321 Vue centrale et partielle du folio 69, la totalité est en page 50.

322 du grec *Kosmos* qui signifie Ordre.

323 Dans l'élaboration des concepts de la matière, au VI[ème] siècle av. J.-C., l'école de Milet énonce que l'eau est la cause matérielle de toutes choses, c'est l'expression de l'idée d'une substance fondamentale dont toutes les autres choses ne seraient que des formes passagères. Anaximandre —élève de Thalès— pensait plutôt qu'il existe un « Mouvement éternel » de la création et de la disparition des mondes passant de l'infinitude à l'infinitude. Anaximène —ami d'Anaximandre— enseignait que l'air est la substance première: « Tout comme notre âme, étant de l'air, assure notre cohésion, la respiration et l'air embrassent le monde entier ». Pour Héraclite d'Ephèse, le feu est l'élément primordial dont le principe fondamental est le « changement impérissable », le feu étant à la fois matière et force motrice. Empédocle fut le premier à penser au pluralisme des substances fondamentales. Son hypothèse était qu'il existait quatre éléments fondamentaux: la Terre, l'Eau, L'Air, le Feu. Il décrit le monde comme étant une sphère infinie, pendant que l'un détruit l'autre synthétise et inversement.

324 Dans le Nouveau Testament, selon St Jean, « les visions de la révélation », le Trône de Dieu est au centre et entouré des 24 vieillards.

325 La conception hermétique du temps circulaire porta au cœur de la culture alchimique l'idée d'une cyclicité du cosmos et de l'existence dans laquelle l'homme aussi était directement engagé.

Conclusion 11 Seuls  et  du folio 69r sont comparables à la représentation cosmologique de α et de Ω circonscrits au cercle.

419-§ L'analogie[326] entre le système de représentation du carré magique et celui de l'hexagone du folio 69r est porteuse de l'enseignement qu'il existe un cycle ; est-il un cycle d'encryptage qui indique, par quelque artifice, qu'une lettre parmi **[O, G, C, T, A, 8]** doit être excessivement représentée ? Ou est-il tout simplement possible que cette coïncidence numérique soit fortuite ; tout comme pourrait l'être la plante à treize branches du folio 34r —dont la sixième branche est pliée (page 51)— avec l'arbre alchimique des treize cycles de la lune ?

420-§ Quant à **[O, G, C, T, A, 8]** : sont-elles toutes des lettres nulles ? Sont-elles des lettres nulles, à certaines pages du manuscrit, puis des lettres, à d'autres pages ? *A priori*, l'alternance de ces signes, en tant que mode statistique de chaque alphabet, laisse penser qu'il y a alternance de règles d'encryptage dans la manipulation des alphabets.

Constat 45 La structure du manuscrit nous suggérait l'Hypothèse 22, le Constat 44 indique que les six lettres —*modes statistiques*— du manuscrit jouent un rôle dans l'alternance des règles d'écriture.

Que se passe-t-il lorsque nous supprimons la lettre [O] de la première page[327] du manuscrit ? Que deviennent les mots ?

421-§ Nous plaçons en ordonnée le pourcentage de mots rencontrés en fonction de leur dimension en nombre de caractères. Nous remarquons que

Constat 46 La suppression de la lettre [O] ne perturbe pas la distribution des mots de trois lettres : ils sont les plus fréquents.

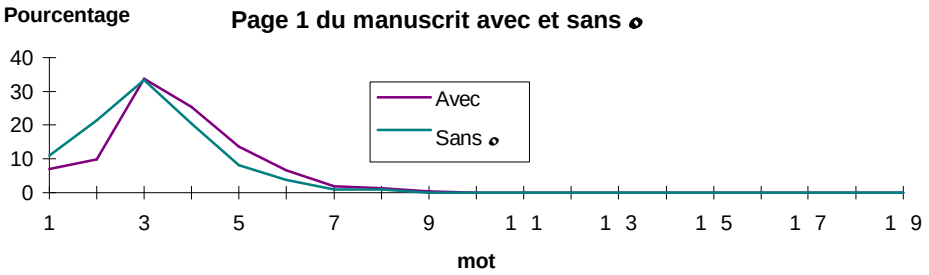
422-§ Mais la suppression de la lettre **[O]** réduit l'effectif des mots de dimensions supérieures en augmentant les effectifs des mots de dimensions inférieures à trois. La lettre **[O]** de cette première page est particulièrement placée (Constat 39) dans des

---

[326] Jean-Marc LEPERS —maître de conférence à l'université PARIS 7 et PARIS 8— décrit l'extrait du folio f69r comme une représentation hexagonale qui oppose le monde du divin au monde terrestre. Le premier triangle est composé des symboles,  ,  , , associés au divin : le est l'infini et représente le créateur, l' est le symbole du poisson chrétien qui décrit l'humain ou le fils du créateur, enfin, la somme des symboles et donne le symbole qui représente l'esprit. Le deuxième triangle est composé des symboles,  ,  , . Ce triangle est certainement la base « chaotique » à partir de laquelle se construisent les symboles ordonnés et divins.

[327] Pourcentages de lettres de la première page : espace(23), **O**(11), **A**(8), **G**(7), **8**(6), **D**(4), **S**(4), **C**(4), **R**(4), **T**(4), **Z**(3), **H**(3), **E**(3), **M**(2), **2**(1), **I**(1), **N**(1), **P**(1), **L**(<1), **F**(<1), **K**(<1) (page 397).

mots d'au moins[328] quatre lettres.



Conclusion 12 La lettre [o] du premier folio a les attributs et le comportement d'une lettre dispensable[329].

[328] Or exceptions.

[329] La suppression d'une lettre dispensable améliore la lisibilité du texte : c'est le cas de la suppression d'une lettre nulle. Par exemple la proposition : *« La suXppresXsion d'uXne letXtre dispenXsable améXliore la lisXibilité dXu tXexte »*, est plus facilement lue, *« La suppression d'une lettre dispensable améliore la lisibilité du texte »*.

•

NOUS AVONS DÉVELOPPÉ L'IDÉE, qui ne demeure que présomption[330], que la faible disparité du second ordre *h2* pourrait provenir d'un système de représentation phonétique ou syllabique. D'une façon générale, nous devons retenir que chaque lettre du manuscrit est peut-être plus porteuse d'information que son simple état de monade alphabétique. En ce sens, chaque lettre risque d'être la représentation plus développée d'une forme textuelle ou phonétique.

423-§ L'abbé TRITHÈME[331] (1462–1516) développa ce type de système mais dans sa forme inverse. Comme dans la séquence *Atbash*, où à *Aleph* correspond *Tau* et *Tau* correspond à *Aleph*, une lettre *A* est substituée par un groupe de mots *Ave Maria*. La forme inverse et réciproque est alors la substitution du groupe de mots *Ave Maria* par la lettre *A*.

424-§ Cette forme de substitution était utilisée dès le treizième siècle sous la forme de langue synthétique proche de celle de Raymond LULLE[332] : bien que la finalité soit différente. Ce principe de substitution fut utilisé pendant les siècles suivants jusqu'à aboutir à l'Espéranto[333]. Entre temps, Athanasius KIRCHER avait lui-même été inspiré par la construction d'une langue synthétique universelle et nous savons que le manuscrit a obligatoirement été écrit avant ses travaux. Raymond LULLE et Athanasius KIRCHER délimitent le segment temporel dans lequel le manuscrit a puisé ses formes ; aussi, si TILTMAN a vu juste[334], il doit exister quelques relations entre les inspirations Lulliennes, Kirchériennes et notre manuscrit.

Combinatoire de lettres Lulliennes

425-§ Raymond LULLE (1233–1316), alors contemporain de Roger BACON (vers 1210–1292), élabora un système de construction linguistique. Le projet développé dans *Ars*

---

330 Hypothèse 19, page 140.

331 *Polygraphia.*

332 Epoque la plus ancienne à laquelle le manuscrit fut hypothétiquement écrit.

333 Proposé au monde pour la première fois en 1887

> *quand le Docteur Lejzer Ludwik ZAMENHOF publia en russe un livre dont le titre était « Langue internationale. Préface et manuel complet » [ECO1994].*

334 Hypothèse 9, page 77, et, Constat 12, page 80.

magna devait permettre de convertir les infidèles [ECO1994].

Principes

426-§ Ce système de langue philosophique parfaite repose sur le principe de la permutation et de l'art combinatoire qui dans son esprit devait déboucher sur une unification culturelle et politique du monde [JERP1989]. Dans ses oeuvres, nous reconnaissons

> *la tradition « platonisante » d'Augustin et d'Anselme, et aussi la logique aristotélicienne, excellente selon* LULLE *pour démontrer, mais impuissante à inventer.*

427-§ Son *Arbre des Sciences* somme dix-huit principes dans ses racines. Neuf d'entre eux sont les *principes absolus et divins* qui définissent l'essence divine[335] à la base de toute création. Toutefois, ces essences ne montrent pas leurs caractères actifs. LULLE supplée à ce manquement par un deuxième groupe d'essences appelées *principes relatifs*[336].

428-§ Elles sont au nombre de neuf et leur finalité est de discerner le principe actif ou inactif des principes absolus.

429-§ La combinatoire de LULLE apparaît dans la communication mutuelle des neuf principes absolus. Le principe *Bonté* et le principe *Grandeur* se combinent en une proposition : l*a bonté est grande* et *la grandeur est bonne*. En tout, soixante-douze combinaisons sont possibles et non quatre-vingt-un car dans la tradition aristotélicienne, il doit être envisageable de trouver un terme moyen entre chaque entité. Ainsi, dire : *la bonté est bonne* n'explique rien pour LULLE. En ce cas, seules les propositions du type : *la grandeur est bonne, la gloire est grande*, représentent un bon syllogisme car elles permettent de mettre en relation les substantifs et les adjectifs des propositions. *Si la grandeur est bonne* et que *la gloire est grande* alors *la gloire est bonne.*

430-§ Il existe neuf *Dignités Divines*[337], il existe neuf lettres[338] représentant ces principes, il existe soixante-douze[339] propositions. Raymond LULLE inscrit ces trente-six liens entre principes dans un cercle autour duquel figurent les neufs lettres qui leurs sont assignées.

---

335 Bonté-Grandeur-Eternité ;Pouvoir-Sagesse-Volonté ;Vertu-Vérité-Gloire.

336 Différence-Concordance-Contrariété ; Commencement-Milieu-Fin ; Majorité-Egalité-Minorité ;

337 Principes absolus.

338 B, C, D, E, F, G, H, I, K.

339 neuf²-neuf=9²-9=72.

431-§ La simplification de la formulation intervient dans cette relation *lettre-principe*. La forme *la grandeur est bonne* se code par le couple de lettres CB. Cette proposition est basée sur les principes absolus dont le caractère actif et inactif se souligne à l'aide des principes justement appelés *actifs*.

432-§ Nous effectuons ce que LULLE appelle : « L'évacuation des chambres », en associant les lettres CB de la proposition aux principes actifs correspondants, ici, « concordance » et « différence ».

433-§ A travers les principes relatifs, la proposition CB revêt maintenant douze propositions : *la différence est concordante, la bonté est différente, la concordance est bonne* et cetera.

434-§ La proposition qui est composée de deux principes est associée à deux questions qui transforment les douze propositions affirmatives en vingt-quatre propositions interrogatives. *La bonté est différente* devient avec l'interrogation *utrum* : *Est-ce que la bonté est différente ?* Ou avec l'interrogation *quid : Pourquoi la bonté est différente ?*

En tout et pour tout, il y a neuf principes absolus, quatre cent trente-deux propositions[340], huit cent soixante-quatre questions[341]. La combinatoire ainsi obtenue est considérable mais elle ne permet pas la justesse du propos.

435-§ La précision de ce sur quoi porte la proposition est construite par l'ajout d'un troisième état aux deux états, substantifs et adjectifs, précédants.

Constat 47 L'ensemble de ces trois états prend la forme d'un système à trois disques concentriques[342] dont chaque disque est pourvu des neuf principes.

436-§ Les deux plus proches du centre sont réservés aux principes absolus et le dernier est dédié aux principes relatifs. Ainsi, la proposition constituée du couple de deux principes absolus, pouvant être interprétée de trente-sept façons[343], est déterminée par le dernier principe du trigramme.

---

340 9(9-1)x($4^{2(\text{car pris deux à deux})}$-4(car une proposition : *la bonté est bonne*, est impossible))/2.

341 9(9-1)x($4^{2(\text{car pris deux à deux})}$-4(car une proposition : *la bonté est bonne*, est impossible)).

342 Le principe des disques concentriques est à la base des systèmes modernes d'encryptages. Le disque de Vogel comportait cinq disques. Il fut cryptanalysé par William F. FRIEDMAN en 1922 dans son ouvrage « The index of coincidence » [FRIE1922]. Pendant la deuxième Guerre, Alan TURING travaillait à la cryptanalyse de la machine allemande ENIGMA dont le principe reposait aussi sur un système de trois ou quatre disques imbriqués.

343 (1 fois le couple+12 propositions avec principes relatifs+24 fois sous formes de questions)=37 fois.

437-§ L'acte le plus important dans cette méthode est introduit par LULLE. Il ajoute une lettre qui n'a pas le sens de principe absolu ni même celui d'un principe relatif.

> **Constat 48 LULLE utilise une lettre, qui n'est ni un principe absolu et ni un principe relatif, il lui donne la fonction intermédiaire qui indique une césure de référence.**

438-§ Sa fonction est celle d'une lettre nulle qui, insérée au trigramme, sépare la combinaison de quatre lettres en une première partie consacrée aux principes absolus et une deuxième partie exprimant le principe relatif. Cette lettre *T* est donc *un artifice mnémonique qui change la référence,*

> *le quadruple BCTC dit Umberto ECO, doit être lu de la façon suivante : b=Bonitas, c=Magnitudo, et donc (puisque le T change la référence...) c=Concordantia,*

et non à nouveau *Magnitudo*. La question correspondante est donnée par la première lettre du quadruple.

> *Par conséquent, BCTC doit être lu comme : si la bonté est grande en ce qu'elle contient en elle-même des choses concordantes*[344].

439-§ La remarque d'Umberto ECO,

> *Ces séries d 'ensembles quadruples sont, à première vue, embarrassantes parce qu'elles semblent contenir des répétitions de lettres*

nous satisfait agréablement, car selon le deuxième principe relatif de LULLE, la « *concordantia* » est grande avec le manuscrit de Voynich. En effet, nous notons sept points de concordances majeures.

Concordances

440-§ L'alphabet de LULLE que nous avons ici utilisé est composé de neuf lettres. Or, nous savons qu'aucune page du manuscrit n'a d'alphabet aussi petit. Dans sa *Dissertatio de arte combinatoria* de 1666, LEIBNIZ se demandait pour quelle raison LULLE s'était arrêté à un nombre aussi restreint d'éléments [ECO1994]. En fait, souligne ECO,

344 Ou « Est-ce que la bonté est grande parce qu'elle contient en elle-même des choses concordantes ? »

Constat 49 LULLE avait proposé des alphabets de dix, seize, douze et vingt principes (Note 356—359).

1- Ces effectifs sont très proches de ceux que nous observons dans le manuscrit ; nous supposons alors qu'il soit possible que l'alphabet ne soit pas limité aux neuf dignités divines.

2- L'insertion d'une lettre mnémonique dans chaque triplet de lettres de LULLE implique que la fréquence de cette lettre « nulle » est proche de la fréquence du caractère espace.

Constat 50 Les lettres [o], [c], [g], [t], [a], [8] ont une fréquence équivalente à celle de l'espace quand nous étudions le manuscrit page par page.

3- Lorsqu'une lettre mnémonique est ajoutée : les triplets de la combinatoire Lullienne se transforment en quadruplés.

Constat 51 La dimension des groupes de lettres se trouve augmentée par l'ajout d'une lettre mnémonique.

441-§ Ce point ne peut nous échapper puisqu'il induit un deuxième effet que nous avons vu dans le chapitre discutant des effectifs en mots.

4- Les mots de trois et quatre lettres sont les plus nombreux parmi l'ensemble des mots présents dans le texte de VOYNICH.

Constat 52 Adéquation entre le rôle nul constaté de la lettre [o] et la dimension des mots.

5- Nous avons étudié l'influence de la lettre **[o]** dans la distribution des mots du manuscrit (Constat 46). Nous avons constaté que sa suppression ne perturbait pas (page 155) la fréquence des mots de trois lettres mais par contre elle réduisait les fréquences des mots de dimension supérieure.

Constat 53 Dans le manuscrit, une proposition s'énonce fréquemment avec trois lettres ; parfois moins, une ou deux lettres suffisent ; parfois plus, de quatre à neuf lettres[345].

442-§ Une proposition est , selon le procédé de LULLE, différemment construite selon le

[345] Les autres cas étant rares (page 409).

nombre de lettres nécessaire à son énonciation. Ainsi, une proposition faite avec une seule lettre prend l'aspect *substantivé* [ECO1994] comme : « B=la bonté », une proposition faite avec deux lettres prend la forme construite du « substantif » complétée par « l'adjectif » : « la bonté est grande ». Puis, et ainsi de suite, trois lettres induisent une construction incluant un « substantif », complété par un « adjectif » précisé avec la conjonction d'un autre « adjectif » : « la bonté est grande et concordante ».

6- La croisade médiatique que Raymond LULLE conduisait dans les cours royales poussait à sa renommé. Il est fort probable que BACON avait quelques idées sur l'*ars magna* et ces principes.

> **Constat 54 Le fait que Roger BACON soit un contemporain de LULLE peut conforter l'idée que BACON se soit, de quelques façons, inspiré de ces méthodes.**

7- La dernière remarque concerne Athanasius KIRCHER. Sa connaissance en ce domaine est évidente. Il traita de la question dans son livre *Ars magna sciendi sive combinatoria*[346].

> **Constat 55 MARCI transmet le manuscrit à KIRCHER qui vient de publier un ouvrage sur un langage universel.**

443-§ Mais KIRCHER n'est pas un contemporain de LULLE puisqu'il vécut entre le seizième siècle et le dix-septième siècle. En 1666, MARCI lui avait écrit et dit de lui, dans la lettre qui accompagnait le manuscrit, qu'il pouvait être le maître des « Sphinx » et seul apte à résoudre l'énigme. Est-ce une coïncidence ou MARCI a-t-il jugé[347] qu'il existait une corrélation entre ce manuscrit et les connaissances de KIRCHER sur l'*Ars magna* ? Le fait est qu'après KIRCHER le manuscrit disparu pendant deux siècles et demi. Etait-il jalousement gardé comme par cet inconnu qui ne laissa s'échapper le manuscrit que parce que la mort l'obligea ? Avait-il résolu cette énigme ? Long silence qui ne fut interrompu que par une sorte de hasard en 1912.

Code alphanumérique de KIRCHER

444-§ KIRCHER s'intéressa au problème de la création d'une langue internationale accessible à tous. Il utilisa le principe de codage par dictionnaire dont il décrivit le fonctionnement dans sa *Polygraphia nova et universalis ex combinatoria arte detecta* de 1663. Selon le père Athanasius KIRCHER, son système n'est pas fait pour dissimuler les

346 Amsterdam 1669.

347 Ou c'est laissé dire par cet inconnu.

secrets, comme il est d'usage pour tous système de codage.

Traduction universelle

445-§ Il propose une méthode de classement alphabétique du vocabulaire. KIRCHER organise son premier dictionnaire[348] de codage en plaçant les vocables[349] de la langue latine dans une première colonne. Les mots sont classés par ordre croissant alphabétique et numérotés[350] en conséquence. Il fait de même pour les autres langues qu'il classe alphabétiquement mais sans numérotations ordonnées. Il adjoint à chaque vocable de langue étrangère le numéro d'indexation de son équivalent latin. A chaque vocable latin, il existe un « équivalent » linguistique dans chaque langue étrangère[351].

446-§ La personne qui désire traduire un mot de sa propre langue utilise le dictionnaire A. Elle repère le mot dans la colonne dédié au vocabulaire de sa langue et récupère le numéro adjoint. Elle transmet ce numéro à son interlocuteur qui utilise le dictionnaire B de décodage. Ce deuxième dictionnaire n'est pas agencé de la même façon que le dictionnaire A. Son organisation s'articule autour de trente-deux tableaux indexés par les chiffres romains du code transmis. Les tableaux contiennent la liste des vocables indexés par les chiffres arabes présents dans la deuxième moitié du code transmis. Contrairement au dictionnaire A les vocables sont arrangés par ligne de synonymes et ordonnés par la colonne des vocables latins.

447-§ Le décodeur prend le code qui lui a été transmis par son interlocuteur. La première partie du code est un nombre romain qui lui indique le numéro de la table qu'il doit consulter. La deuxième partie du code est un nombre arabe qui précise le numéro d'indexation du mot dans la table. Le décodeur trouve alors le vocable latin correspondant au code transmis. Dans le cas où le receveur ne comprend pas le latin ; il découvre sur la même ligne l'ensemble des vocables équivalents en langue italienne, espagnole, française et allemande. Le dictionnaire A est donc un entonnoir qui permet à un étranger, connaissant une des cinq langues référencées, de passer par un code intermédiaire qui ne nécessite pas la connaissance du latin. Le dictionnaire B est l'opposé de l'entonnoir. Il transforme l'unique code en cinq traductions possibles. Ce système de communication n'implique pas que les intervenants parlent la même langue.

---

[348] Il existe deux dictionnaire A et B. Le dictionnaire A est dédié au codage et le dictionnaire B sert au décodage.

[349] Choisis par KIRCHER selon des critères empiriques.

[350] La numérotation est romaine et arabe. La première fait référence à un numéro de tableau auquel il faudra se référer pendant la procédure de décodage ; le deuxième numéro est une numérotation d'ordre.

[351] Le système de KIRCHER prend en compte cinq langues : le latin, l'italien, l'espagnol, le français et l'allemand.

Analogies

448-§ La codification que nous venons d'expliquer est basée sur la structure bipolaire *chiffre romain-chiffre arabe*. Un code est écrit avec sept lettres possibles, I, V, X, L, C, D, M, et dix chiffres possibles de zéro à neuf. En tout, un code est écrit à partir d'un alphabet de dix-sept symboles. La dichotomie entre ces deux types de notations numériques est analogue à celle de Raymond LULLE (Constat 48) qui séparait les *principes absolus* des *principes relatifs* par un caractère qui indique le changement de la référence *absolue* en référence *relative*. Cependant, la langue parfaite de LULLE s 'exprime avec un alphabet de neuf[352] lettres et seule l'introduction de cet *artifice mnémotechnique* permet de distinguer la partie gauche de la partie droite du code.

> **Constat 56 La langue internationale de KIRCHER marque l'opposition entre les références grâce à une représentation numérique romaine par les lettres qui s'oppose à la représentation numérique par les chiffres arabes.**

449-§ TILTMAN avait reconnu (Hypothèse 9) dans le manuscrit de Voynich une tendance non systématique à une structuration tripartite des vocables. Il lui sembla que chaque mot était très remarquablement constitués d'un début, d'un milieu et d'une fin. Il pensa alors que le manuscrit avait été écrit avec un système de langue universelle, très développé au dix-septième siècle, mais dont l'origine remontait au treizième siècle avec la langue parfaite de Raymond LULLE. Toutefois, la non systématisation de cette structure dans le manuscrit ne permettait pas curieusement d'affirmer cette hypothèse, TILTMAN ne semble pas avoir exploré la méthode de KIRCHER qui dans sa première approche montre des codes composés par deux entités *lettre-chiffre*. Seulement, le simple lexique des dictionnaires A et B ne permet pas d'exprimer toutes les propositions de la langue naturelle. Le père Athanasius KIRCHER indique le temps, le mode, les flexions[353] et le nombre verbal, avec quarante-quatre signes particuliers. Umberto ECO nous cite un exemple simplifié de codage :

> *disons que le nominatif est marqué avec une sorte de N et la troisième personne du singulier du passé simple sera notée par nous avec un D alors la proposition, « Petrus noster amicus venit ad nos », s'exprime avec les codes, XXVII.36N XXX.21N II.5N XXIII.8D XXVIII.10 XXX.20*

450-§ on constate que *petrus* se dit avec un code tripartite XXVII.36N, tandis que *nos* s'énonce avec le code bipartite XXX.20.

---

[352] Bien qu'il proposa aussi des alphabets de 10, 12, 16, 20 principes (page 191).

[353] Nominatif, génitif, datif, au singulier et au pluriel.

451-§ Il est encourageant de constater que le système de KIRCHER montre des similitudes de structures avec le manuscrit de Voynich. Nous sommes donc en droit de nous dire que l'adressage de cette énigme par MARCI au père Athanasius KIRCHER n'est probablement pas le fruit d'une coïncidence fortuite. La publication de *Polygraphia nova et universalis ex combinatoria arte detecta* en 1663 serait alors le motif de la lettre de MARCI en 1665–1666. Nous ne sommes pas certains de cette hypothèse. La première publication de 1663 est rare. KIRCHER ne l'avait réservée qu'à quelques personnes haut placées et il a fallu attendre l'année 1680, après la mort de MARCI, pour qu'elle soit plus largement diffusée [BACK1932]. MARCI était un lecteur passionné des travaux de KIRCHER, et KIRCHER considérait MARCI comme un ami. Il est pourtant impossible de savoir si MARCI a obtenu une copie de l'édition de 1663. René ZANDBERGEN souligne que leurs correspondances étaient très peu fréquentes, et réduites à une moyenne de deux lettres par an, entre 1659 et 1665. Toutefois, si la question est : « Est-ce que MARCI connaissait les méthodes de KIRCHER ? », la réponse est que MARCI était convaincu que KIRCHER était le meilleur expert du domaine cryptographique.

452-§ KIRCHER avait la réputation de pouvoir tout déchiffrer et MARCI lui avait déjà envoyé d'autres ouvrages qu'il décrypta avec son « habituel succès » (Lettre de MARCI, page 30) : KIRCHER n'était-il pas celui qui venait de décrypter[354] les hiéroglyphes égyptiens ?

453-§ Nous ne savons pas si Athanasius KIRCHER a pu décoder le manuscrit. Son système de langue universelle est fort dans sa capacité à traduire les langues indépendamment de la connaissance de toute autre langue que celle du receveur. Mais son problème majeur est que la perte du dictionnaire A rend impossible le codage des messages ; plus grave est la perte du dictionnaire B. Lorsqu'un code est reçu, il doit être décodé par l'intermédiaire des tables indexées du dictionnaire B. Il est le seul lien qui restitue le message dans une des cinq langues indexées par KIRCHER. En perdant ce dictionnaire vous perdez tout espoir de traduire les codes en langue naturelle. L'existence d'un tel registre de codes est donc la condition indispensable pour le décodage du système de langue internationale.

454-§ Le manuscrit de Voynich n'est pas complet. Il manque vingt[355] folios. Nous ne savons pas à quelle période ils ont été séparés du manuscrit. Cependant, trois *scenarii* se présentent à nous.

---

[354] KIRCHER étudia les hiéroglyphes et publia un premier ouvrage en 1636 *Prodomus coptes sive Aegyptiacus* qui traita des rapports entre la langue copte et l'égyptien, et entre le copte et le grec. Il considéra que les hiéroglyphes étaient des signes aux valeurs idéographiques ; sa traduction fut donc fausse ; toutefois, ce qui est remarquable dans sa démarche est sa reconstruction de liens entre la langue grecque, copte et égyptienne ; cette idée se matérialisa près de deux siècles après par la découverte de la pierre de Rosette et les travaux de comparaisons de CHAMPOLLION (page 21 & Note 9).

[355] Il manque les folios 12, 59-64, 74, 91-92. L'ensemble représente 40 pages.

455-§ Le premier scénario est que l'hypothèse, que le manuscrit soit le résultat d'une langue synthétique universelle, soit fausse ; permet d'envisager d'autres orientations de recherches qui laissent probable l'aboutissement à une solution.

Hypothèse 25 Le langage n'est pas une combinatoire d'inspiration Lullienne.

456-§ Le deuxième scénario est que l'hypothèse, que le manuscrit eut été écrit avec un système de langue parfaite, soit vraie ; alors

Hypothèse 26 Il doit exister un dictionnaire de traduction *code-mot* (du type « table » ou « cercles »).

457-§ Et, nous savons que le manuscrit contient des « cercles »[356] qui ressemblent à ceux de Raymond LULLE ou bien à ceux de VOGEL. Nous trouvons des ressemblances parce que les « cercles » du manuscrit sont, « concentriques »[357], « sectionnés »[358] et « étiquetés »[359].

458-§ Le troisième scénario est une hypothèse catastrophique qui découle du deuxième scénario. Nous savons qu'il manque vingt folios dans le manuscrit.

Hypothèse 27 Si les folios disparus sont ceux du ou des dictionnaires alors la probabilité de décoder le manuscrit est nulle.

459-§ Les approches que nous ferions dans ce cas ne nous permettraient pas d'affirmer, avec certitudes, nos résultats. Nous nous retrouverions dans le même cas de NEWBOLD tentant de donner de la clarté à un texte transposé que l'on essaye de reconstruire par le procédé anagrammatique.

La diversité des hypothèses, des constats et des rares conclusions, est liée à la problématique du manuscrit. Toutefois, nous avons abouti à des esquisses de solutions qui réduisent le *champ des hypothèses*.

460-§ Nous savons que les substitutions monographiques et digraphiques (Pages 109 et 125)

---

356 Globalement : folios 57v, 67—73, 85—86.

357 De 1 à 4 disques, dont le centre comporte parfois, rien, un bélier, deux poissons, un soleil, un taureau, un capricorne, les gémeaux, le cancer, le lion, la vierge, la balance, le scorpion, le sagittaire. Il manque le folio 74 et la rosette du verseau.

358 De 3, 4, 5, 6, 8, 9, 10, 11, 12, 14, 16, 17, 18, 19, 20 sections.

359 Les sections des cercles sont généralement titrées mais dans la langue de Voynich.

sont désormais très improbables sur l'ensemble du manuscrit.

461-§ Il existe en fait au moins six alphabets qui ont probablement servi à sa rédaction ; seulement, ce que nous ne savons pas est : sont-ils des alphabets de substitutions cryptographiques ou bien sont-ils différemment utilisés en fonction des règles de construction propositionnelle d'un langage synthétique ?

462-§ Nous avons mis en exergue (page 125) l'existence des symboles particuliers qui ne commencent, ne finissent, jamais un mot et participent à la jonction des parties externes des vocables comme TILTMAN avait commencé de l'observer.

463-§ En poursuivant notre étude sur les assemblages de trois lettres nous avons détecté la rareté des trigrammes internes aux mots. Ces trigrammes sont largement représentés par quatre familles ; il y a ceux qui commencent par la lettre **[C]** et ceux qui commencent par la lettre **[Z]** puis **[R]**, **[I]**, et dont les positions dans les mots font penser qu'il existe des positions d'équilibre dépendantes de la diversité des vocables (page 130).

464-§ Le désordre apparent du manuscrit semblait pouvoir être mesuré par les outils de la théorie de l'information ; en fait de solution, nous écopons d'un nouvel embarras (page 135) dont la seule solution paraît résider dans la perception du manuscrit de Voynich comme une transcription phonétique (Hypothèse 19). Seulement, depuis l'expérience du Docteur Leo LEVITOV, nous sommes devenus méfiants *vis à vis* de telles hypothèses.

465-§ En étudiant le manuscrit comme un texte composé de mots (page 145), nous constatons que la diversité des vocables est plus importante quand ces vocables sont occurrents. Dans un certain sens ceci signifie qu'une attention particulière a été portée sur les mots courants, de la même façon que KIRCHER créa son dictionnaire de langue synthétique, c'est-à-dire d'une façon empirique (page 193).

S'agit-il réellement d'un langage synthétique ou bien est-ce que l'auteur a voulu dissimuler ses écrits en insérant des lettres nulles ?

466-§ Le dilemme est que le langage synthétique peut lui aussi user de lettre nulle qu'on appelle artifice mnémotechnique. La problématique de la recherche de cheminement est posée bien que sept concordances (page 191), entre le manuscrit et la langue parfaite de LULLE, plaident pour cette option. Les dessins de « rosettes »[360] accentueraient cette option mais nous sommes très réservés quant au recours à la « relation de sens » entre les figures et le texte.

[360] Cercles concentriques.

467-§ Nous allons donc poursuivre notre étude en recherchant des structures plus à même de nous révéler des indices favorables ou non à nos hypothèses.

468-§ A travers la recherche de motifs nous montrerons comment extraire les indices cryptanalytiques de la représentation multiple en répondant à l'interrogation :

Existe-t-il des règles de constructions internes aux mots du manuscrit ?

469-§ Cette approche locale et limitée aux mots s'étendra à l'ensemble des motifs du manuscrit qui ne seront plus définis comme des vocables mais comme des éléments de base nécessaires à la construction de structures complexes dont les connexions nous renseigneront sur la nature du manuscrit de Voynich.

III

Les structures de motifs

14 novembre 1998 —Première édition

Partie III

Les structures de motifs

•

Sommaire

14 novembre 1998 —Première édition

470-§ Nous exposons que toute séquence de symboles est descriptible par les trois notions que sont *la redondance, la symétrie et l'asymétrie* de motifs [PRAT1940]. Toutes trois sont interdépendantes. La redondance peut s'exprimer à l'intérieur[361] d'un motif symétrique. Un motif symétrique a la capacité d'être une sous partie[362] d'un motif redondant et un motif ni symétrique et ni redondant ne sera qu'asymétrique. En fait, chaque motif est décomposable en d'autres motifs et en cela toute séquence discrète de symboles est décomposable en inclusions de motifs *redondants, symétriques* et *asymétriques*. Ces jeux de construction permettent au cryptanalyste de spéculer sur leurs significations ; que ce soit dans le télégramme de PANIZZARDI ou dans l'analyse du Perse ancien, c'est la reconnaissance de structure de mot qui permit leur décryptage.

471-§ La recherche d'équivalence conduit l'analyste à établir au premier degré une substitution de symbole entre entité cryptée et entité de sens clair. La substitution de CÉSAR en est l'exemple, tout comme la substitution symétrique *Atbash*. Toutefois, notre stratégie de recherche en structures remarquables nécessite un détachement linguistique[363].

472-§ La forte redondance de motifs, soulignée par TILTMAN, nous indique qu'il existe aussi des séquences particulières non répétitives. Nous nous intéressons à la dichotomie entre les parties répétitives et les parties uniques des mots du manuscrit pour mettre en exergue les jeux de constructions de ces mots si réticents à livrer leur signifiant.

[361] Dans le cas ou le motif symétrique est déterminé avant le motif redondant.

[362] Dans le cas ou le motif redondant est recherché avant le motif symétrique.

[363] Pour les raisons qui ont été développées jusqu'ici, entre autres : nous ignorons la langue naturelle sous-jacente et nous ne connaissons pas le procédé cryptographique employé. Nous savons bien évidemment que nous devrons faire appel à des inductions linguistiques mais notre obligation méthodologique est de les retarder au plus tard possible.

•

NOUS CONCEVONS comme évident ce qu'est un motif. Pourtant nous sommes bien empruntés lorsqu'il faut en donner une définition qui soit fidèle à la méthode employée dans la pratique de terrain. Nous entendons différemment le vocable « motif » selon l'endroit où il est prononcé, qui le dit et pourquoi. Le sens le plus simple de « motif » est le déclencheur de l'action. Il est l'élément suffisant qui pousse à agir. En quelques sortes,

Le motif est l'élément porteur d'un minimum d'information pour une information qualitative.

473-§ Le motif détient l'information suffisante comme le cercle[364] est suffisant pour exprimer un cycle où la fin rejoint le début et constitue une représentation cosmographique de l'éternité (page 184). Seulement le motif ne se limite pas au domaine de la représentation graphique. Nous le retrouvons en musique et dans la communication orale [SCIE1998].

474-§ Une étude des capacités d'apprentissage des passereaux pour le chant montre qu'il n'existe pas de distinction réelle entre le passereau « Swamp sparrow » et le passereau « Song sparrow »

pourtant l'isolement acoustique des jeunes passereaux que l'on insère par la suite dans un groupe de passereaux de la même espèce pousse ces individus à communiquer avec les motifs de leur propre espèce à l'exclusion de tout autre motif [MARL1977]. Dans ce *cas le motif caractérise l'espèce* et le « Swamp sparrow » se distingue du « Song sparrow ».

475-§ Continuons cette approche de définition dans le domaine musical hindou. Leur chant traditionnel rãga se compose de phrases mélodiques. A chaque phrase correspond un signal. Le darãmad est une séquence mélodique qui annonce une dastgãh. Ce signal permet de reconnaître les motifs mélodiques. Parmi les dastgãh, il existe des séquences mélodiques qui ont des fonctions particulières comme le dastgãh Râstpandjgâh qui sert de conclusion au chant rãga .

Le motif est un signal mélodique. Il permet d'établir une communication entre les acteurs musicaux.

---

364 Les premiers motifs du cunéiforme s'associaient aux signifiants simplement : deux traits parallèles pour énoncer l'amitié et deux traits qui se croisent pour exprimer la discorde.

476-§ Dans le domaine génétique nous retrouvons des signaux dont le rôle est d'indiquer un début de traduction grâce au codon ATG ou une fin de traduction par les codons TAA, TAG, TGA. La terminologie *signal* se distinguant de *motif* comme si un motif était l'un des constituants du signal. La séquence de bases AATAAA formant un motif n'étant pas suffisante pour constituer le *signal* de la transcription génétique.

477-§ En poésie, les signes, les lettres et les sons répétés constituent l'élément musical ou rythmique de tout texte. La répétition d'un même schéma rythmique conduit à renforcer une impression comme le « Toujours aimer, toujours souffrir, toujours mourir » de Corneille en serait une illustration. Tout comme l'allitération se consomme en poésie comme une friandise.

478-§ Nous retrouvons le vocable *motif* en cristallographie. Au 17ème siècle ROMÉ DE L'ÎSLE constata que les cristaux étaient formés d'un empilement régulier d'une unique structure[365]. Cette structure est variable selon les cristaux mais les résultats de ses observations montraient l'existence de motifs élémentaires propices à la construction de structures plus grandes.

Structure et motif sont apparemment liés par la répétition et la périodicité.

479-§ Les structures élémentaires se retrouvent dans la chimie des polymères. Les macromolécules synthétiques sont constituées par la répétition linéaire d'un même motif. En 1968, le biologiste LINDENMAYER étudiait la croissance des végétaux. Il remarqua qu'une plante se décomposait en structures plus petites qui elles-mêmes se décomposaient en une seule structure élémentaire. La branche d'un arbre était identique à l'arbre lui-même bien qu'il existe une différence de croissance entre ces deux parties semblables [LIND1968]. Les deux structures étaient simplement de niveaux de complexité différents.

Nous savons jusqu'à présent que le motif sert à distinguer les espèces et sert de signal, qu'il détient une information suffisante que sa répétition et sa périodicité décrivent une structure de complexité particulière.

480-§ Nous avons vu différents aspects d'un motif que nous venons de résumer. Nous allons maintenant porter notre regard sur trois cas d'étude de motifs et préciser notre définition[366], le premier de ces cas est représenté par les travaux de Fletcher PRATT

[365] La forme du plus grand cristal étant copiée sur la structure la plus élémentaire de ce cristal. Il existe sept réseaux possibles —cubique, hexagonal, quadratique, rhomboédrique, orthorhombique, monoclinique et triclinique— qu'on appelle les « sept systèmes cristallins ». On remarquera que la « nature » n'admet que les axes de rotation 2, 3, 4 ou 6 dont les figures sont « la bande, le triangle, le carré et l 'hexagone » [LOCH1994].

[366] La recherche de définition est très contextuelle à notre domaine et nous ne tentons pas de définir ce vocable universellement.

sur la reconnaissance de structures internes aux mots de la langue anglaise, le deuxième est un cas historique que l'on nomme *Affaire DREYFUS,* et enfin, le troisième et dernier cas est la résolution du *perse ancien.* Finalement, au terme de ces trois exposés nous apprécions ce que *motif* signifie en cryptanalyse et surtout nous saurons quels sont les indices —ou structures— que nous devrons rechercher dans notre manuscrit.

Motifs particuliers de la langue anglaise

481-§ En 1940, dans son ouvrage traitant de l'histoire de la cryptographie, Fletcher PRATT liste des ensembles de mots qu'il appelle « mots usuels à forme caractéristique en anglais ». Ces mots apparaissent au moins une fois dans un texte normal de 10000 mots et ils sont listés « sans tenir compte éventuellement de leurs dérivés ».

482-§ Il remarque que des mots peuvent posséder une forme facilement reconnaissable comme le participe présent « beGINNING » ou bien « MUseUM ».

483-§ Toutefois, il ne précise pas quels sont ses propres critères permettant de dire que tel mot est plus reconnaissable, par telles ou telles lettres plutôt que, par telles autres lettres. Il nous dit qu'il s'agit avant tout de « mots usuels », c'est-à-dire qu'ils font partie des mots les plus utilisés dans la vie courante.

484-§ Une autre remarque intéressante est la méthode qu'utilise F. PRATT pour catégoriser ces mots « à forme caractéristique », il utilise une codification numérique associée à l'occurrence de chaque lettre. Le mot « beGINNING » voit sa partie reconnaissable « GINNING » codée sous la forme 1233231. Ainsi, si vous découvrez la séquence suivante « be1233231 » dans un texte alors il est très probable, mais pas certain, que le mot correspondant par analogie soit « BEGINNING ». Dans cette liste figurent des formes particulières différentes des autres par leur symétrie parfaite. Le premier groupe est codé par les nombres « 1221 » et est le plus diversifié en nombres de mots distincts. Nous y trouvons par exemple les mots: AFFAir, bAGGAge, ATTAch et puis une grande partie dont la terminaison est « ing » comme: kILLIng, shINNIng, mISSIng. Un autre groupe à forme symétrique est le « 12321 » qui contient des mots comme MAdAM, prECIpICE, LEvEL, REfER. Voici la liste des formes que F. PRATT a établie en fonction de leur nombre.

Forme codée	Nombre	Forme codée	Nombre	Forme codée	Nombre	Forme codée	Nombre	Forme codée	Nombre
1121	14	1212	5	12231	5	12313	1	1234221	1
1121121	**1**	12131	18	122321	1	123132	2	1234412	1
11212	1	12132	2	12311	5	123141	2	1234421	1
1122	2	12133421	1	12312	12	12341	3		
11231	3	121341	2	123122	1	12331	1		
11232	7	121344	1	**123123**	**1**	1233231	1		
11233	5	1213453	1	123142	1	123341	1		
112344	2	**1221**	**43**	1231423	1	123412	6		
1211	2	12212	2	**12321**	**10**	123421	3		

Tableau 8 Liste des motifs de la langue anglaise par Fletcher PRATT.

485-§ Nous synthétisons les critères qui entrent en compte dans la formation de cette liste.

486-§ Le premier critère est l'occurrence, c'est-à-dire le nombre de fois qu'un mot est utilisé sur le nombre total de mots prononcés. Fletcher PRATT l'établit à 1 fois pour 10000. Le mot doit apparaître au moins une fois pour 10000 mots prononcés.

487-§ Le deuxième critère est la redondance de forme que nous trouvons dans le mot « brINGING » : la forme « 123123 » est redondante.

488-§ Le troisième critère considère à la fois la redondance et l'asymétrie comme l'est « poSSESSES » dont la forme codée « 1121121 » est composée de deux répétitions de « 112 » plus « 1 » qui crée l'asymétrie.

489-§ Il y a des mots dont la symétrie est cassée par l'insertion d'une lettre différente, « vIsItIng » en est l'expression.

490-§ Finalement, puisque nous avons déjà cité ci-dessus le cas des formes symétriques, le sixième critère semble être celui qui associe la redondance et l'asymétrie de forme mais avec l'insertion d'au moins une lettre qui rompt la séquence comme « AvAilAble » ou « PREPaRE » tout comme « beGINNING ».

Le motif de « DREYFUS » dans le télégramme de PANIZZARDI

491-§ La cryptologie que nous appelons, plus professionnellement, depuis William F. FRIEDMAN, la cryptanalyse, étudie les documents cryptés avec l'idée qu'il existe des formes reconnaissables qui sont porteuses d'une certaine information. Le cryptologue A. SINKOV que nous avons déjà cité —Méthode de KASISKI— [HODG1988] préconisait de trouver une séquence de symboles à laquelle nous devions associer un mot probable : cette méthode est bien étrange dans un monde si empreint de *sciences* car elle porte le nom « *d'intuition* ». Or comment pourrions-nous discuter de cette méthode ? Peut-être qu'au travers du *télégramme de PANIZZARDI* nous pourrions montrer que l'intuition n'est pas entièrement du domaine de l'irrationnel et que

possédant un minimum d'information il est possible d'être intuitif dans un contexte circonscrit.

492-§ Tout commence le 15 octobre 1894 à 9 heures, le Capitaine DREYFUS est arrêté pour haute trahison[367]. La preuve de son innocence ou de sa culpabilité est dissimulée dans un message codé. Seulement, selon la stratégie de décryptage du télégramme le Capitaine DREYFUS passe du banc des accusés à celui des non coupables.

Le télégramme chiffré de PANIZZARDI

493-§ Le document est une communication chiffrée entre l'attaché militaire PANIZZARDI de l'Ambassade Italienne à Paris et son Etat-major en Italie. Ce message est postérieur à la mise en accusation de DREYFUS et date du 2 novembre 1894.

Figure 18 Télégramme de PANIZZARDI.

[367] Nous passerons sur les pièces du dossier d'accusation tel que le bordereau et les lettres de PANIZZARDI mais nous nous intéressons au télégramme crypté de PANIZZARDI.

494-§ Le service du chiffre français pensa que ce message était important pour l'appréciation de la culpabilité du Capitaine.

Commando stato maggiore Roma
913 44 7836 527 3 88 706 6458 71 18 0288 5715 3716
7567 7943 2107 0018 7606 4891 6165
PANIZZARDI

Figure 19 Télégramme de PANIZZARDI [KAHN1980].

Les traits du cryptogramme

495-§ Nous constatons qu'il existe des caractères d'espacement entre des groupes de nombres. Ce caractère séparateur[368] trahit la structure du code en montrant qu'il existe des groupes de nombres de dimension 1, 2, 3 et 4. Le cryptogramme de PANIZZARDI est un système codique de nombre. Nous appelons ces groupes des *groupes codiques*.

496-§ La méthode cryptographique était inconnue du service du chiffre mais ce système de codage rappelait un système de codage publié la même année par Paolo BARAVELLI sous le titre *Dizionario per corrispondenze in cifra.* Cet ouvrage comportait quatre parties.

- La première chiffrait les voyelles et les signes de ponctuations par des chiffres allant de zéro à neuf.
- La deuxième partie chiffrait les consonnes et les verbes auxiliaires par un bichiffre.
- La troisième partie chiffrait les syllabes.
- La quatrième partie permettait à un groupe de deux bichiffres de chiffrer pour un mot repérable par son numéro de page et de ligne.

497-§ Bien sûr ce système de code pouvait être surchiffré[369]. Lorsque le service du chiffre du Ministère des Affaires Etrangères Français appliquait le code de BARAVELLI au message chiffré, le message clair obtenu restait inintelligible.

L'hypothèse du motif probable

498-§ Les cryptanalystes pensaient que le nom de *DREYFUS* devait figurer dans le cryptogramme [KAHN1980]. En décomposant le nom de *DREYFUS* en unités distinctes *dr, e, y, fus,* afin de les coder par le système de BARAVELLI, ils obtinrent la

[368] Espace entre les groupes de nombres.

[369] Le surchiffrement consiste à appliquer un encryptage sur le cryptogramme ; comme le procédé repose sur un système numérique alors on peut imaginer une multitude de transformations algébriques ou géométriques.

séquence de codes 227 1 98 306. La comparaison entre ce code et celui de PANIZZARDI devait permettre de connaître la différence cryptographique entre ces deux approches. Il fallait donc repérer une séquence de groupes codiques de type 3, 1, 2, 3. Fait heureux, une seule séquence de ce type était présente dans le cryptogramme, elle était composée de la suite de nombres 527 3 88 706.

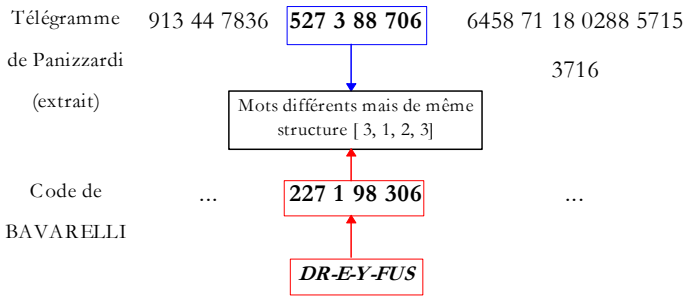


Figure 20 Comparaison entre les deux motifs de DREYFUS

499-§ Fait remarquable, seulement quelques chiffres différaient de la version classique de BARAVELLI. Une grande partie du cryptogramme *DREYFUS* était codée simplement sans surchiffrage ?27 ? ?8 ?06 ce qui indiquait que seuls les numéros de page ainsi que l'ordre des voyelles de la section première avaient dû être modifiés.

500-§ Par cette cryptanalyse, le message décrypté devenait

> *Si le capitaine DREYFUS n'a pas eu de relations avec vous, il serait bon de faire publier par l'ambassadeur un démenti officiel. Notre émissaire prévenu [KAHN1980].*

Stratégie

501-§ Cette dernière partie n'était pas assurément décryptée et la culpabilité de DREYFUS s'affirmait ou s'infirmait par cette dernière phrase. Pour cela, le commandant Pierre-Ernest MATTON rédigea un message, comme un pêcheur dissimule l'hameçon dans un appât attrayant, dont sa structure et le syllabage des noms propres pouvaient être déterminés et difficilement modifiables par le chiffreur. PANIZZARDI communiqua immédiatement ce message sans y apporter de démarquage[370]. Le message chiffré et

[370] Opération qui consiste à réécrire le message dans une autre structure et avec d'autres mots sans en changer la signification.

transmis par PANIZZARDI à son Etat-major confirma après interception[371] du cryptogramme par les agents Français l'exactitude de la dernière hypothèse :

> *Si le capitaine DREYFUS n'a pas eu de relations avec vous, il serait bon de faire publier par l'ambassadeur un démenti officiel pour éviter les commentaires de la presse.*

Structure et motif dans l'étude du Perse ancien

502-§ La cryptanalyse est une science qui s'étudie à travers les siècles. Les grandes découvertes de la cryptologie ne sont pas spontanées. Elles sont le fruit de la perspicacité et de la ténacité d'individus qui ont semé des hypothèses et parcouru des chemins que les descendants n'ont pas eu à traiter. Les résultats de recherches sont récoltés comme une moisson séculaire où chaque individu contribue à la découverte d'un élément de vérité. L'aboutissement se mesurant bien souvent à la somme des travaux de plusieurs générations d'hommes et de femmes.

503-§ L'étude du perse ancien a conduit des archéologues comme Carsten NIEBUHR et son disciple TYCHSEN à consacrer leur vie entière pour des découvertes aussi importantes que succinctes.

Carsten NIEBUHR et le Cunéiforme de Babylone

504-§ Au 18ème siècle, l'archéologue Carsten NIEBUHR étudia les inscriptions rédigées en caractères cunéiformes de Babylone. La première recherche qu'il entreprit fut de distinguer les différents systèmes d'écriture, il en découvrit trois qu'il nomma type I, II et III. Il constata que le seul sens de lecture[372] possible était de gauche à droite.

505-§ Finalement, il établit les statistiques monogrammiques des caractères et mourut. Son élève TYCHSEN poursuivit ces travaux. Il remarqua qu'un signe avait une

---

371 La stratégie de MATTON est encore d'actualité, nos communications sécurisées sont assurées par un algorithme appelé DES pour Data Encryption Standard [DUCL1992]. La particularité de cet algorithme est d'être symétrique, il chiffre et déchiffre avec le même jeux d'instructions. Cette propriété est la complémentation [DAVI1995]. La sécurité des informations chiffrées par le DES dépend de la non compromission de cet algorithme. Dans le cas où il est possible, pour une personne extérieure au système sécurisé, d'accéder au processus de chiffrement, il est concevable de reconstituer la clé de chiffrement à partir des textes chiffrés par cet algorithme. La manipulation habituelle est d'insérer une séquence d'information claire dans le message chiffré intercepté, lorsque ce message est déchiffré, la partie claire du message chiffré devient elle-même chiffrée. Il apparaît alors évident *« d'éviter les attaques à clair choisi, par exemple en contrôlant l'accès à l'exécution de l'algorithme DES »* [DAVI1995].

372 La technique d'écriture avec une calame indique le sens de la lecture. Le sens de lecture du manuscrit est supposé de la même façon selon Jacques GUY. Il doit normalement « se lire » de gauche à droite et de haut en bas pour les raisons suivantes : chaque paragraphe a sa dernière ligne plus courte que les autres, les caractères majuscules, 𐎍, 𐎐 et 𐎓. commencent la première ligne de plusieurs paragraphes et des labels sont souvent placés à gauche du commencement d'un texte (folio 66r).

représentation statistique très au-delà de l'habitude. Avec vingt-cinq pour-cent de l'effectif total, le signe oblique était trop représenté. TYCHSEN avait effectivement émis cette hypothèse par analogie avec les langues connues et il avait constaté que seule la lettre « e » de la langue française était si distincte des autres lettres.

506-§ L'autre fait constaté était l'absence d'espace entre les signes. TYCHSEN pensa qu'il fallait bien qu'il y ait un indicateur exprimant la fin d'un mot et le commencement du mot suivant. Sa conclusion fut que exprima cette séparation.

L'hypothèse de TYCHSEN et la recherche de motif par GROTEFEND

507-§ TYCHSEN avait présumé le caractère espacement, il remarqua la répétition fréquente d'une séquence de signes et il pensa qu'un motif de ces répétitions faisait référence à un roi.

508-§ Pour cela, TYCHSEN rechercha à établir un lien entre le document de l'ancienne Perse et la possible nomination d'un Roi. Suite à une déduction, il supposa que ce roi devait être Arsace. Malheureusement ce système ne permit pas de décrypter ce langage. En effet, TYCHSEN se trompait dans la datation de l'écriture type I.

509-§ Quelques années après la mort de TYCHSEN, l'opiniâtre Georges Frédéric GROTEFEND reprit les travaux de ses prédécesseurs. Il conserva l'hypothèse que indiquait un caractère séparateur mais il n'était pas d'accord avec la datation de TYCHSEN. En effet, GROTEFEND constata que les trois types apparaissaient sur une même tablette d'argile, il en conclut que ces trois types ne pouvaient qu'être de la même époque[373], et qu'alors, la période d'écriture correspondait à celle où les trois[374] langues étaient parlées en même temps.

510-§ Heureusement, comme dans l'analogie entre le cryptogramme présumé de DREYFUS et son cryptogramme surchiffré, une seule période prétendait à cette hypothèse : la période de l'empire persan où les Mèdes, les Perses et les Babyloniens étaient à peu près sur un pied d'égalité [PRAT1940].

[373] L'écriture sur tablette d'argile est figée dans le temps par la cuisson de l'argile dans un four. Il n'est pas possible de recueillir des écrits de différentes époques sur une même tablette.

[374] Il est remarquable que le décryptement repose sur une coïncidence analogue à celle du décryptement des hiéroglyphes. Ici, la tablette contient trois langues (Figure 21) : ancien perse, babylonien et élanite ; la pierre de Rosette contient : le grec, le copte et l'écriture hiéroglyphique.

Figure 21 Tablette réunissant l'ancien Perse à gauche, le babylonien au centre et l'élamite à droite [JEAN1987].

511-§ GROTEFEND rechercha le «*mot probable*» que TYCHSEN avait déduit mais avec la différence qu'il considéra les trois formes de la terminologie « roi ».

Il y avait la forme courte « roi » , la forme longue « des rois » et le mot redoublé « roi des rois ».

Fletcher PRATT souligne que ce choix n'était pas fait au hasard, *« le mot probable n'est jamais purement arbitraire »* car à cette époque il était courant chez les rois sassanides[375], postérieurs à l'ancienne Perse, de porter le titre *« roi des rois »*.

512-§ La troisième[376] hypothèse soumettait l'idée que la structure de rédaction des tablettes devait être similaire à celle de l'époque médiévale.

Deux textes commençaient par une référence de même structure. L'une disait : *X---------, roi des rois, fils de Y, roi des rois--------*, et la deuxième disait : *Z----------, roi des rois, fils de X, roi des rois--------*. La filiation des rois était connue bien que l'ancienne langue soit perdue,

[375] Epoque médiévale.

[376] La première étant le caractère espace et la deuxième concerne les mots probables.

il était alors possible de retrouver le *X* commun aux deux structures et d'en déterminer le très bon syllogisme de *Y* et *Z*.

513-§ GROTEFEND découvrit une quinzaine de lettres et leurs prononciations phonétiques. Vingt-cinq années après sa mort, il fut possible de lire phonétiquement l'ancien perse.

Implications méthodologiques

514-§ Nous avons vu que la résolution du cryptogramme de *DREYFUS* et de l'ancien Perse se faisait en trois étapes. La première consistait à trouver le signe séparateur qui indique où commence et où finit un mot. La deuxième est la recherche d'une certaine analogie de structure entre ce que nous connaissons et ce qui a pu être utilisé[377]. Dans le cas présent, il fallait trouver la structure *-X roi des rois, fils de Y roi des rois* - dans l'autre cas, il fallait juxtaposer les deux suites : **527 3 88 706** et **227 1 98 306,** reconnaissables[378] sous le nom de DREYFUS. La troisième étape consistant à associer chaque unité chiffrée, lettre, signe, à une unité claire et intelligible.

515-§ Le vocable *motif* est à multiples facettes ; qu'il soit le motif qui se lie à la raison ou celui qui décrit une structure de complexité particulière, il est toujours celui qui permet d'établir, une *concordance*, une *contrariété*, une *différence* des éléments du monde perçu.

> **En cryptanalyse, le motif est celui qui distingue une séquence d'éléments parmi un désordre apparent : –il révèle les traits du cryptogramme; il est le signal d'une information suffisante pour orienter la méthodologie d'analyse suivante, il caractérise le genre et la nature de la méthode d'encryptage : –code de BARAVELLI, qui se confirme à travers le jeux d'imbrications de ce signal dans des structures plus complexes de motifs : –filiation royale dans le Perse ancien.**

516-§ Parallèlement à l'étude du Cunéiforme de Babylone ; dans le manuscrit de Voynich, le caractère espace est un séparateur de mots. Seulement, est-il le seul représentant de sa condition ?

> **Existe-t-il un caractère, analogue à ce trait incliné cunéiforme, qui indique une séparation supplémentaire à celle du caractère espace ?**

[377] Implication de la notion temporelle : celle du manuscrit reste à déterminer.

[378] Seule l'expérience de MATTON a pu confirmer cette analogie.

517-§ Car si nous prolongeons l'idée que ce manuscrit est écrit avec un système de langue parfaite alors nous imaginons qu'il existe d'autres caractères séparateurs[379] inclus dans les mots du manuscrit.

518-§ Raymond LULLE utilisait la lettre « T » pour séparer deux modes de représentations sémantiques (page 187). Au dix-septième siècle, Cave BECK usait d'un système plus complexe où un mot est séparé en deux groupes de quatre chiffres et trois lettres par les lettres « S » ou « T » (page 80). Athanasius KIRCHER marquait la distinction entre codes grâce à deux systèmes différents de représentations graphiques : l'un utilisant les chiffres arabes et l'autre les chiffres romains (page 193). Seulement, nous n'avons jusqu'alors que les conclusions de TILTMAN ; elles énoncent que les mots du manuscrit apparaissent avec des structures à la fois remarquables et illogiques. TILTMAN lista[380] les racines des mots et leurs suffixes [TILT1951] mais aucune règle n'avait été mise en exergue.

La difficulté est la suivante : il nous faut trouver une analogie de structure de mots entre ce que nous connaissons des langues cryptées ou parfaites, et le manuscrit.

519-§ Or, nous n'avons aucune certitude quant à la nature des langages utilisés dans le manuscrit ; nous avons même des doutes sur la datation des écrits et nous avons une totale ignorance du ou des sujets qui y sont discutés : pour résumer, nous ne possédons comme certitude[381] que les lettres du manuscrit.

520-§ Nous allons donc utiliser une méthode particulière qui met en évidence la représentation multiple des caractères d'un texte et la structure de formation des vocables du texte sans aborder quelque corrélation avec les langues naturelles.

[379] Artifice mnémotechnique (page 187).

[380] Nous vous proposons de consulter la figure 27 de la page 105 de l'étude de Maria d'Império [IMPE1980].

[381] Tout compte fait des erreurs possibles de transcriptions.

•

LA TRANSCRIPTION, l'entropie *h2* et les constats des pages 191–193, sont autant de raisons qui nous poussent à penser que le manuscrit est porteur d'une représentation multiple.

521-§ La transformation des écrits du manuscrit en séquences de lettres a pour conséquence de générer une séquence de lettres polysubstituées. La raison est que la *perception holistique* des symboles du manuscrit par le lecteur risque d'être différente de celle de l'auteur[382]. Des mots qui sont normalement identiques deviennent différents parce qu'un ou plusieurs symboles ont été faussement[383] transcrits : NEWBOLD avait commis des erreurs d'interprétation en confondant des taches d'encre avec des signes ; par la suite le groupe de FRIEDMAN réalisa sa transcription qui ne fut pas parfaite aux yeux de CURRIER. Il existe donc des lettres qui sont à représentations multiples par erreur.

522-§ La forte redondance décrite par *h2* (page 139) laisse penser que la substitution multiple en est la cause et qu'elle serait basée sur des représentations de formes multiples des chiffres (page 72) et [TILT1951].

523-§ L'hypothèse formulant que le langage écrit du manuscrit soit un langage synthétique implique que les structures soient occurrentes et parfois différentes d'un seul élément comme : le substantif, l'adjectif, le verbe ou un autre signe particulier.

Représentations multiples

524-§ En premier lieu nous déterminons la famille représentative des caractères les plus courants de la ponctuation. Il ne s'agit pas de découvrir tous les signes mais simplement ceux qui interviennent dans l'énumération n-grammique. Autrement dit, le caractère essentiel est celui qui exprime l'espace. Le plus courant, le caractère d'espacement doit permettre de découper le texte en une séquence de mots.

525-§ Habituellement, l'espace est détectable selon trois critères. Le premier de ceux-ci est la représentativité statistique[384], le deuxième est la valeur de l'écart-carré [CASA1994], le

---

[382] Cf. Note 137.

[383] En fait, toute la responsabilité ne repose pas sur l'analyste qui bien souvent doit se contenter de copies de qualités moyennes.

[384] L'espace est un des caractères les mieux représentés.

troisième est l'incidence de la répartition[385] des espaces sur le découpage du texte en une séquence de n-grammes [KASI1863]. En conjuguant ces trois axes de recherche nous déterminons le caractère essentiel de la régularité textuelle[386]. Sa découverte nous permet d'apprécier la distribution graphique[387] des n-grammes en fonction de leur nombre.

Non-coïncidences

526-§ Maintenant, le code chiffrant l'espacement est présumé. Nous analysons les mots dont les lettres ont été polysubstituées[388].

527-§ Nous listons dans un ordre quelconque tous les mots[389] du manuscrit. Toutes les occurrences de mots sont supprimées : il ne reste que les vocables diversifiés.

528-§ Nous calculons la soustraction, entre la longueur des vocables de même dimension et leur *distance de Hamming,* qui représente la non-coïncidence[390] entre vocables. Ces coïncidences montrent que le nombre de lettres de chaque mot influence le

---

385 La présence de la cuvette 5,6,7-gramme peut confirmer que la répartition des mots est correcte et qu'alors les caractères 'espacements' ont bien été découvert. Si l'asymptote est inférieure à x=6 alors il existe au moins un code découvert erroné. Si l'asymptote est supérieure à x=6 alors il reste à découvrir d'autre(s) code(s) symbolisant l'espace, rien ne confirmant l'exactitude des découvertes.

386 L'espace est inéluctable.

387 Cf. Annexe, Les mots et leurs fréquences, page 409.

388 Prenons par exemple la correspondance de polysubstitution placée dans la présente colonne droite. A la lettre claire 'G' peut correspondre trois lettres: 'a', 'b' ou 'c'.

Nous pouvons écrire le mot 'GEDEON' de 3x4x5x3x5=900 façons différentes, AFKRU en étant une première, BFLSV en étant une seconde. En ce sens, l'ensemble des cas est représenté par le segment Seg(gedeon)=[AFKRU,CJQTY].

G → { a ∨ b ∨ c }
E → { f ∨ h ∨ i ∨ j }
D → { k ∨ l ∨ m ∨ p ∨ q }
O → { r ∨ s ∨ t }
N → { u ∨ v ∨ w ∨ x ∨ y }

389 Nous découpons le texte en mots de dimension fixe lorsque le caractère séparateur n'est pas connu.

390 Par exemple, si M1='AFKRU' et M2='CJQTY' alors Cm(1,2)=∅, c'est-à-dire que les mots M1 et M2 ne peuvent être considérés comme un même et unique mot.

	M1	M2	Mn-1
M1	-	-	-
M2	Cm(1,2)	-	-
Mn-1	Cm(1,Mn-1)	Cm(2,Mn-1)	-
Mn	Cm(1,Mn)	Cm(2,Mn)	Cm(Mn-1,Mn)

Toutefois, la certitude n'est pas établie. Dans ce cas nous ne pouvons que rejeter temporairement cet axe de recherche. Considérons un autre cas. Si M1='AFKRU' et M2='AFLRU' alors nous constatons que l'intersection des deux ensembles de codes est non nulle.

comparatisme par analogie. Quand un mot est de petite dimension[391], il n'offre pas beaucoup de combinaisons, il reste difficile de déterminer sa composition et ce uniquement par induction. Quand un mot est de grande taille sa combinatoire est importante mais sa composition monogrammique[392] est moins compliquée à déterminer du fait même que sa grandeur implique sa rareté. Remarquons que les monogrammes et les digrammes sont très peu diversifiés mais extrêmement nombreux[393]. Leur présence tend à être équiprobable et difficile à discerner.

529-§ Les mots de sept lettres[394] offrent un maximum de diversité quand il s'agit de la langue anglaise (Figure 38). Tandis que les mots répartis autour de ce *mode statistique* ont une diversité diminué. La probabilité de l'événement *n*-grammique pour *n* tendant vers un est équiprobable ; tandis que pour *n* tendant vers l'infini : la probabilité *n*-grammique est univoque. Ceci confirmant deux points importants:

les mots de dimension infinie sont déterminables mais leur rareté offre peu de découverte sur l'ensemble d'un texte.

De même, le surnombre des mots de petites dimensions les rend difficilement opposables entre eux.

530-§ Le langage et l'écriture sont liés à l'unité de temps. Au discours posé s'associe le mot recherché qui se trouve être moins courant. Aux ordres et au démonstratif s'accordent les mots courts [WITT1961]. La fréquence d'utilisation des mots de longueur *n*-grammique est dépendante[395] de *n* [PIER1966], la diversité des mots employés est fonction de *n*. Nos recherches sont donc orientées par la variabilité[396] de *n*.

531-§ A l'issue des recherches en coïncidence et non coïncidence nous ne connaissons pas les lettres claires[397]. Mais nous connaissons les codes qui expriment la même unité alphabétique. En effet, *la coïncidence se détermine sans la connaissance de la langue de*

391 Au moins digrammique (2 symboles, 2 lettres).

392 Monogramme, un symbole, une lettre, une entité.

393 Cf. Annexe, Les mots et leurs fréquences, page 409.

394 Les mots de cinq lettres sont les plus diversifiés dans le manuscrit de Voynich.

395 Cf. Page 147.

396 Précisons cette dépendance : une non coïncidence de un sur un bigramme n'a pas la même implication qu'une non coïncidence de un sur un décagramme. Dans le premier cas, le rapport de la non coïncidence par la coïncidence est de 1/1; dans le deuxième cas, le rapport est de 1/9. Autant on peut être sceptique sur l'interprétation d'un taux de un, autant un rapport de 1/9 est sujet à une interprétation inductive sur l'élément de coïncidant pas.

397 Lettres ayant un sens linguistique dans la langue naturelle considérée.

rédaction[398], elle a de ce fait la prétention de regrouper des symboles en familles de symboles. Nous n'avons donc pas à assumer, à ce niveau, des règles inductives de linguistique [CHOM1957]. Chaque famille de codes décrit une substitution de symbole par de multiples symboles. L'ensemble des familles constituent le dictionnaire de la substitution à représentations multiples[399].

Dictionnaire

532-§ Ce dictionnaire[400] associe une suite de codes à une lettre dite *lettre découverte*. Cette relation est une surjection. Prenons par exemple le mot *researΔh ;* notre hypothèse première est que Δ[401] est la lettre « c ». Nous utilisons pour cela trois règles principales pour intégrer et contrôler notre hypothèse.

La première règle est un contrôle de présence

> **si le code Δ est déjà présent dans le dictionnaire des codes ldy_P et si il n'y a pas de conflit notable alors ldy peut être la lettre « c ».**

La deuxième règle dit que

> **si le code Δ n'est pas présent dans ldy_P mais que la lettre « c » est déjà reconnue comme étant ldy alors on ajoute le code Δ à la famille de ldy, c'est-à-dire que $ldy_{P+1} = Δ$.**

La troisième des règles énonce que

> **si le code Δ n'est pas présent et que ldy n'est pas la lettre « c » alors on ajoute une nouvelle famille ldz dont le premier code ldz_0 est Δ: ldz → [$(code\ ldz)_0$]=« c »[402].**

533-§ L'application de cette méthode[403] sur le manuscrit de Voynich révèle deux résultats fondamentaux.

---

398 Nous avons expliqué cette méthodologie à travers le nombre de coïncidence de FRIEDMAN et de son indice de coïncidence (page 168 et note 290).

399 Applicable aussi aux polysubstitutions.

400 On dit qu'un symbole s'exprime de façons différentes et nous écrivons cet état comme suit: ld0 → [(code ld0)0 , (code ld0)1 , ... (code ld0)N]. La lettre découverte ld0 s'exprime dans le texte avec les codes ld0N. Si nous continuons, la lettre découverte ld1 s'écrit dans la relation: ld1 → [(code ld1)0 , (code ld1)1 , ... (code ld1)M], et ainsi de suite, ldy → [(code ldy)0 , (code ldy)1 , ... (code ldy)P].

401 Δ est le symbole d'une variable que l'on appelle « Delta » (lettre grecque).

402 Nous ne sommes pas contraints de spécifier la lettre claire tant que la langue sous-jacente n'est pas connue.

La recherche des non-coïncidences entre vocables de même dimension montre qu'il existe une structure remarquable pour chaque vocable. La structure d'un mot de trois lettres est analogue à celle d'un mot de quatre lettres, et ainsi de suite, le mot de sept lettres a une structure analogue à un mot de huit lettres.

	1	2	3	4	5	6	7	8
3)	1229	654	996					
4)	2173	1547	975	1388				
5)	2094	1096	1292	784	1189			
6)	784	521	614	517	364	508		
7)	224	117	199	144	100	106	119	
8)	14	6	21	15	14	14	6	11

Nous traduisons le tableau en suites d'inégalités qui se lisent de la façon suivante ; pour un mot de trois lettres : une première lettre est plus substituée que la deuxième qui elle-même est moins substituée que la troisième lettre.

3	<	1	>	2	<	3									
4	<	1	>	2	>	3	<	4							
5	<	1	>	2	<	3	>	4	<	5					
6	<	1	>	2	<	3	>	4	>	5	<	6			
7	<	1	>	2	<	3	>	4	>	5	≅	6	<	7	
8	<	1	>	2	<	3	>	4	>	5	≅	6	>	7	<	8

Figure 22 Structures des mots du manuscrit d'après leurs substituants.

534-§ Le manuscrit offre des vocables dont les structures sont ordonnées. La constitution des vocables[404] de trois, quatre,.., huit lettres montre quatre comportements.

- La première lettre d'un vocable est la plus substituée. Elle représente l'effectif le plus important des différentes positions.

- La troisième lettre est la deuxième lettre à être la plus substituée quand elle n'occupe pas l'avant dernière position du vocable.

- La dernière position est systématiquement plus substituée que l 'avant dernière lettre du vocable.

- En terme de stabilité, l'avant dernière position est la plus stable parce qu'elle est constamment inférieure à la dernière position ; elle est suivie de la deuxième position qui n'est supérieure à la troisième position que dans le cas d'un mot de

[403] Nous recueillons les non-coïncidences égales à l'unité, c'est-à-dire, les vocables de même dimension ne diffèrent que d'une seule lettre. Les vocables retenus ont une dimension au moins égale à trois lettres.

[404] Sauf celui de neuf lettres ; seuls deux vocables sont présents et c'est insuffisant pour mettre en évidence la structure.

quatre lettres. Les positions qui suivent la troisième lettre sont croissantes mais stables[405].

535-§ Nous résumons la structure en indiquant l'ordre dans lequel s'effectue la substitution.

Position	P1	P2	P3	P4	Pn-x	Pn-x+1	Pn-x+k	Pn
Ordre	1	3	2	4	n-x	n-x+1	n	n-x+k

Cette structure est très ordonnée, Jacques GUY avoue qu'il s'attendait plutôt à une alternance —en partie équilibrée— des positions de substitution de sorte qu'au lieu d'avoir : 1 > 2 < 3 > 4 > 5 > 6> 7 < 8, on aurait : 1 > 2 < 3 > 4 < 5 > 6 < 7 > 8., *comme dans le Fidjien* précise-t-il. Le paradoxe est l'inversion des positions de substitution. Nous devrions nous attendre à ce que les dernières positions soient les plus substituées, or, ici, c'est le contraire[406] et l'hypothèse serait alors que sa cause soit liée à une notation phonétique[407] des symboles de VOYNICH.

536-§ La deuxième observation, basée sur l'hypothèse de la substitution à représentations multiples, est qu'une seule famille[408] de codes est constituée. Les codes sont donc tous interdépendants. Ils possèdent tous un code moyen qui les connecte. La tradition aristotélicienne est respectée. En effet, quand un code B se substitue à un autre code A et que ce code B se substitue à un autre code C ; alors les codes A et C sont des substituants identiques. Ce bon syllogisme Lullien[409] montre des substitutions multiples cycliques :

> **Conclusion 13 Il n'existe pas plus d'une famille de codes à représentations multiples sur l 'ensemble du manuscrit.**

537-§ Par contre, l'étude locale page après page met en évidence des représentations multiples et une interdépendance entre structures de mots.

538-§ L'utilisation de systèmes de substitutions à représentations multiples crée des connexions ou des coïncidences entre les alphabets de substitution. L'étude globale d'un manuscrit soumis à ces types de systèmes ne permet pas de dégager chacun des alphabets.

---

405 Il existe une légère contradiction de l'ordre de six millièmes à la sixième position de substitution du mot de sept lettres.

406 Cette contrariété crée un doute sur le sens réel de lecture du manuscrit. Le sens est présumé être comme celui révélé par sa forme écrite ; c'est-à-dire de haut en bas et de gauche à droite.

407 Jacques GUY fait remarquer que si la dernière lettre est de haute fréquence alors on peut présumer qu'elle soit probablement une voyelle plutôt qu'une consonne comme dans la langue grecque.

408 **[2, 4, 8, A, C, D, E, F, G, H, I, K, L, M, N, O, P, Q, R, S, T, Z]**, soit vingt et une lettres.

409 Combinatoire de lettres Lulliennes, page 187 et Note 65.

539-§ Lorsque nous effectuons une recherche locale, page après page, nous remarquons qu'il existe une multitude d'alphabets de substitution que nous devons relativiser par rapport à la substitution naturelle[410] des lettres d'un langage non crypté.

Constat 57 Il existe cinq[411] types de dictionnaires de substitution. Ils sont constitués de une à cinq familles de lettres[412].

540-§ Les pages 5 et 89 du manuscrit sont pourvues de cinq familles de lettres de substitution qui sont relativement proches.

Page 005	Page 089	Distance de Hamming
G O A	**G O**	2
C T S 4	**C T**	2
D P H	**D P S**	2
K R E	**K R M**	2
8 2	**8 4**	1

541-§ Tandis que la page 1 contient de nombreuses non-coïncidences interdépendantes et réunies dans une seule famille[413] : **[N, M, L, R, E, S, 2, T, C, Z, A, D, 8, H, G, O, P, F],** ce qui signifie que la page 1 est source d'une grande diversité de vocables.

542-§ Entre les deux cas de ci-dessus nous trouvons les dictionnaires contenant de deux à quatre familles de lettres. Le dictionnaire[414] de la page 24 se décompose en quatre familles qui sont proches de celles de la page 5 et de la page 89. Cependant, la page 24 est plus familière de la page 5 que de la page 89.

Page 005	Page 024	Distance de Hamming
G O A	**G O A**	3
C T S 4	**T S**	2
D P H	**D 4 H**	2
K R E	**E 8 R**	1
8 2		

Page 089	Page 024	Distance de Hamming
G O	**G O A**	2
C T	**T S**	1
D P S	**D 4 H**	1
K R M	**E 8 R**	1
8 4		

543-§ La similitude entre familles de lettres positionne la page 24 à proximité de la page 5 ; tandis que la page 89 est éloignée de la page 24 et très similaire à la page 5. Les pages 24 et 89 sont opposées par rapport à un centre commun occupé par la page 5.

410 Le texte latin *Apologia Apuleii* possède cinq familles de substitution. La première famille se compose des signes ponctuants. La deuxième famille a quatre lettres {s, S, t, m}, la suivante est uniquement composée de voyelles {e, u, i}, puis du groupe {n, p} et finalement {c, C}.

411 51 dictionnaires d'une seule famille de lettres, 73 dictionnaires de deux familles de lettres, 55 dictionnaires de trois familles de lettres, 16 dictionnaires de quatre familles de lettres et 2 dictionnaires de cinq familles de lettres.

412 Cf. Annexe, page 364.

413 N M L R E S 2 T C Z A D 8 H G O P F (First Study Group).

414 Rappel : un dictionnaire est une réunion de familles de représentations multiples.

544-§ Le deuxième point concerne les alphabets de substitutions en fonction des positions dans le vocable. La méthode révèle une caractéristique de diversité des familles en fonction de la dimension et de la position des substitutions dans le vocable.

545-§ Les similitudes entre alphabets de substitution en première position des mots d'une même page sont grandes et dans la plupart des cas la diversité de ces alphabets est décroissante.

546-§ La position *Pi* du mot de dimension *d* a un alphabet de non-coïncidence formé à partir de l'alphabet de non-coïncidence du mot précédant de dimension *d-1*. Toutefois, la position *Pi* voit son alphabet systématiquement complété par des lettres n'appartenant pas à *Pi-1* du mot *d-1*.

547-§ La page 228 a les familles de lettres suivantes que nous classons en fonction de la dimension du vocable étudié et de la position de la substitution :

3-grammes	
P1	**2 8 A C D E G H O P R S T**
P2	**2 8 A C D E H O P**
P3	**2 8 A C E G M N O R**
4-grammes	
P1	**4 8 D E G H O P R S T**
P2	**A C D H O R**
P3	**2 8 A C D H O R S**
P4	**2 8 E G K M O R**

5-grammes	
P1	**2 4 8 D E G H O R S T**
P2	**C D H O S T**
P3	**2 8 C D H O P T**
P4	**8 C D T Z**
P5	**2 8 E G K M O R**
6-grammes	
P1	**4 D E H O P S T**
P2	**A D F H O P**
P3	**8 C D E H P S T**
P4	**C O T**
P5	**8 C T**
P6	**2 E G O R**

Figure 23 Alphabets de substitutions par n-grammes et par position.

548-§ La page 228 est composée de vocables de dimension maximale égale à six lettres et ayant au moins et au plus une non-coïncidence. Chaque mot de dimension *d* possède *Pd* positions de substitutions. Un mot de trois lettres aura au mieux trois positions de substitutions.

549-§ Les premiers vocables référencés ont une dimension de trois lettres. La famille de lettres en première position *P1* du mot de quatre lettres se compose à partir de lettres de la première famille du mot de trois lettres plus le symbole **[4]** . En procédant par le même raisonnement, nous disons que la famille de lettres en première position *P1* du mot de cinq lettres se compose aussi des lettres de la première famille du mot de quatre lettres plus le symbole **[2]** . De même, la famille de lettres en position *P1* du mot de six lettres se compose des lettres de la première famille du mot de cinq lettres.

Conclusion 14 Les positions *P1* des vocables sont liées par la nature des familles de substitutions et permettent de dire qu'il existe une cohésion entre les vocables des pages prises une à une.

550-§ Ce phénomène d'inclusion nous dit aussi que la diversité des vocables diminue quand la dimension des mots grandit (Constat 36) mais elle n'est pas systématiquement[415] constatée pour toutes les pages du manuscrit ; ainsi dans la page 229, les vocables de cinq lettres sont autant diversifiés que les vocables de trois lettres.

Les premières positions *P1* des différents vocables sont liés. Qu'en est-il des autres positions ?

551-§ Le schéma qui ressort (Figure 23) décrit une relation entre les alphabets aux positions *Pi* des mot *Mi* avec les alphabets aux positions *Pi-1* des mots *Mi-1*.

552-§ La famille de substitution en deuxième position du mot de quatre lettres se constitue à partir des lettres de la famille de substitution en première position du mot de trois lettres.

553-§ Par ce même raisonnement, la famille de lettres en troisième position du mot de cinq lettres se forme à partir des lettres de la famille de substitution en deuxième position du mot de quatre lettres ; plus les lettres **[2], [8], [P], [T]**.

554-§ Puis, la famille de lettres en quatrième position du mot de six lettres se crée à partir des lettres de la famille de substitution en troisième position du mot de cinq lettres.

Conclusion 15 Un alphabet de substitution, pour une position *Pi* d'un mot *Mi,* se crée à partir de l'alphabet de substitution du mot *Mi-1* à la position *Pi-1*.

555-§ Les inclusions et la diversité de lettres aux différentes positions des mots corroborent la structure que nous avons mis en évidence (Figure 22). Et surtout, la représentation fonctionnelle de la Conclusion 15 donne un aspect stratifié qu'on retrouve dans les cercles concentriques.

556-§ La première position est la plus diversifiée ; elle laisse une grande liberté pour « commencer »[416] le mot. La deuxième position du mot est moins diversifiée que la première ; elle réduit les possibilités de construction. La troisième position devient beaucoup plus libre que la deuxième position ; elle s'octroie plus de possibilités dans

[415] L'approche locale, page par page, montre des comportements non vérifiés à l'échelle du manuscrit.

[416] Devons-nous en conclure que le décalage à l'origine de l'encryptage se fait à partir de la première lettre du mot ?

la substitution multiple. Ces trois positions de substitution respectent la structure trigrammique *1>2<3*. Cette règle est respectée quelque soit la dimension du mot[417]. La quatrième position est plus diversifiée que la position précédente quand le mot est de quatre lettres ; sinon, elle est moins diversifiée que la troisième position. De même, la cinquième position est plus diversifiée que la quatrième position quand le mot est de cinq lettres ; sinon, elle est moins diversifiée que la quatrième position : il en est de même pour tous les mots.

Conclusion 16 Quand une position *n* est au moins égale à 4, elle est plus diversifié que la position *n-1* si le mot est de *n* lettres ; sinon, elle est moins diversifiée que la position *n-1*.

557-§ Il existe une relation causale entre la diversité de la substitution multiple de positions et les effectifs de chaque position substituée. La diversité est ici la source du nombre.

558-§ La diversité des substitutions est inégale selon les positions. La première position offre une grande diversité qui se trouve réduite en deuxième position ; la deuxième position offre une diversité réduite qui augmente en troisième position, puis la diversité est à nouveau réduite pour les positions suivantes, exceptée la dernière position qui offre à nouveau une diversité croissante.

559-§ Les alphabets de la substitution de positions sont construits selon les deux règles citées en Conclusion 15 et Conclusion 16.

560-§ Nous avons décrit une structure de motifs limitée par le mot, inscrit dans le texte, circonscrit par les caractères séparateurs. Maintenant, nous allons étudier les structures de motifs indépendamment des mots du manuscrit en considérant la totalité du texte comme une séquence de caractères ; les *a priori* que l'espace, la fin d'une ligne, et la fin d'un paragraphe sont les bornes qui circonscrivent ce qui est à étudier disparaissent pour laisser place à l'étude d'une séquence unique dans laquelle nous allons rechercher des constructions de motifs.

[417] Toutefois, nous remarquons que les mots de quatre lettres adoptent quelques fois une autre attitude : la diversité des lettres de substitution par position étant décroissante.

•

LES SÉQUENCES de symboles peuvent être hiérarchisées par leurs niveaux d'ordres ou de désordres. La pratique habituelle est le calcul la fonction h() de SHANNON. Mais ici nous nous attachons, non pas à tous les éléments constitutifs des séquences, mais à une catégorie de conglomérats d'éléments que nous appelons « les motifs »[418]. Le principe de recherche d'inclusion de motifs procède de la monadologie de LEIBNIZ.

Inclusions de motifs

561-§ Nous pensons que la complexité de construction d'une chaîne de caractères est dépendante de la connexion de ces motifs comme dans une chaîne l-système dont la forme devient de plus en plus complexe quand augmente le nombre de motifs inclus à l'intérieur d'autres motifs [LIND1968] ; en d'autres termes, nous devons rechercher des chemins d'inclusions de motifs contenus dans un texte afin d'en apprécier le niveau de construction indépendamment de toutes connaissances *a priori*.

562-§ Il nous faudra réfléchir sur la démarche que nous devrons adopter. Entre autre, faut-il privilégier les recherches des grandes structures avant de chercher les structures de dimensions inférieures ou bien faut-il au contraire privilégier les petites structures aux détriments des grandes ?

La mise en relation d'idées suit un cheminement d'inclusions

563-§ Chaque idée peut être mise en relation avec d'autres « énonciations » mais il existe des différences de construction dont les origines sont « les contextes » dans lesquels les idées sont pensées. DESCARTES parlait de ce cheminement comme de différentes voies utilisées pour raisonner ; mais nous devons reconnaître aussi que le degré de construction est variable selon le penseur qui lui-même est soumis à un contexte particulier de temps de réflexion et de rédaction du message ainsi qu'à sa capacité à utiliser les idées appartenant à d 'autres acteurs. La différence de penser, en tant que faculté ou aptitude à construire un chemin de déduction, nous conduit à considérer une hiérarchisation structurelle de l'énonciation; c'est-à-dire que le langage emprunte des formes différentes pour affirmer de mêmes idées. WITTGENSTEIN montrait qu'il

[418] Cf. La recherche de définition du terme « motif » à travers trois approches de cryptanalyse, page 207.

existait différentes structures de langages signifiant la même idée[419][WITT1961] mais dont l'énonciation variait en complexité.

564-§ Les langues parfaites de KIRCHER, LULLE, DALGARNO, WILKINS et BECK, expriment ces différences et reposent pareillement aussi sur la combinatoire. D'une façon plus simple nous considérons la problématique sous l'angle des permutations[420]. Quand le nombre d'éléments constituants la proposition est petit, il n'existe que peu de constructions possibles, et inversement, le nombre s'accroît factoriellement quand les éléments sont nombreux. En écrivant la structure[421] qui englobe l'ensemble des permutations des éléments d'une proposition Lullienne ou Kirchérienne, nous mettons en exergue leurs jeux parfaits d'inclusions des motifs successivement redondants[422] et symétriques.

565-§ Lorsque la symétrie parfaite de cette structure propositionnelle se « dégrade » en une séquence de plus en plus particulière, jusqu'à devenir une structure purement asymétrique et donc d 'énonciation unique, symétrie et asymétrie s'opposent.

> *La symétrie, dit DAGOBERT Frey dans un article « On the problem of symmetry in Art » [Studium generale, p. 276], signifie repos, obligation; asymétrie mouvement et relâchement; le premier mot veut dire ordre et règle, le second arbitraire et hasard, l'un rigidité et contraintes formelles, l'autre vie, jeu et liberté [WEYL1952].*

566-§ Les contraintes formelles que la symétrie oblige sont à déterminer ; nous avons mis en évidence certaines de ces contraintes[423] ; mais nous n'avons pas encore connaissance de toutes ces structures particulières et de leurs interactions : c'est précisément ce que nous voulons mettre en exergue.

Méthode de recherche de motifs

567-§ Nous avons vu qu'un motif est une suite reconnaissable d'éléments. Il est vrai que le fait de le reconnaître signifie que nous avons la capacité de l'apprécier, mais dans la langue écrite anglaise étudiée par Fletcher PRATT, toute séquence de lettres n'est pas

---

[419] Pour Pierre GUIRAUD, une phrase contient des mots sémantiquement « vides » et des mots « outils » appelés mots « pleins ». Nous utilisons dans nos phrases des mots qui font partie de nos habitudes linguistiques et dont la présence ne modifie pas le sens de la phrase [BEAU1986]. Nous pouvons en effet comparer deux phrases dont l'une est de type télégraphique: « J'arriverai lundi par l'avion de six heures de l'après-midi» peut être réduite à « Arriverai lundi avion dix-huit heures »

[420] Nous limitons l'explication aux permutations car la combinatoire engendre d'autres cas qui complexifient l'exposé.

[421] Cf. Annexe, Monde des permutations Ordonnées , page 416.

[422] Redondance sans interruption par d'autres symboles.

[423] Listes page 283.

motif.

Restriction aux motifs symétriques et redondants

568-§ Fletcher PRATT[424] dit que pour lui un motif est distingué du plus évident[425] vers l'apparence d'un probable motif. Nous voyons bien que dans sa liste de motifs usuels de la langue anglaise il y a des règles de sélection.

569-§ Nous avons reconnu six règles : –la première est l'occurrence car il y a nécessité à « être » pour être vue, –la redondance immédiate d'une même forme est une deuxième règle (brINGING), –puis vient le motif symétrique qui est la structure la plus énumérée par Fletcher PRATT (Tableau 8). La quatrième forme est la symétrie transformée en asymétrie par l'intrusion d'une seule lettre comme dans les mots anglais *beGINNInG, poSSESSEs* et *vISItIng*. Et finalement, il y a les motifs à la fois redondants et asymétriques par l'insertion d'au moins une lettre différente comme dans les vocables *AvAilAble* et *PREPaRE*.

570-§ Les trois mots qui décrivent ces cinq remarques sont « redondance, symétrie et asymétrie ». Seulement l'asymétrie implique une quantité de degré d'appréciation de ce quoi est asymétrique. Nous connaissons l'asymétrie simple qui ne diffère de la symétrie que d'un élément comme le vautour Egyptien dont seule l'orientation de sa tête transforme la symétrie en asymétrie [FISC1986]. Or, que disons–nous des autres asymétries ?

> **Un texte est considéré dans son entier comme asymétrique s'il n'est pas symétrique ; ce seul problème risque de bloquer définitivement nos recherches puisqu'un texte symétrique est un cas exceptionnel d'ordre parfait.**

571-§ En attendant de trouver une solution acceptable et dans l'immédiat, les seules possibilités qui s'offrent à nous sont la redondance immédiate[426] et la symétrie.

Primauté de la symétrie

572-§ La recherche des motifs doit privilégier l'un ou l'autre de la symétrie ou de la redondance. Il est nécessaire de découvrir l'un avant l'autre puisque les deux en même temps est actuellement impossible. Alors,

---

[424] Motifs particuliers de la langue anglaise, page 209.

[425] On retrouve toute la difficulté d'énoncer ce qui « va de soi ».

[426] Nous appelons « redondance immédiate » une répétition de motif sans interruption.

faut-il privilégier la recherche des motifs symétriques ou bien au contraire faut-il laisser la priorité à la recherche de redondances de motifs ?

573-§ Pour répondre à cette problématique nous devons nous rappeler les processus de MARKOV et plus précisément du graphe de répartition des n-grammes en fonction de la succession de voyelles et de consonnes (page 117). Soit V une voyelle et C une consonne dont les probabilités de réalisation sont égales. L'événement[427] d'une voyelle unique V ne montre pas de redondance. L'apparition du deuxième événement équiprobable C fournit la séquence VC. Cette suite de lettres est ni redondante et ni symétrique. Maintenant, si la troisième lettre tirée est une consonne la séquence VCC est ni redondante ni symétrique mais si la troisième lettre tirée est une voyelle alors la suite VCV est symétrique. En ce sens,

Conclusion 17 La symétrie devance la redondance.

La procédure[428] traitant de la recherche d'un motif symétrique devra être appelée —à dimension égale de motif— avant la procédure traitant de la recherche d'un motif redondant.

Dimension des motifs recherchés

574-§ La priorité de recherche de motifs peut se faire des motifs les plus petits vers les motifs les plus grands ou bien des motifs les plus grands vers les motifs les plus petits.

575-§ Quand nous recherchons les petits motifs avant les grands motifs nous favorisons l'émergence des petits motifs. Les grandes structures ne peuvent alors apparaître clairement[429]. Au contraire en recherchant les grandes structures, avant toute autre, nous laissons possible la découverte des sous structures composant la structure principale[430].

576-§ Nous utilisons en fait la méthode de René Just HAÜY (1784) qui lui-même s'inspira des travaux de ROMÉ DE L'ÎSLE. HAÜY remarqua que le spath d'Islande[431] —de forme rhomboédrique— se brisait en cristaux de plus en plus petits et de forme rhomboédrique identique puisque c'est la propriété même de ce noyau que d'être une

[427] Nous pourrions aussi commencer par une consonne.

[428] Ce point éclairci est important car il influe directement sur notre méthode de programmation.

[429] Nous n'aurions pas pu mettre en exergue le principe l-système d'inclusions de motifs dans notre résolution de la page 416 concernant « la génération automatique de permutations ordonnées » par l'utilisation de règles de réécriture l-système si nous n'avions pas procédé de la sorte.

[430] Variation du champ informationnel, page 243.

[431] Cristal d'Islande dont la biréfringence —dextrogyre et lévogyre— fut découverte par BARTHOLIN et mènera les scientifiques à la théorie ondulatoire de la lumière.

forme ultime [LOCH1994].

Il semble à notre évidence qu'il soit préférable d'opérer de la sorte en détectant les grandes structures de motifs avant les petites structures de motifs.

Types de structures

577-§ La recherche de telles organisations nous oblige à procéder méthodiquement. Un document constitue un regroupement de textes aux thèmes variés constituants d'un thème général. De ce fait, il apparaît indispensable de procéder en premier lieu à la recherche des structures les plus importantes, indépendamment de leurs fréquences.

Les structures identiques ne comptent que pour une seule structure. Ce principe d'analogie simple évite d'écarter statistiquement les structures les moins fréquentes.

Ensuite, graduellement, nous recherchons les structures subalternes de ces structures, puis les sous-structures de ces sous-structures, et ainsi de suite, jusqu'à aboutir à une forme indécomposable.

Ayant alors connaissance des structures les plus basiques, nous déterminons leurs imbrications mutuelles dans la formation d'autres organismes encore à l'état de gestation[432].

[432] Cette démarche s'oppose à l'approximation de SHANNON [PIER1966] qui dit que nous pouvons construire des « phrases » par des tirages de n-grammes. En premier lieu par exemple, nous pouvons faire une approximation d'ordre 0 par tirage aléatoire de lettre appartenant à un alphabet. Mais la séquence obtenue de lettres ne montre pas de phrase ni même de mot qui soit intelligible. Nous pouvons aussi pratiquer un tirage d'ordre 1 selon les statistiques d'apparition des lettres de cet alphabet. De façon à approcher « la réalité de la langue ». En tentant une approximation par des ordres supérieurs comme le digramme ou le trigramme, nous sentons bien que la phrase obtenue s'éloigne d'un état de construction aléatoire mais encore aucun sens n'apparaît. Finalement seule l'approximation par les mots donne un début de satisfaction bien que les règles syntaxiques ne soient pas présentes.

La diffusion du message nécessite un calcul supplémentaire permettant de rendre le message intelligible à tous. Toutefois, quand nous disons « à tous » nous devons préciser « au groupe social auquel appartient l'individu ». Jurgen RUESCH parle de cette asymétrie de la communication chez l'enfant qui doit évoluer vers un système adulte dit « symétrique » et de telle sorte que l'enfant devienne adulte [RUES&BATE1988]. En fait, quiconque change de groupe culturel se retrouve placé dans une communication asymétrique comme un enfant dans un monde d'adultes.

Mais la construction de ses éléments de communications ne sont pas aléatoires et font référence aux individus que le communiquant côtoie, et par la même, sa méthode de communication est liée directement au groupe social auquel il appartient. Nous sommes donc très loin de ce que décrit SHANNON puisque la notion de contexte n'est pas présente dans sa méthode (dimension constante des n-grammes). Toutefois l'idée intéressante semble être dans la distinction entre une approche d'ordre 0 et une approche basée sur une dimension grande du n-gramme que nous appelons « empan » de lecture.

Variation du champ informationnel

578-§ Les êtres humains sont capables de traiter l'information visuelle avec une grande célérité. La vitesse à laquelle nous sommes capables de traiter l'information est fonction de notre capacité à mémoriser les signes. En lecture, certains d'entre nous ne lisent qu'au rythme de syllabes prises une à une ce qui correspondrait au cryptanalyste qui analyse un cryptogramme lettre après lettre, digraphes après digraphes, puis n-graphes après n-graphes (page 95). La difficulté d'établir le « sens », que prennent ses éléments d'information mis bout à bout, ralentit la vitesse de lecture et la compréhension des informations lues [AFL1998].

579-§ A chaque lecture d'une nouvelle syllabe le lecteur doit agréger ce nouvel élément aux éléments déjà acquis. Puis, le lecteur recherche le sens de cette chaîne d'information. Dans ce cas le lecteur est dit « déchiffreur syllabique » [AFL1998]. Cet individu doit prendre de plus en plus de syllabes pour espérer comprendre la signification de la chaîne qu'il est en train de construire ; mais il est confronté à son incapacité à mémoriser toutes les syllabes lues, notre mémoire immédiate nous permettant de conserver le souvenir des trois ou quatre dernières fixations visuelles, mais la prochaine fera disparaître la plus ancienne mémorisée [FOUC1994].

580-§ Nous augmentons notre vitesse de lecture et surtout nous améliorons notre compréhension de l'information en augmentant le nombre de syllabes lues à chaque fixation. L'élargissement de cet empan permet alors de reconnaître plus aisément la signification d'un groupe de signes, comme par exemple la séquence { le, ch, at, no, ir} de { le chat noir }, sachant qu'en fait dans le premier cas il est nécessaire de revenir sur des syllabes antécédentes car oubliées pendant la lecture des syllabes suivantes.

581-§ La compréhension est affectée variablement selon la difficulté des termes employés dans le texte lu. La dimension de l'empan est alors modulée de telle façon que le lecteur puisse capter au mieux le sens de sa lecture.

La dimension de l'empan est dans ce cas fonction de la notion de contexte.

582-§ Pour nous autres cryptologues il est important de connaître ces faits. Nous étudions un document selon deux approches. La première méthode est celle du déchiffreur syllabique qui s'intéresse à l'information statistique n-grammique, comme la recherche du trigramme le plus fréquent, et puis il y a la méthode de recherche des structures indépendantes de la notion statistique[433]. Cette dernière méthode se base sur l'observation qu'il existe des vocables aux caractéristiques morphologiques

[433] Dans la mesure où la structure existe (Motifs particuliers de la langue anglaise. Page 209).

repérables.

583-§ Toutefois, nous nous plaçons toujours dans la situation de la *non connaissance de la langue usitée* et de la *non connaissance de la complexité du document* car ne l'oublions pas notre but est de construire une méthodologie qui permette l'étude du manuscrit de Voynich.

Nous sommes donc dans le cas du lecteur recherchant une dimension d'empan adéquat au texte étudié.

584-§ Sa lecture est dite *flexible* qui s'oppose à *rapide*. Notre système de recherche doit pouvoir s'adapter à la structure du message de telle façon que le repérage d'indice se fasse par la découverte des motifs grands vers les motifs les plus petits. Tout comme une lecture flexible implique une modulation du *faisceau de vision*, nous recherchons les motifs les plus importants susceptibles de fournir un maximum d'information puis, si nous ne les trouvons pas, nous recherchons les motifs de dimensions inférieures fournissant à leur tour la meilleure satisfaction.

Implications méthodologiques

585-§ Nous rechercherons les motifs de dimensions de plus en plus petites. A dimension égale la recherche des motifs symétriques est privilégiée au détriment des motifs redondants. Le motif POSSESSE[434] devient PO$SSESS!E puis PO$#2#(S)E#2#(S)!E. Toutefois, en pratique, la redondance d'une unique lettre n'a pas lieu d'être[435]. Il existe une limite basse du plus petit motif recherché que nous avons évalué à trois parce que la distinction claire entre symétrie et redondance commence à partir de trois éléments. En effet, deux lettres identiques ne montrent pas si leur structure est symétrique ou redondante, elle semble être les deux à la fois.

[434] Principe de codage d'une symétrie et d'une redondance. Nous utilisons deux symboles pour isoler un motif symétrique. Nous attribuons à «$» le signal de commencement de la symétrie et le symbole «!» indique la terminaison de la symétrie. Le vocable *POSSESSE* s'écrit *PO$SSESS!E*. Une redondance est la répétition d'une même forme. Nous encadrons cette forme avec deux symboles, «(» et «)», différents de ceux de la symétrie, que nous ajoutons à un préfixe «#n#» exprimant le nombre d'occurrences : le motif *POSSESSE* s'écrit *PO#2#(SSE).* Ainsi, parmi les deux propositions de codage de *POSSESSE,* seule *PO$SSESS!E* correspond à la Conclusion 17.

[435] Valeur informative de la répétition d'une lettre selon SHANNON.

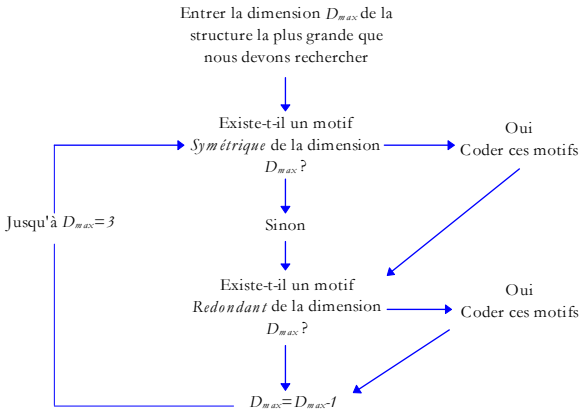


Figure 24 Méthode de recherche des motifs.

Connexions internes de motifs

586-§ *Il faut qu'il y ait des substances simples puisqu'il y a des composés: car le composé n'est autre chose qu'un amas ou aggregatum des simples [LEIB1714].*

587-§ Notre méthode poursuit ce chemin ouvert par LEIBNIZ. Nous recherchons les formes complexes et leurs formes simples. Les substances simples sont incluses dans la forme composée. Dans l'absolu, nous aboutissons à la décomposition d'une séquence de signes en signes que nous appelons communément monogramme ou lettre si il s'agit d'un alphabet. Le vocable {estival} se décompose en vocable {est} et {val} puis {val} en {va} et {est} en {es}, tous les deux décomposables en lettres {e,s,v,a}. Par exemple, le cheminement pourrait être l'inclusion des mots {es, va, est, val} dans {estival} et qu'ayant les formes simples nous sommes capables de trouver la forme composée en complétant ces formes par les éléments manquants. Cette approche est similaire à *la théorie de la forme*[436]. Dans l'apprentissage à la lecture flexible [AFL1998] la reconnaissance de formes se fait par le *test de clôsure* [BEAU1986] crée par Wilson L. TAYLOR en 1953. Ce type d 'exercice montre que nous avons tendance à compléter une forme incomplète. Dans l'exemple précédent nous avons commis l'induction suivante que la séquence de symboles {estival} était le vocable « estival » de la langue française, nous avons déduit que les mots Français « est », « va », « es », « va » pouvaient être des formes simples de « estival » parce que nous connaissions la langue utilisée. Dans le cas où la langue ne nous est pas connue nous procédons de la même manière mais sans assumer l'induction de la signification des motifs. Nous trouvons des motifs ainsi que leurs formes incluses sans porter de jugement sur leurs significations. Nous constatons simplement le *degré* d'inclusion le plus important qui

[436] Connue sous sa dénomination Allemande *Gestalt*.

montre une certaine idée de l'état de construction du texte décortiqué. Cet état de complexité est formalisé

> *par l'analyse, la résolvant en idées et en vérités plus simples, jusqu'à ce qu'on vienne aux primitives [LEIB1714].*

588-§ Nous considérons en premier lieu le manuscrit dans sa globalité, nous recherchons ses structures et ses inclusions ; puis, ainsi de suite, dans ces formes incluses, nous recherchons les formes qu'il comprend, jusqu'à aboutir aux formes simples[437] de la symétrie et de la redondance.

589-§ Cette méthode à l'avantage de favoriser les grandes structures. Si nous avions procédé par une méthode inverse nous aurions favorisé la découverte de petits motifs qui ne permettent pas la mise en exergue des *« empans »* porteurs du maximum d'information. La découverte d'un petit motif empêche la découverte d'un grand motif, tandis que, la découverte d'un grand motif permet de découvrir par la suite les petits motifs qui le composent par inclusion.

590-§ Maintenant, nous passons à son application. Nous attendons que le manuscrit révèle la nature de ses motifs et les connexions de ses motifs. Nous jaugerons ces comportements par deux approches complémentaires que sont le calcul statistique[438] et la représentation graphique structurelle des motifs connexes[439].

---

[437] Dans l'étude d'autres formes complexes nous pouvons procéder de même sans connaître la langue et le sens de lecture de chaque séquence de symboles. Nous tentons d'être indifférent face aux résultats afin d'éviter la tentation d'induction liant la cause de tout phénomène à un résultat escompté. Par exemple, la notion statistique n'a aucun effet dans la recherche d'inclusions de motifs. Elle n'oriente pas les choix de traitement car le quantitatif n'est pas l'expression de la « composition de l'amas ou *aggregatum* des formes simples », le quantitatif ne montre qu'une présence plus remarquable: en chimie le polymère a cette particularité d'être la répétition d'une même molécule bien que cette multiplication engendre des principes actifs propres ; le chimiste doit, en premier lieu par couches successives, rechercher la structure élémentaire du corps qu'il étudie.

[438] Mesures de proportions et de diversités.

[439] Programme de représentation de données connexes, RESEAU-LU, crée par André MOGOUTOV, Université de Saint-Pétersbourg. Maître de Conférence Associé à l'Université PARIS 8 Saint-Denis.

Application

•

LA MÉTHODE que nous proposons est indépendante du sens[440] que nous attribuons aux motifs recherchés. Nous n'avons donc pas la nécessité de constituer une base de données de textes qui serait limitée à une langue naturelle. Nous avons tout intérêt à diversifier notre base de textes à des séquences sans rapport afin d'en mieux évaluer leurs différences. Nous avons donc pris la décision de réunir des documents aussi différents que possibles[441] que sont les textes disponibles par voie électronique, le plus souvent en ASCII simple, ainsi que des textes cryptés.

591-§ Nous débuterons par observer la nature des motifs symétriques et redondants que nous trouverons dans des textes écrits en langues naturelles ; ces premiers résultats nous donnerons un premier aperçu sur leur complémentarité. Nous noterons que leur imprégnation dans les textes suit une logique logarithmique dans laquelle le manuscrit est encore une fois atypique.

592-§ Nous créerons trois instruments de calculs devant nous renseigner sur la proportion, la diversité des niveaux de construction et le coefficient de degré de construction des motifs des textes.

593-§ La troisième étape consistera à construire la représentation des motifs connexes symétriques et redondants.

---

[440] Mises à part : la dimension, la symétrie et la redondance.

[441] La récupération de ces documents en langue anglaise, française, latine, s'est faite par le réseau Internet. Les documents cryptés ont été obtenus par trois méthodes. La première est une transposition, la deuxième est une polysubstitution de VIGENÈRE et la troisième est une combinaison des deux premières. Deux textes (CURRIER et FRIEDMAN) sont référencés comme étant le manuscrit de Voynich et leurs méthodes d'encryptage ne sont pas connues ce qui leur confère un intérêt supplémentaire.

14 novembre 1998 —Première édition

Premiers résultats

594-§ Nous remarquons que les motifs de grandes dimensions sont redondants[442] bien que nous favorisons la recherche de motifs symétriques au détriment des motifs redondants. La symétrie est présente pour des motifs de dimensions inférieures à dix caractères tandis que les motifs redondants sont essentiellement présents au delà des motifs symétriques[443].

595-§ Cependant, nous relevons quelques indices. En premier, nous remarquons que les plus grands motifs sont des motifs redondants. Ils indiquent dans la plupart des cas un titre suivi de l'introduction du paragraphe par ce titre comme dans le texte *Fables*. Une partie ou l'intégralité de l'intitulé du paragraphe est réutilisé pour introduire le paragraphe.

596-§ Le deuxième cas est celui de la précision ou du renforcement de l'information. Dans le *Voyage de Beagle* nous trouvons le motif suivant « *between* ***one hundred and one hundred and*** *fifty rhinoceroses »* qui indique les limites de l'information. Nous retrouvons, comme exemple issu du *Manuel de Guérilla CIA*, le motif « *combatant guerrillas,* ***armed propaganda, armed propaganda*** *teams, »* qui exprime l'énumération. Et enfin dans *History of Animals* le motif précise un qualitatif « *other animals come* ***nearer and nearer*** **».**

Le troisième cas est celui du motif redondant qui apporte une sonorité particulière.

#2#(ACHAL)	détacha la chaloupe
#2#(ENTRE)	Il entre en tremblant d'émotion
#2#(QUISE)	la marquise, qui se leva

597-§ Les motifs symétriques font leur apparition. Ils apportent de nouvelles sonorités qui sont « à cheval » sur plusieurs vocables.

$CEDEMEDEC!	à force de médecines
$E#2#TECE#2#TE!	Paquette, cette jolie suivante

Nous ne percevons pas systématiquement ces formes à l'écoute, souligne PAUL Guillaume[444] [SCIE1998], bien qu'elles soient nombreuses[445] ;

---

[442] Cf. Annexe, page 364.

[443] Cf. Annexe, page 357.

[444] Il montre à travers deux expériences qu'une séquence courte de notes de musique répétée symétriquement (ex : canon palindromique de *L'offrande musicale* par J. S. BACH) est perçue, par l'auditeur, comme un ensemble de deux séquences avec une sorte de symétrie. Par contre, lorsque la séquence s'agrandit, la rétrogradation des notes n'est plus perçue comme séquence symétrique à la première.

[445] De 10 à 20 % dans le langage écrit.

> *L'œuvre musicale organise et qualifie le temps... Or toute composition musicale suppose l'équilibre des forces qu'elle anime. Elle appelle une symétrie qui ne sera perçue par l'auditeur que pour autant que sa mémoire lui rappelle des éléments préalablement entendus dont le retour satisfait ce besoin d'équilibre.*

La perception de cette symétrie étant liée à l'effort de mémoire [PAUL1937].

598-§ Le quatrième genre de motif est celui dont l'importance est à souligner. Le *« The blood is the life ! The blood is the life ! »* du comte Dracula est la signature de l'ouvrage. Certains autres motifs nous apportent des précisions supplémentaires sur le contenu du roman comme les deuxièmes et troisièmes plus grands motifs *« A presage of horror »* et *« For Dear Lucy's sake »*. Nous retrouvons ce type de motif dans le *« Manuel de Guérilla CIA » ;* ce manuel indique diverses techniques dont l'une concerne la *Reduplication,* c'est-à-dire l'absolue nécessité d'éviter les redondances lorsqu'un message est transmis.

> *Reduplication, when the phrase begins with the same word that ends the previous one. For example: "We struggle for* ***democracy, democracy*** *and social justice." The concatenation is a chain made up of duplications. For example: "Communism transmits the deception of the child to the young man, of the young man to the adult, and of the adult to the old man."*

Notre méthode a effectivement détecté leur « précieux » conseil.

599-§ Le dernier motif qui attire notre attention est celui que nous avons trouvé dans *Athènes*. Il nous semble intéressant car il nous rappelle la méthodologie de décryptage du Perse ancien par TYCHSEN et GROTEFEND (page 216). Le motif repéré est ***« therwhoisyourmo ».*** Il pose la question « qui est votre mère ? »

> *When they are examined, they are asked, first, 'Who is your father, and of what deme? who is your father's fa****ther? who is your mother? who is your mo****ther's father, and of what deme?*

600-§ Cet extrait montre des interrogations sur une filiation. Le deuxième motif « ***ofLysimachusandThemistoclesson »*** trouvé, quant à lui, répond à ce type de question avec la structure W, X, fils de Y, fils de Z.

> *The leaders of the people during this period were Aristides,* ***of Lysimachus, and Themistocles, son of Lysimachus, and Themistocles, son*** *of Neocles, of whom the latter appeared to devote himself to the conduct of war, while the former had the reputation of being a clever statesman and the most upright man of his time.*

601-§ D'un aspect quantitatif, l'ensemble des motifs représente entre 10 et 20 % d'un texte[446] dont la majeure partie est symétrique. La diversité des motifs est logarithmique et fonction de la dimension des textes (Figure 25). Toutefois, cette progression a une oscillation de plus en plus importante.

602-§ Nous constatons en effet que la proportion de motifs croît moins vite que la dimension des textes. La conséquence est qu'à un instant donné il faudra une très grande variation de la dimension du texte pour détecter l'apparition d'un nouveau motif.

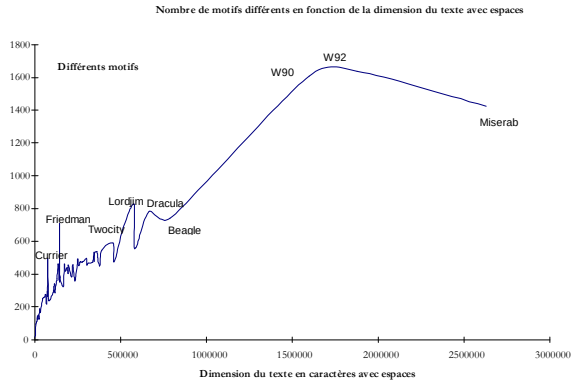


Figure 25 (à gauche) Diversité[447] des motifs symétriques et redondants en fonction de la dimension des textes avec espaces.

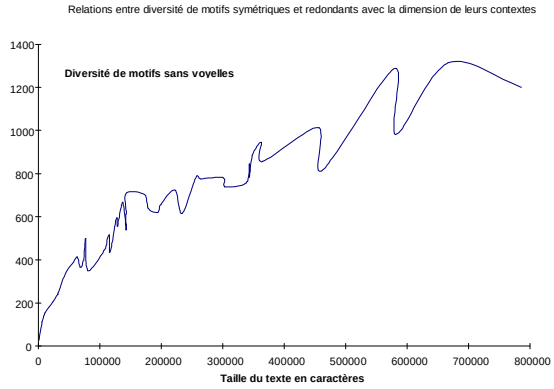


Figure 26 (à droite) Diversité des motifs sans voyelles en fonction de la dimension des textes.

603-§ Les deux textes MS408 sont en avance par rapport aux autres textes. Si nous conservons les mêmes proportions entre « dimension du texte » et « diversité de motifs » alors la version CURRIER devrait être représentée par un texte de près de 500000 caractères et la version de FRIEDMAN devrait être représentée par un texte de plus de 500000 caractères.

Constat 58 La diversité de motifs dans les deux versions (CURRIER et FRIEDMAN) par rapport à la dimension de ces deux textes est deux fois celle que nous attendions.

604-§ Cependant, lorsque nous pratiquons cette même opération, mais avec des textes sémitiques, les différences avec les deux versions de CURRIER et de FRIEDMAN ne

[446] Cf. Annexe, page 425.

[447] Cf. Annexe, Symétries et redondances dans MS408, page 425.

sont plus aussi importantes[448]. Nous pourrions même aller jusqu'à dire qu'elles s'intègrent dans la courbe mettant en relation la diversité des motifs en fonction de la dimension des textes.

605-§ A ceci près qu'il existe une différence qui indiquerait que la dimension « réelle » du manuscrit serait plus importante[449].

> **Constat 59 La diversité de motifs des deux versions (CURRIER et FRIEDMAN) est supérieure à celle attendue mais beaucoup plus proche que celle annoncée dans le Constat 58 quand les voyelles sont supprimées.**

Il en découle l'hypothèse,

> **Hypothèse 28 Le Constat 58 conjugué au Constat 59 laissent penser que les symboles du manuscrit sont, soit des représentants d'éléments au moins digraphiques, soit des éléments substitués par représentations multiples avec variations dans leurs applications.**

Cette Hypothèse 28 expliquerait alors la condensation de la taille du manuscrit et la surprenante diversité de motifs.

> **Constat 60 La dimension du manuscrit semble deux fois supérieure à sa taille réelle[450] parce que la diversité de motifs est très au-dessus de ce qui est attendu (Constat 35).**

606-§ Toutefois, nous ne concluons pas sur ce constat puisque nous ne connaissons pas la langue de rédaction de MS408. Mais dans le cas où la langue est connue[451] alors il est possible d'estimer si le message crypté est issu d'une représentation codique.

607-§ Maintenant, nous poursuivons notre étude sur les connexions entre motifs et leurs jeux d'inclusions.

---

[448] Cf. Annexe, Diversité des motifs sans voyelles, page 354.

[449] De l'ordre de 50% en plus (sans voyelles et avec espaces), c'est-à-dire, la version de CURRIER serait en fait un texte de 120 000 caractères et la version de FRIEDMAN serait un texte de 250 000 caractères.

[450] Latin, anglais, français.

[451] Cas du cryptanalyste qui travaille sur un message militaire.

Les chemins d'inclusions de motifs

608-§ Nous avons vu dans le paragraphe « Connexions internes de motifs » que nous pouvions décomposer une séquence de caractères en groupes de caractères ; nous nous limiterons uniquement à l'étude des inclusions de motifs symétriques et redondants du manuscrit selon ses deux transcriptions.

Méthode de décomposition

609-§ La méthode que nous utilisons permet de mettre en exergue les chemins d'inclusions entre motifs. Chaque chemin se construit à partir de la liste des motifs symétriques et redondants qui ont été trouvés dans le texte[452]. Nous trions cette liste par ordre de grandeur de motif. Nous lisons cette liste des motifs les plus grands vers les motifs les plus petits. A chaque nouveau motif, nous parcourons le reste de la liste de la position du nouveau motif jusqu'à la fin de la liste. Si un motif se trouve être une partie de ce nouveau motif alors le nouveau motif est un corps composé. Nous continuons cette opération jusqu'à connaître l'ensemble des décompositions des motifs de la liste étudiée. Toutefois, nous pouvons ignorer un certain degré d'inclusion afin d'orienter les recherches. Nous considérons que seules les inclusions d'au moins deux motifs sont nécessaires pour l'étude en question ou bien nous considérons qu'un maximum de trois motifs inclus est suffisant : c'est à la personne étudiante de déterminer sa liberté méthodologique.

Les trois niveaux de comparaison

610-§ Nous allons évaluer par notre méthode le niveau de construction d'un texte sans pour autant porter de jugement de valeur sur la nature de l'information contenue dans ce texte.

611-§ Dans l'ouvrage *Dorian G**ray,*** nous obtenons une série d'inclusions de motifs redondants et symétriques qui, si nous la limitons à au moins deux inclusions de motifs par motif principal, nous permet de visualiser leurs indépendances. La Figure 27 comprend un ensemble de graphes montrant les relations entre motifs redondants et symétriques.

[452] Nous appelons « texte » une séquence quelconque de caractères.

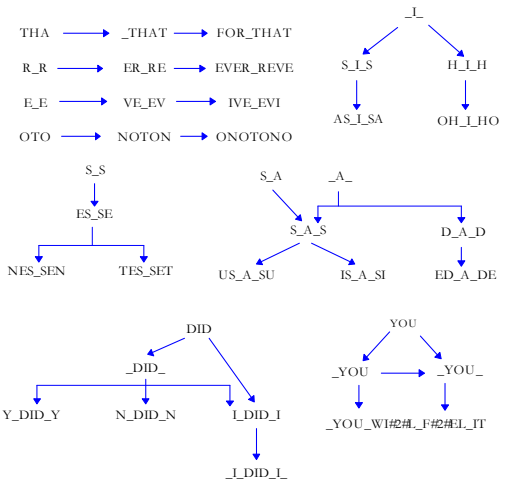


Figure 27 Représentation des vingt-trois chemins d'inclusions[453] de motifs de *Dorian Gray*.

612-§ Nous ne montrons que les inclusions linéaires, comme FOR_THAT ⊃ _THAT ⊃ THA, de degré minimal 3. Ainsi l'élaboration des chemins d'inclusions reste contextuelle car elle ne considère que les motifs présents dans le texte. Si nous considérons FOR_THAT ⊃ _THAT ⊃ THA comme une décomposition logique, par rapport à la connaissance de la langue anglaise, elle n'en demeure pas moins indépendante du sens. Le motif THA a été sélectionné dans le texte parce qu'il était successivement redondant en *n*(THA), à l'identique de *n*(_THAT), tout comme *n*(FOR_THAT).

Il existe des inclusions de motifs pour lesquelles il n'existe apparemment pas de « sens ». L'inclusion ONOTONO ⊃ NOTON ⊃ OTO en est l'expression. Pourtant cette séquence appartient au texte d'Oscar WILDE[454] et apporte une sonorité particulière (Note 444).

613-§ Ce niveau de construction place le texte par rapport à un ordre parfait du type l-système [LIND1968] où la structure principale est décomposable en sous-structures ; nous avons ici la capacité de juxtaposer deux modes de construction afin d'en apprécier les différences ou les similitudes.

453 Le degré minimum d'inclusions est de trois motifs.

454

> *The sullen murmur of the bees shouldering their way through the long unmown grass, or circling with* ***monotono****us insistence round the dusty gilt horns of the straggling woodbine, seemed to make the stillness more oppressive. The dim roar of London was like the bourdon note of a distant organ. In the... »*

614-§ La comparaison se fait sur trois axes :

1- La première comparaison que nous faisons entre les différentes constructions est une recherche du niveau ou degré d'inclusion de motifs[455].

DEFINITION* Le degré d'inclusion est le nombre de motifs constituant un chemin.

DEFINITION* Le degré d'inclusion le plus haut est le nombre maximal de motifs constituant le chemin le plus grand[456].

Le chemin _I_DID_I_ ⊃ I_DID_I ⊃ _DID_ ⊃ DID est de degré 4 et est plus grand que le chemin EVER_REVE ⊃ ER_RE ⊃ R_R de degré 3.

615-§ 2- La deuxième comparaison que nous devons faire montre quelle est la proportion de motifs contenue dans les textes comparés.

$$P_{motif} = \frac{\sum_{m=1}^{n} Motif_m}{N} \quad \begin{cases} P_{motif}\ Proportion\ de\ motif(s)\ dans\ le\ texte\ T \\ Motif_m\ Dimension\ du\ motif\ m \\ N\ Dimension\ du\ texte \end{cases}$$

Equation 13 Proportion de motifs dans un texte.

616-§ 3- Finalement, le troisième axe comparatif est celui de la répartition des chemins d'inclusions. Nous exprimons cette répartition en calculant la proportion de chaque degré d'inclusions par rapport au nombre total de chemin d'inclusions, mais elle doit être spécifiée avec le nombre de chemins différents que nous appelons la diversité.

---

[455] Nous différencions par exemple les chaînes l-systèmes (page 416) d'après leurs degrés d'inclusions de motifs. Ainsi la représentation d'une factorielle 5 est la chaîne suivante :

fac(5)=**A**+**5**(B+3(C+2(D+E)))+**A**+**5**((C+2(D+E))+B+2((D+E)+C+(E+D)))+**A**+(((D+E)+C+(E+D))2+B+((E+D)2+C))**5**+**A**+(((E+D)2+C)3+B)**5**+**A**

elle est d'un niveau inférieur d'inclusion au niveau d'inclusion d'une chaîne factorielle 6 :

fac(6)=**A**+**6**(B+4(C+3(D+2(E+F))))+**A**+**6**((C+3(D+2(E+F)))+B+3((D+2(E+F))+C+2((E+F)+D+(F+E))))+**A**+3(2((D+2(E+F))+C+2((E+F)+D+(F+E)))+B+(((E+F)+D+(F+E))2+C+((F+E)2+D))2)+(2((D+2(E+F))+C+2((E+F)+D+(F+E)))+B+(((E+F)+D+(F+E))2+C+((F+E)2+D))2)3+**A**+((((E+F)+D+(F+E))2+C+((F+E)2+D))3+B+(((F+E)2+D)3+C))**6**+**A**+((((F+E)2+D)3+C)4+B)**6**+**A**

[456] Une séquence dont le degré d'inclusion est zéro est parfaitement diversifiée puisqu'aucun motif est en connexion avec un autre motif.

$$P_d = \frac{n_d}{N} \begin{cases} P_d \, Proportion \ de \ chemins \ de \ degré \ d \\ n_d \, Nombre \ de \ chemins \ de \ degré \ d \\ N \, Nombre \ total \ de \ chemins \end{cases}$$

Equation 14 Diversité de niveaux de constructions.

617-§ Nous établissons aussi le rapport entre le nombre de chemins et la dimension du texte étudié ; ce dernier outils étant utile dans la comparaison entre différents niveaux de constructions de différents textes.

$$R = \frac{Nc}{Nt} \begin{cases} R \text{ coefficient de degré de construction} \\ Nc \text{ Nombre total de chemins} \\ Nt \text{ Nombre de caractères contenus dans le texte} \end{cases}$$

Equation 15 Coefficient de degré de construction.

618-§ Si nous comparons la Figure 27 et la Figure 28, nous constatons simplement les différences d'inclusions. Les motifs du texte *Dorian Gray* apparaissent plus interdépendants[457] que ceux du texte de *Through the looking glass*.

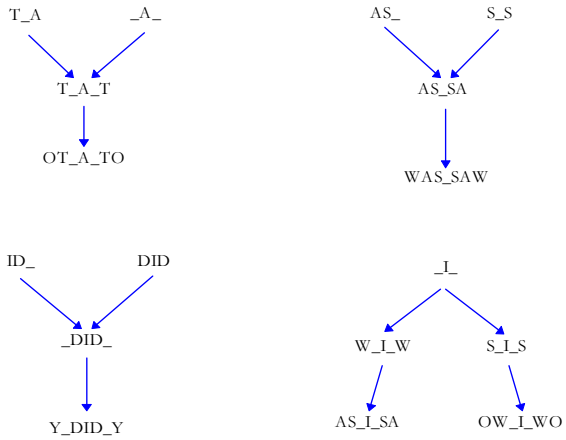


Figure 28 Représentation des huit chemins d'inclusions[458] de motifs de *Through the looking glass*.

[457] Uniquement en ce qui concerne les chemins d'inclusions.

[458] Note 453.

619-§ La diversité est plus grande pour le texte de *Dorian Gray*. Elle est de 23 chemins contre 8 pour *Through the looking glass*. De même, le degré d'inclusions est de 4 pour le premier texte et de 3 pour le deuxième texte. Les répartitions sont de $0{,}91D_{egré}3+0{,}09D_{egré}4$ pour *Dorian Gray* contre $1{,}00D_{egré}3$ pour *Through the looking glass*. Finalement, nous comparons les proportions de motifs symétriques et redondants dans les textes respectifs et nous concluons qu'ils sont voisins[459] de 0,5 pour-cent. Le texte de *Dorian Gray* présente plus d'interdépendances, pour une même représentation quantitative de motifs, que le texte *Through the looking glass* n'en fait.

620-§ Toutefois, cette comparaison ne dit rien à propos de la qualité des ouvrages ; nous n'utilisons cette méthode que pour repérer des structures qui peuvent être utilisées pour la cryptanalyse. En effet, la simple similitude entre chemins d'inclusions nous aide dans le choix de nos hypothèses. Surtout, la capacité d'un texte à fournir plus ou moins de chemins d'inclusions est significative, du désordre du texte probablement crypté ainsi que, des différentes formes d'expression. Nous verrons qu'il existe une relation entre la diversité des méthodes d'encryptage et les chemins d'inclusions.

Les structures de motifs dans MS408

621-§ Nous ne faisons aucune hypothèse quant à la langue naturelle du rédacteur[460] puisque nous ne connaissons que la séquence de symboles de VOYNICH ; sachant qu'il est possible que MS408 soit un agrégat de plusieurs textes de langues différentes et de rédacteurs eux-mêmes différents, nous ne supposons aucune langue. Nous nous limitons à retrouver la ou les structures d'inclusions internes au texte (page 254).

622-§ Le manuscrit a été discrétisé sous six formes[461] relativement différentes dont une seule couvre à peu près la totalité du manuscrit. Nous n'en utilisons que deux. La première est celle obtenue par le groupe de travail de W. F. FRIEDMAN et la deuxième est celle du Capitaine CURRIER, nous avons deux manuscrits. Nous allons consacrer un paragraphe à chacun de ces textes.

Version CURRIER

623-§ Au cours du séminaire du 30 Novembre 1976, le Capitaine CURRIER a rendu publics ses résultats d'analyses. Il a commencé son exposé par la phrase :

> *Je commencerai par dire que je n'ai aucune solution.*

[459] $Pmotif_{Dorian\ Gray}=9{,}1\%$ et $Pmotif_{Through\ the\ looking\ glass}=8{,}6\%$

[460] Les contradictions de constats ne permettent pas de le savoir.

[461] Cf. Tableau 2, page 103. Les membres de l'EVMT participent aussi à l'effort de correction et de transcription.

624-§ Mais, il avait remarqué quelques trouvailles importantes. Il identifia plusieurs morphologies distinctes d'écritures qu'il estima[462] être comprises entre cinq et huit. Il remarqua aussi des écarts statistiques entre distributions de lettres de parties différentes du manuscrit. Il conclut à la présence de deux systèmes d'écriture contrairement au groupe de recherche de FRIEDMAN qui n'en avait découvert qu'un seul (page 164).

625-§ Nous ne ferons pas à nouveau les analyses statistiques car nos prédécesseurs ont déjà étudiés cette question. Nous appliquons simplement la même méthode de recherche d'inclusion de motifs que nous avons pratiquée avec les textes de langues naturelles.

L'Equation 13 donne le tableau suivant :

Texte	Quantité de symétrie	Quantité de redondance	$\frac{Qs}{Qr}$	$\frac{Qs}{Nlettre}$	$\frac{Qr}{Nlettre}$	$\frac{(Qs+Qr)}{Nlettre}$	Nlettre
CURRIER	6676	5517	1.210078	**0.066909**	**0.055293**	0.122203	99777

Tableau 9 Proportions de Symétrie et de Redondance dans VMS408 selon CURRIER.

L'Equation 14 donne la formule des répartitions des degrés d'inclusions:

1,05706E-005 F(degré 5) 0,000147988 E (degré 4) 0,00102535 D (degré 3) 0,00344602 C (degré 2)

Tableau 10 Répartitions des degrés d'inclusions selon CURRIER.

626-§ Le degré maximum atteint est de cinq motifs inclus.

[462] Au moins deux statistiquement différentes.

ODAE_ODC8G_4 ⊃ ODC8G_4 ⊃ ODC8G_ ⊃ C8G_ ⊃ 8G_

Version FRIEDMAN

627-§ Quant à la version texte de FRIEDMAN, l'Equation 13 fournit les indications suivantes :

Texte	Quantité de symétrie	Quantité de redondance	$\frac{Qs}{Qr}$	$\frac{Qs}{Nlettre}$	$\frac{Qr}{Nlettre}$	$\frac{(Qs+Qr)}{Nlettre}$	Nlettre
FRIEDMAN	11116	9995	1.112156	**0.060327**	**0.054244**	0.114571	184261

Tableau 11 Proportions de Symétrie et de Redondance dans MS408 selon FRIEDMAN.

L'Equation 14 donne la formule des répartitions des degrés d'inclusions:

Aucun(degré 5) 0,000221093 E (degré 4) 0,000997755 D (degré 3) 0,00251139 C (degré 2)

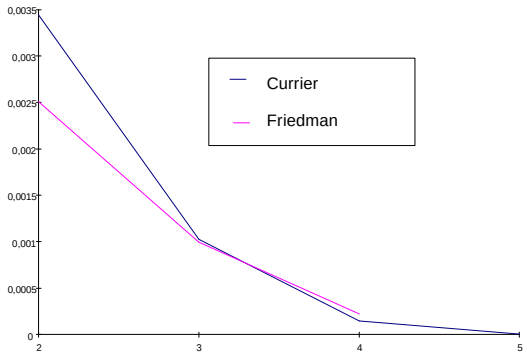
Tableau 12 Répartitions des degrés d'inclusions selon FRIEDMAN.

628-§ Le degré maximum atteint est de quatre motifs inclus. Il y a trente-six chemins de degré maximal quatre. Nous présentons un exemple et nous notons que le chemin trouvé dans le texte de CURRIER n'existe pas dans le texte de FRIEDMAN.

E_SC8G_4ODA ⊃ C8G_4OD ⊃ G_4OD ⊃ _4O

Comparaison

629-§ Le degré d'inclusion de CURRIER est plus élevé que celui de FRIEDMAN. Les équations des répartitions ne sont pas identiques dans leurs proportionnalités.



630-§ Si nous comparons ces deux équations avec celles obtenues pour les textes de langues naturelles, nous obtenons ces différences[463].

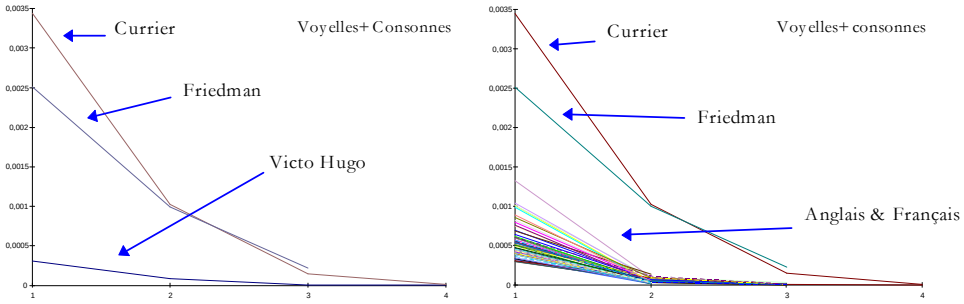
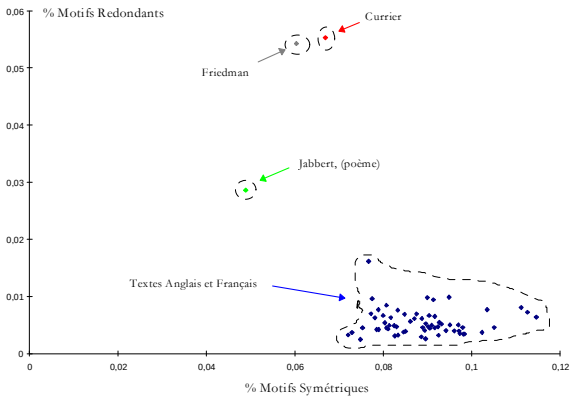


Figure 29 (à gauche) MS408 et le texte de Victor Hugo « Les misérables »

Figure 30 (à droite) MS408 et les textes de langues naturelles (Anglais et Français)

631-§ En ce qui concerne les proportions de motifs symétriques et redondants nous disons que celles de MS408 de CURRIER et celles de MS408 de FRIEDMAN sont quasiment identiques bien qu'il y ait un petit peu moins de motifs symétriques chez FRIEDMAN que chez CURRIER. Toutefois, ces proportions sont encore une fois bien différentes de celles de l'anglais, du français et du latin[464].



463 Les deux courbes du haut (Figure 29 et Figure 30) sont celles de MS408. Elles sont obtenues grâce à l'Equation 14 (page 258). Les courbes qui sont placées en bas sont issues des textes de langues naturelles.

464 Figure 34 et Figure 35, page 265, et Annexe,

Figure 31 Textes avec espaces et voyelles.

632-§ Il semble que ces différentes entités agglomérées dans le manuscrit de Voynich soient une agglomération de différentes structures. L'étude des répartitions des degrés d'inclusions (Figure 32 et Figure 33) montre que MS408 s'intercale dans le groupe des textes dépourvus de voyelles.

Constat 61 La suppression des voyelles dans un texte a pour conséquence une augmentation du nombre des chemins et de leurs degrés d'inclusions.

633-§ Il existe donc un excédant de lettres dans le manuscrit qui se comporte comme un excédant de lettres consonantiques. Nous pensons que la représentation multiple ou un changement de « mode » statistique en est la cause[465] . Les degrés d'inclusions de ce manuscrit s'intercalent dans une polysubstitution de consonnes, nous sommes tentés de dire que le désordre des lettres du manuscrit est maîtrisé par un cycle nullement définit comme répétitif[466].

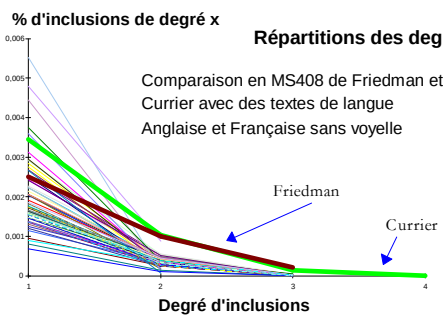


Figure 32 (à gauche) MS408 et les textes dépourvus de voyelles.

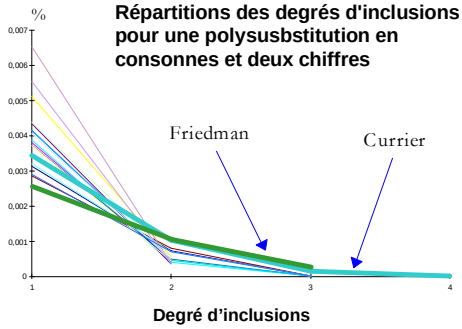


Figure 33 (à droite) MS408 et les textes polysubstitués sans voyelles.

634-§ Nous confirmons l'attitude consonantique par l'Equation 15 (page 258) qui nous indique que les proportions de chemins dans les deux versions MS408 sont en dehors

[465] Hypothèse 28, page 254 et Tableau 13 Statistique des symétries et redondances, diversité.

Symétries et redondances sans voyelles avec espaces, page 392.

[466] Nous opposons l'encryptage par clé courte de polysubstitution et l'encryptage par clé du type « vers littéral » de dimension égale au cryptogramme. Dans le premier cas l'encryptage est périodique mais dans le deuxième cas le cycle est unique et égal à la dimension du manuscrit.

du groupe des textes avec voyelles.

Constat 62 Tandis que les versions MS408 sont intégrées dans le groupe des textes sans voyelles[467].

635-§ Le Tableau 19 (page 425) décrit la proportion de chemins d'inclusions par rapport à la taille d'un texte et il montre qu'il est peu probable que MS408 comporte des voyelles. La partie gauche du tableau nous renseigne sur la position de MS408 par rapport à des textes dénués de voyelles. Nous remarquons que les écarts sont progressifs et continus. La partie droite du tableau montre au contraire une réelle dichotomie entre les deux versions MS408 et les textes composés de voyelles et de consonnes.

Constat 63 L'aspect consonantique du manuscrit est accentué par le nombre de chemins d'inclusions qu'il contient.

636-§ Nous pourrions ainsi considérer que le manuscrit de Voynich est ni plus ni moins une monosubstitution de consonnes. Mais ceci n'est que peu probable parce que

Constat 64 La représentation graphique de la proportion de motifs redondants en fonction de la proportion de motifs symétriques plaide pour une méthode d'encryptage[468] plus complexe.

637-§ En effet, la disposition des groupements de textes est fonction de la nature du cryptage. En bas, à gauche de la Figure 34, se trouve le groupe des textes polysubstitués[469]. En bas à droite se trouvent les textes transposés[470]. MS408 se situe au dessus du groupe des textes anglais, français et encore plus éloigné du latin médiéval (Figure 35).

[467] Cf. Annexe, page 425.

[468] La signification stricte de « chiffrement » n'est pas respectée du fait même que nous ne connaissons pas le procédé utilisé.

[469] Légèrement distincts car plus proches de la représentation multiple que de la polysubstitution par clé.

[470] Dont les protéines font partie. Entre les deux groupes, et sous le groupe des langues naturelles, nous trouvons les ADNc.

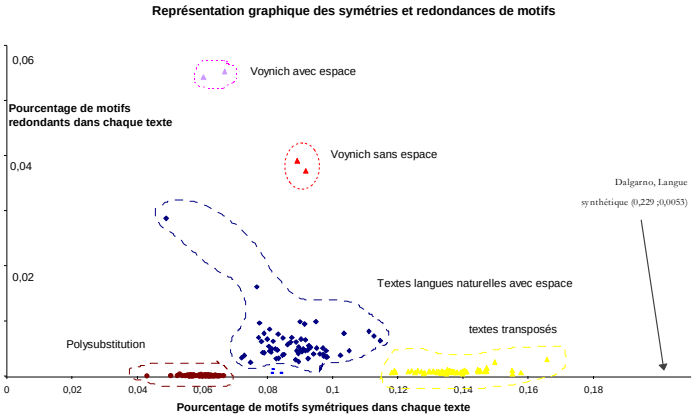


Figure 34 (à gauche) Symétries et Redondances de motifs dans des textes.

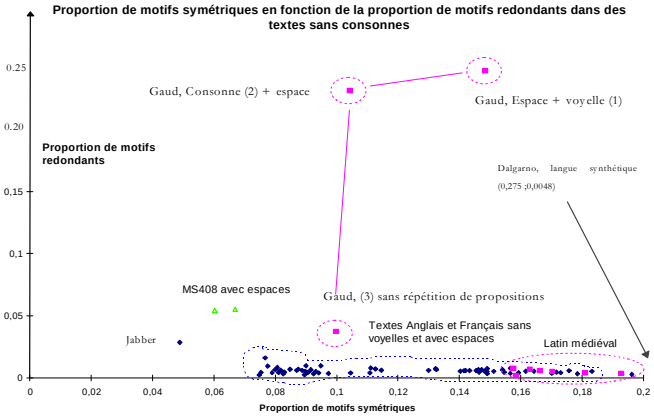


Figure 35 (à droite) Textes latins sans voyelles et avec espaces.

638-§ Nous obtenons la représentation de la Figure 35 en limitant l'affichage aux seuls textes clairs de langues naturelles et aux deux versions de MS408.

639-§ Elle nous informe que MS408 est à l'opposé des méthodes classiques d'encryptage postérieures au 15ème siècle.

Conclusion 18 Bien que le manuscrit ait les attributs d'une polysubstitution, la proportion de motifs redondants est trop différente.

640-§ Si il y a polysubstitution ce n'est alors pas selon la méthode de Blaise de VIGENÈRE[471].

---

471 En 1587, Blaise de VIGENÈRE [VIGE1586] expose dans son ouvrage le « Traité des chiffres » la méthode d'encryptage par table d'alphabets. Il préconise l'utilisation d'une table de polysubstitutions avec clé. La méthode est simple, elle consiste à découper le texte à chiffrer avec une clé de longueur clé(l). Chaque élément de texte sera couplé avec un élément de la clé (*Blaise de VIGENÈRE montra sa préférence pour l'emploi de clé courte intelligible),* le couple formé est (clé(i) , texte$_i$).

Les lacunes de cette méthode d'encryptage peuvent être résumées en trois points.

- Premièrement, la connaissance *a priori* de la table de polysubstitution permet de valider ou de rejeter l'hypothèse de la lettre claire. Quand nous validons une hypothèse mettant en relation une lettre claire avec sa lettre cryptée nous validons la découverte de toutes les lettres du groupe crypté.
- Le deuxième point concerne la longueur de la clé de polysubstitution. La table de VIGENÈRE a une dimension supérieure à la longueur de la clé. Quand la clé est de dimension inférieure à l'alphabet de la table alors seules quelques lignes de la matrice sont utilisées. La table est dans ce cas sous-exploitée et le cryptogramme est moins désordonné.

Causes d'une redondance inhabituelle

641-§ Cette grande différence de proportion en motifs redondants peut trouver son explication dans la représentation multiple. Cette méthode associe un ensemble de symboles à un unique. Il est en effet courant de trouver dans MS408 des successions de motifs qui ne diffèrent que d'un symbole [CURR1976] ; nous supposons qu'il existe un rapport direct entre la proportion de motifs redondants et la représentation multiple sous toutes ses formes. La suppression des voyelles d'un texte est une possibilité mais une langue synthétique basée sur la combinatoire en est une autre.

Suppression des voyelles

642-§ La première possibilité d'une quantité inhabituelle de redondances de mots différents d'un seule lettre s'explique avec une suppression de voyelles.

643-§ Admettons les deux vocables « coûter » et « coûteux », ils sont tous les deux de dimensions différentes mais lorsque nous ne conservons que leurs consonnes nous obtenons les deux vocables consonantiques, « ctr » et « ctx », qui ne diffèrent[472] que d'une seule lettre, et de partie commune « ct ». Nous retrouvons cet aspect dans le document référencé *Gaudeamus Igitur* dans la Figure 35.

Avec Voyelles	Sans Voyelle
Vivat membrum quod libet,	Vvt mmbrm qd lbt,
Vivant membra quae libet;	Vvnt mmbr q lbt;

644-§ Nous voyons que la distinction, entre deux phrases se suivant, dépend de quelques lettres, *Vivat membr**um** qu**od** libet,* et ,*Viva**n**t membra qu**ae** libet,* que nous retrouvons dans la version consonantique, *Vvt mmbr**m** q**d** lbt,* et *Vv**n**t mmbr q lbt.*

- Le troisième et dernier point discute de la fragilité de la clé littérale. La connaissance du contexte linguistique permet d'orienter les hypothèses mettant en relation les lettres présumées avec une lettre de la clé. Quand la clé est un vocable et que nous connaissons sa dimension alors nous savons qu'un certain nombre de vocables sont probables. Quand nous découvrons quelques lettres de cette clé alors il nous est possible de présumer de la présence de certaines lettres plutôt que d'autres par le simple test de clôsure [BEAU1986]. Ce test repose sur la théorie de la forme, il consiste à compléter par des mots une phrase dont certains mots sont absents : test qui s'étend à la reconnaissance d'un mot d'après une approximation de sa forme. La clé non cryptée fragilise la sûreté de la méthode.

Ainsi dans le cas de la méthode VIGENÈRE, il apparaît indispensable de pallier à ces trois défauts. Les solutions apportées pour réduire ces risques d'attaques ont été de générer une table d'alphabets désordonnés pour réduire le nombre de lettres découvertes par hypothèse émise. En 1710, Jean SESTRI [SEST1710] avait apporté une amélioration en construisant non plus un alphabet décalé mais un alphabet d'involution.

[472] Nous constatons dans le manuscrit que les positions des mots les plus instables se situent sur les quatre premières lettres (Figure 22) des mots et qu'alors la forme adjectivée n'est pas la cause de ce constat. Nous considérons que le sens de l'écriture est orienté de gauche à droite et de haut en bas. Lorsque nous inversons le sens de lecture alors les quatre premières lettres deviennent les quatre dernières lettres des mots qui correspond à ce que nous constatons dans les langues européennes mais pas d'une façon aussi régulière.

645-§ Nous comparons ce texte composé de voyelles et de consonnes avec ce même texte mais dénué de ses voyelles puis nous l'opposons à l'ensemble des textes qui sont à notre disposition (Figure 34 et Figure 35).

646-§ Nous observons que le manuscrit de Voynich se distingue très fortement des autres textes par sa capacité à être redondant. Et que lorsque les textes de langues sont dénués de consonnes alors l'écart qui les sépare de ce manuscrit est réduit mais toujours important. Surtout, nous remarquons qu'un texte latin *Gaudeamus Igitur* constitué comme un poème tend à se rapprocher d'un texte anglais *Jabber Wocky* constitué lui aussi comme un poème et que tous deux « se rapprochent » de ce manuscrit. Ces derniers points sont importants car dans le cas du manuscrit de Voynich nous constatons qu'il ne procède ni d'une polysubstitution et ni d'une transposition.

Est-ce que la simple suppression des voyelles suffit à expliquer cette surabondance de redondances ?

647-§ En étudiant le texte de *Gaudeamus Igitur*, nous nous apercevons que le nombre de redondance de motifs est quatre fois plus important que dans les deux versions de MS408. Quand le texte latin *Gaudeamus Igitur* est complet alors le taux de motifs symétrique est de 0,15 et le taux de motifs redondants est de 0,24 (Figure 35. Cas *Gaud(1)*). Quand ce texte est dénué de ses voyelles les taux ci-dessus cités deviennent : 0,09 et 0,23 (Figure 35. Cas *Gaud(2)*).

Jabber avec Voyelles	Jabber Sans Voyelle	Gaudeamus Igitur Avec Voyelles	Gaudeamus Igitur Sans Voyelle
Jabberwocky Lewis CARROLL	Jbbrwck Lws Crrll	Gaudeamus Igitur	Gdms gtr
'Twas b**rilli**g, and the slithy toves	'Tws br**ll**g, nd th slth tvs	Gaudeamus igitur,	Gdms gtr,
Did gyre and gimble in the wabe:	**Dd** gr nd gmbl n th wb:	Iuvenes dum sumus;	vns dm sms;
All **mim**st w**ere** the b**oro**groves,	ll **mm**st w**r** th br**g**rvs,	Post iucundam iuventutem,	Pst cndm vnttm,
And th**e mome** raths outgra**be.**	nd th **mm** rths tg**rb.**	Post molestam senectutem	Pst mlstm snctm
"**B**eware the Jabberwock, my son!	"**B**wr th Jbbrwck, m sn!	Nos habebit humus,	Ns hbbt hms,
The jaws that bi**te, t**he claws th**at catc**h!	Th jws tht b**t, t**h clws th**t ctc**h!	Nos habebit humus.	Ns hbbt hms.
Beware the **Jubjub** bird, and shun	Bwr th **Jbjb** brd, nd shn		
The frumious Bandersnatch!"	Th frms Bndrsntch!"	Ubi sunt, qui ante nos	b snt, q nt ns
He took his vorpal sword in hand:	H tk hs vrpl swrd n hnd:	In mundo fuere?	N mnd fr?
Long time the manxome fow he sought--	Lng tm th mnxm fw h sght--	Vadite ad superos,	Vdt d sprs,
So h**e re**sted by the **Tumtum** tree,	S h **r**std b th **Tmtm** tr,	Transite ad inferos,	Trnst d nfrs,
And stood awhile in thought.	nd std whl n thght.	Ubi iam fuere,	b m fr,
And, as in uffis**h th**ough**ht h**e stood,	nd, s n ffs**h th**g**ht h** std,	Ubi iam fuere.	B m fr.
The Jabberwock, with **eye**s of flame,	Th Jbbrwck, wth s f flm,		
And whiffling through **h th**e tulgey wood,	nd whfflng thrg**h th** tlg wd,	Vita nostra brevis est,	Vt nstr brvs st,
And burbled as it came!	nd brbld s t cm!	Brevi finietur;	Brv fntr;
One, two!One, two!And through and through	**n, tw!n, tw!nd thrgh nd thrgh**	Venit mors velociter,	Vnt mrs vlctr,
The vorp**al bla**d**e we**nt snicker - snack!	Th vrp**l bl**d **w**nt snckr - snck!	Rapit nos atrociter;	Rpt ns trctr;
H**e lef**t **it** de**ad, a**nd with its head	H **lf**t **t** d**d,** nd wth ts hd	Nemini parcetur,	Nmn prctr,
H**e we**nt galumphing back.	H **w**nt glmphng bck.	Nemini parcetur.	Nmn prctr.
And hast thou slain the Jabberwo**ck**?	nd hst th sln th Jbbrw**ck**?		

Come to my arms **by b**eamish b**oy**!	**C**m t m rms **b b**msh b!
O frabious day!Callooh!C**alla**y!	frbs d!Cllh!C**ll**!
He chortled in his joy.	H chrtld n hs j.
'Twas b**rilli**g, and the slithy toves	'Tws br**ll**g, nd th slth tvs
Did gyre and gimble in the wabe:	**Dd** gr nd gmbl n th wb:
All **mim**sy w**ere** the b**oro**groves,	ll **mm**s w**r** th br**g**rvs,
And th**e mome** raths outgrabe.	nd th **mm** rths tgrb.

Vivat academia,	Vvt cdm,
Vivant professores,	Vvnt prfssrs,
Vivat membrum quod libet,	Vvt mmbrm qd lbt,
Vivant membra quae libet;	Vvnt mmbr q lbt;
Semper sint in flore,	Smpr snt n flr,
Semper sint in flore.	Smpr snt n flr.
Vivat et respublica	Vvt t rspblc
Et qui illam regit,	t q llm rgt,
Vivat nostra civitas,	Vvt nstr cvts,
Maecenatum caritas,	Mcntm crts,
Quae nos hic protegit.	Q ns hc prtgt.
Vivat omnes virgines,	Vvt mns vrgns,
Faciles, formosae,	Fcls, frms,
Vivant et mulieres,	Vvnt t mlrs,
Tenerae, amabiles,	Tnr, mbls,
Bonae, laboriosae.	Bn, lbrs.
Pereat tristitia,	Prt trstt,
Pereant osores,	Prnt srs,
Pereat diabolus	Prt dbls
Quivis antiburschius,	Qvs ntbrschs,
Atque irrisores.	tq rrsrs.

Constat 65 La suppression des voyelles ne paraît pas être responsable d'une grande variation de la proportion des redondances mais par contre elle est responsable de la diminution du nombre de motifs symétriques.

648-§ Quand les redondances de phrases identiques sont supprimées et que le texte est dénué de ses voyelles alors les taux sont respectivement 0,10 et 0,03 (Figure 35. Cas *Gaud(3)*). Au bout de ces trois étapes de réduction des redondances nous obtenons un texte « latin » sans voyelles et sans répétition de phrase.

Avec Voyelles	Sans Voyelle et sans répétition de phrase
Gaudeamus Igitur	Gdms gtr
Gaudeamus igitur,	
Iuvenes dum sumus;	vns dm sms;
Post iucundam iuventutem,	Pst cndm vnttm,
Post molestam senectutem	Pst mlstm snctm
Nos habebit humus,	Ns hbbt hms.
Nos habebit humus.	
Ubi sunt, qui ante nos	b snt, q nt ns
In mundo fuere?	N mnd fr?
Vadite ad superos,	Vdt d sprs,
Transite ad inferos,	Trnst d nfrs,
Ubi iam fuere,	B m fr.
Ubi iam fuere.	
Vita nostra brevis est,	Vt nstr brvs st,
Brevi finietur;	Brv fntr;
Venit mors velociter,	Vnt mrs vlctr,
Rapit nos atrociter;	Rpt ns trctr;
Nemini parcetur,	Nmn prctr.
Nemini parcetur.	

Vivat academia,	Vvt cdm,
Vivant professores,	Vvnt prfssrs,
Vivat membrum quod libet,	Vvt mmbrm qd lbt,
Vivant membra quae libet;	Vvnt mmbr q lbt;
Semper sint in flore,	Smpr snt n flr.
Semper sint in flore.	
Vivat et respublica	Vvt t rspblc
Et qui illam regit,	t q llm rgt,
Vivat nostra civitas,	Vvt nstr cvts,
Maecenatum caritas,	Mcntm crts,
Quae nos hic protegit.	Q ns hc prtgt.
Vivat omnes virgines,	Vvt mns vrgns,
Faciles, formosae,	Fcls, frms,
Vivant et mulieres,	Vvnt t mlrs,
Tenerae, amabiles,	Tnr, mbls,
Bonae, laboriosae.	Bn, lbrs.
Pereat tristitia,	Prt trstt,
Pereant osores,	Prnt srs,
Pereat diabolus	Prt dbls
Quivis antiburschius,	Qvs ntbrschs,
Atque irrisores.	tq rrsrs.

649-§ CURRIER constatait que MS408 comportait de nombreuses séquences répétitives de symboles ne différant que d'un ou de quelques symboles. Nous constatons précisément la même chose du texte de *Gaudeamus Igitur* dans la version de ci-dessus (Figure 35. Cas *Gaud(3)*).

> **Constat 66 L'incantation poétique du texte *Gaudeamus Igitur* en latin médiéval tend vers la structure du manuscrit de Voynich lorsque ce texte est dépourvu de voyelles et de propositions immédiatement répétées.**

650-§ Dans ce cas, le système d'encryptage ressemblerait à un système codique du type sténographique. L'aspect même des lettres y fait penser (Constat 3). Et nous avons été surpris de retrouver une partie des symboles du manuscrit de Voynich dans un ouvrage du 18ème siècle traitant de la *brachygraphie*[473] [GURN1789].

En tous cas, il apparaît évident que

> **Constat 67 Le jeu de construction de l'incantation poétique du texte de *Gaudeamus Igitur* est responsable de sa capacité à être très pourvu en motifs redondants.**

Devons-nous pour autant penser que ce manuscrit soit la simple translation d'un écrit sémitique en notation sténographique ?

---

473 L'Art d'écrire avec des caractères abrégés que l'on appelle aussi « Short-hand » ou sténographie. Introduit à la cour d'Angleterre par le traité du Docteur Timothy BRIGHT en 1588.

651-§ Le Capitaine CURRIER avait relevé qu'il existait deux types de langages dans la partie consacrée à l'Herbier. Ces deux langages notés A et B sont différents statistiquement et selon CURRIER ils sont aussi différents dans leur graphologie (Constat 37).

652-§ La remarque de CURRIER corrobore la Conclusion 18 dont le propos concernait l'insuffisance des redondances de motifs dans un système d'encryptage par polysubstitutions, les représentations multiples évolutives étant plus aptes à augmenter les redondances immédiates.

653-§ Dans le cas où le texte est écrit comme le poème *Jabber Wocky* de Lewis CARROLL ou comme *Gaudeamus Igitur* (Constat 66 et Constat 67), nous devrions penser qu'en fait de langages A et B, il existerait au moins deux méthodes[474] de représentations. L'hypothèse que MS408 serait une substitution à représentations multiples deviendrait plausible.

654-§ Mais cet ordre si régulier que nous avons mis en évidence (page 228) n'est pas si rigoureux[475] dans les textes de langues naturelles.

655-§ Nous notons que cet ordre n'est pas prévisible bien que la suppression des voyelles d'un texte contribue à ordonner les priorités de substitution aux différentes positions des vocables.

Il existe donc une organisation des symboles de VOYNICH qui s'inspire plus d'un langage syntaxique que d'un langage naturel.

656-§ La suppression des voyelles ne serait alors pas la raison principale de la structure du manuscrit (Constat 61) ce qui somme toute est logique puisque la structure est déterminée par les règles de construction de chaque proposition.

Combinatoire

657-§ La problématique de l'importante redondance de motifs du manuscrit est explicable aussi par le jeu des permutations des entités intervenant dans les langues d'inspiration Lullienne.

658-§ Nos travaux montrent que les mots du manuscrit sont trop bien réglementés dans leur élaboration pour être le produit d'un encryptage *a posteriori* ; ici la structure des

474 Constat 44, page 181.

475 Structure de phrase différente, variation dans la position de l'adjectif, des pronoms et des substantifs.

mots est sous-jacente[476] au cryptogramme de la même façon que la synchronisation des lettres d'un texte clair avec une clé cyclique se retrouve dans le message crypté ; en ce sens que la notion d'encryptage est interprétable comme notre incapacité à traduire.

Si nous faisons abstraction de cette incapacité à traduire alors le manuscrit est un texte quelconque dont les mots sont agencés selon une méthode qui reste à définir.

659-§ Nous savons que les mots du manuscrit s'obtiennent suivant deux principes essentiels :

- Par l'ordonnancement des positions de substitutions de chacune des lettres d'un mot (Figure 22, page 228).
- Par la construction d'un mot à partir d'un autre mot de dimension inférieure (Conclusion 15, Conclusion 16, page 233).

660-§ Ces deux principes sont synthétiques. Nous ne les observons pas dans les langues naturelles. Le langage qui intègre ces caractères synthétiques est comparable à un langage synthétique dont la nature[477] n'est pas encore définissable. Cependant, quelque soit cette nature synthétique nous savons qu'elle a pour source la notion d'arrangements d'entités que les deux principes cités ci-dessus nous révèlent.

Dans la langue de LULLE, tout commence à partir d'un ensemble d'entités dont leurs permutations —ou leurs combinatoires— créent des propositions (page 187). Nous simplifions sa méthode pour montrer en quoi la combinatoire édifie la redondance.

661-§ A partir de « quatre pierres » nous construisons « vingt-quatre » maisons que nous écrivons sous la forme[478] : « ABCD, ABDC, ACBD, ACDB, ADBC, ADCB », et nous remarquons que les deux premières lettres sont semblables deux à deux ; les racines de ces petits mots de quatre lettres sont : « AB », « AC » et « AD ».

662-§ Cependant, les mots du manuscrit ont des dimensions *variables* (page 151) entre l'unique lettre et le mot de treize lettres[479]. La permutation d'un seul groupe de lettres

[476] A opposer avec l'opération qui consiste à rendre volontairement illisible un écrit ; ainsi, les symboles du cunéiforme de Babylone et les hiéroglyphes égyptiens n'étaient plus compris mais ils n'étaient pas cryptés pour qu'ils soient incompris. Ce point de vue rejoint en partie une des idées du Docteur Leo LEVITOV (Note 106).

[477] Transcription phonétique, sténographie, langage universel taxinomique ou combinatoire, pasilalie ou pasigraphie.

[478] Uniquement le premier groupe des permutations.

[479] Pour la version de FRIEDMAN et de une à dix-huit lettres pour la version de CURRIER (page 409 et 151).

est alors insuffisante pour exprimer la diversité de ces dimensions de vocables. Dès lors que nous pratiquons la permutation de lettres issues de groupes de dimensions différentes[480], nous pratiquons une combinatoire de ces lettres et nous obtenons des mots de dimensions différentes. Or, ceci n'est pas en adéquation avec un système Lullien qui n'admet la combinatoire d'éléments identiques que si il existe un artifice mnémotechnique pour les différencier (Constat 48) ; comme uniquement seize lettres sur trente n'admettent pas une transition sur elles-mêmes, il existe quatorze lettres qui se succèdent parfois à elles-mêmes (page 393).

Constat 68 Quatorze symboles ont une transition sur eux-mêmes, ils ne sont pas en adéquation avec une proposition Lullienne.

663-§ Nous hypothéquons que si des symboles identiques du manuscrit se succèdent alors leur signification est autrement pensée que celle d'un vocable dans un état substantivé ou adjectivé.

664-§ Les symboles rencontrés dans les langues synthétiques et qui ont ce comportement sont ceux qui décrivent un numérique comme ceux de la langue de KIRCHER[481] dans laquelle apparaît une dichotomie[482] codique opposant chiffres romains et chiffres arabes (page 193).

665-§ Dans cette optique, il serait plus adéquat de penser que la nature de ces transitions entre symboles signifierait que le manuscrit a pour utilité de classer des informations.

Hypothèse 29 La redondance serait alors l'expression d'une indexation par langue synthétique.

666-§ La méthode permettant d'orienter les hypothèses, vers une augmentation de la certitude, consiste à rechercher les différents foyers de motifs qui sont à la source des jeux de constructions des chemins d'inclusions de motifs symétriques et redondants (page 254).

Implications de la diversité sur la connexion des motifs

667-§ La structure du document est révélée par les proportions des motifs redondants et symétriques dont leurs connexions créent des graphes relationnels d'écrivant un état

[480] Référence à la diversité des modes statistiques (page 181).

[481] De même que le système de Cave BECK qui admet l'indexation par les nombres (page 80). Le système se complexifie lorsqu'il se transforme en *pasilalie* (règles de prononciations phonétiques des codes).

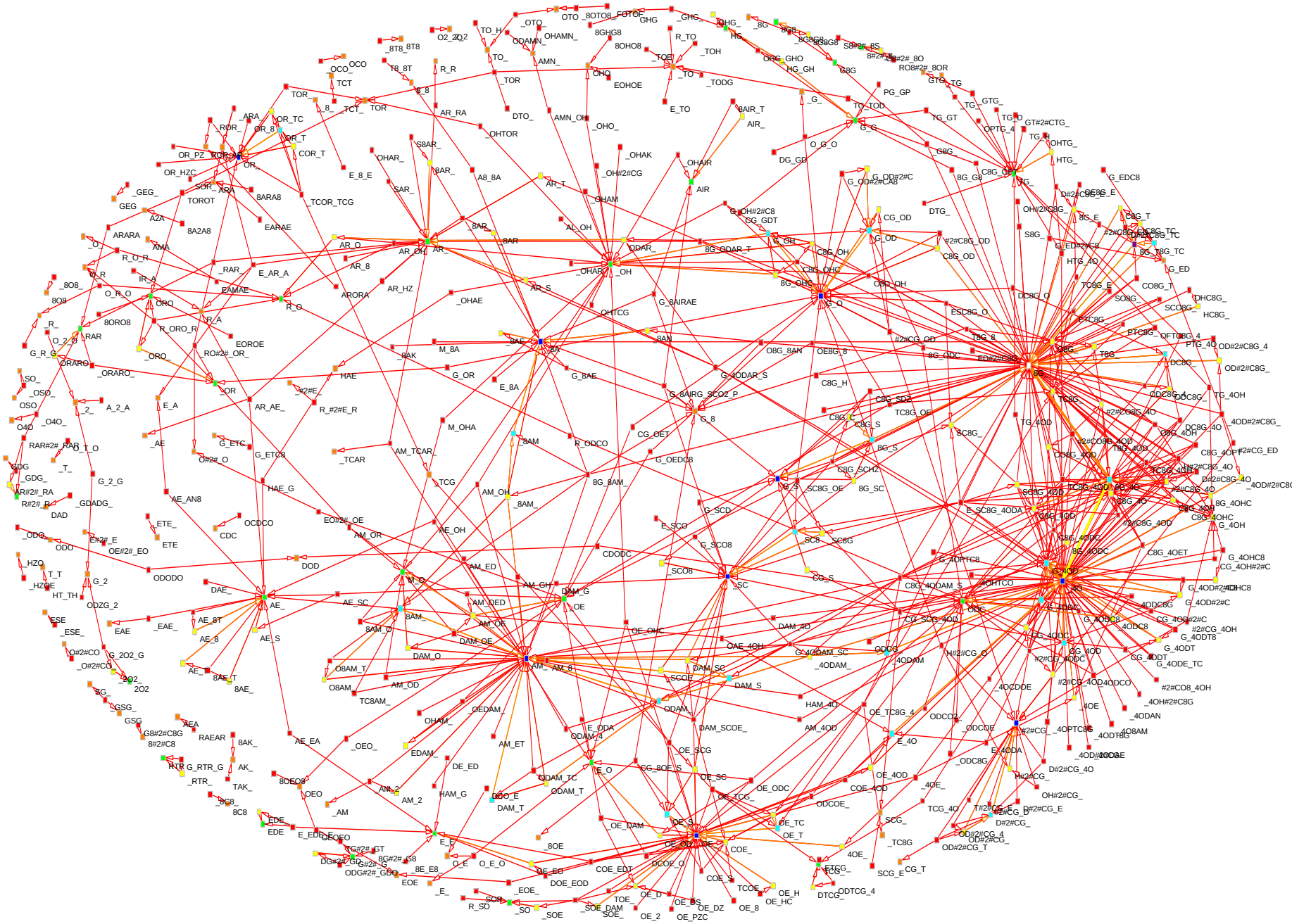
[482] Les systèmes de DALGARNO, WILKINS, LULLE, ne permettent pas à des symboles de se succéder à eux-mêmes dans le cadre de la *pasigraphie* (écriture ne permettant pas une lecture phonétique).

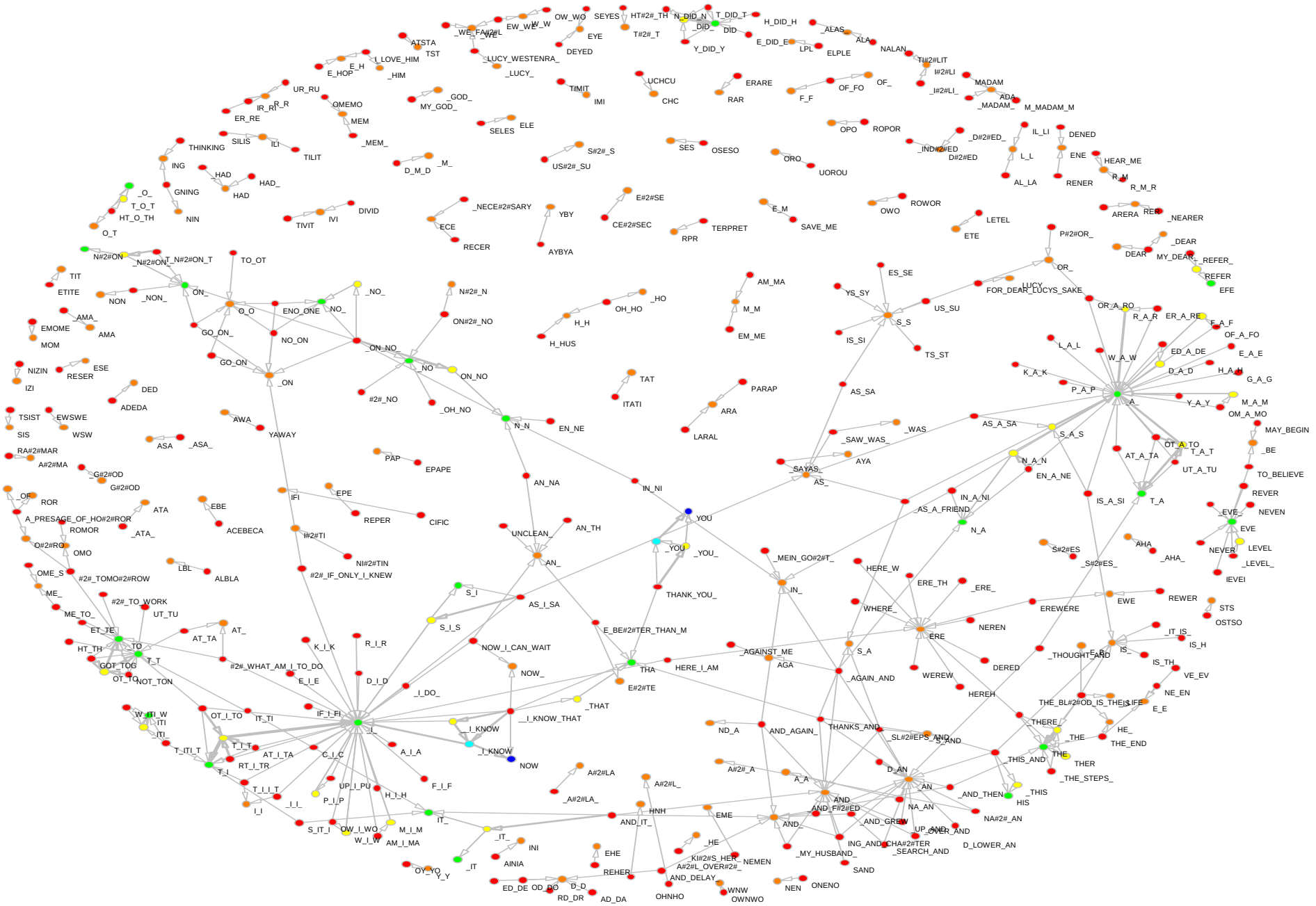
de construction.

668-§ Nous avons précédemment positionné le manuscrit par rapport à des comportements connus. Certes, cela procède de l'analogie à cette différence près que nous recherchons indirectement les indices d'une structure par rapport à des structures connues sans pour autant induire une hypothétique conclusion[483].

[483] Nous ne sommes pas dans la position de GAUSS à qui le sentiment de connaître la solution lui permettait de rechercher comment son esprit avait ainsi abouti.

Notre stratégie se base sur l'aspect du positionnement du manuscrit par rapport « à ce que nous connaissons » et nous ne privilégions pas la conclusion au détriment du cheminement comme cela fut le cas pour l'expérience cryptanalytique du Capitaine DREYFUS, NEWBOLD, LEVITOV, FEELY et STRONG.





14 novembre 1998, Graphes des motifs connexes dans le manuscrit de Voynich, 240

Motifs connexes anglais, français, latins

669-§ Prenons l'exemple du graphe des inclusions de motifs du texte *Dracula* (page 277). Nous repérons facilement deux foyers principaux occupés par les motifs, « _I_ » et « _A_ », que nous traduisons en français par le pronom « je » et l'article « un, une ». Ces deux motifs se lient par divers dédales dont le plus court est « _I_ ⊂ S_I_S ⊂ AS_I_SA ⊃ AS_ ⊂ AS_A_SA ⊃ _A_ ».

670-§ Autour de « _I_ » se construisent des motifs de plus en plus grands jusqu'à la proposition qui est le résultat d'une conjugaison entre petits motifs. Ces propositions se présentent comme des *termes moyens* entre foyers ; « _I_ » et « _ON », partagent la proposition « _IF_ONLY_I_KNEW » ; « _I_ » et « ERE », sont inclus dans un terme partagé « HERE_I_AM » ; puis les motifs engagés dans la construction se regroupent par trois pour former des propositions comme « NOW_I_CAN_WAIT », décomposable en trois motifs « _I_ », « AN_ » , « NOW_ » qui sont liés à des propositions très voisines comme : « _I_KNOW », « _I_KNOW_THAT », ce dernier motif étant lié à « _THAT », puis « THA », lui-même lié à « THANK_YOU_ » par sa conjugaison avec le motif « _YOU ».

Les petits motifs sont symétriques et quelques petits motifs asymétriques créent l'exception ; les formes se conjuguent pour modeler l'asymétrie des propositions dont la plus sensée dans *Dracula* est « THE BLOOD IS THE LIFE »[484].

671-§ Les motifs de la langue française s'associent différemment des motifs de la langue anglaise. Il existe de réelles distinctions structurelles qui catégorisent la connexité de leurs motifs.

672-§ Le foyer principal (page 442) est occupé par un mot de trois lettres, « ETE », qui se lie dans un déploiement progressif[485] avec les foyers « _SE », « S_S », « E_E ». Cette structure est très symétrique et ne fait intervenir que de rares motifs asymétriques.

Le participe passé « ETE » se développe symétriquement en « AS_ETE_SA ». La préposition « _A_ » est étonnamment isolée dans sa propre structure de motifs symétriques ; tandis que les motifs les plus longs sont « MANGEONS DU JESUITE » et « LES ETRES ETENDUS QUI SENTENT ».

673-§ Le latin médiéval contient des structures compartimentées de motifs. Les structures sont petites et très rarement connectées entre elles. Il ne semble pas exister de foyer majeur ; ceux qui nous paraissent les plus conséquents sont occupés par les

484 Notre méthode ne se fixe pas pour but d'extraire le « sens » linguistique d'un document. Cependant, parfois le « sens » linguistique tombe « à point nommé ».

485 Comparer les graphes de la page 442 (*Candide)* et de la page 444 (*Micromega).*

motifs : « NON », « TAT », « RER, ERE », « S_S », « ITI, TIT », « ILI », « E_E », « L_L », « IBI » ; les motifs sont très symétriques[486] mais un foyer est peu pourvu en motifs diversifiés.

Nous connaissons les liens étroits entre la langue latine et la langue française. Les représentations graphiques des chemins d'inclusions l'expriment surtout lorsque nous étudions ces langues sans leurs voyelles.

674-§ L'approche consonantique montre[487] que le latin et le français partagent des foyers communs[488] autour desquels s'agencent principalement les motifs symétriques.

675-§ Les différentes représentations des connexions entre motifs placent les textes dans les trois cas de la comparaison *différence-concordance-contrariété* ; le texte anglais est structuré différemment du texte latin et du texte français, tandis que, le texte latin et le texte français ont une grande part de concordance. La troisième comparaison est la contrariété à laquelle nous savons le manuscrit familier.

Motifs connexes du manuscrit

676-§ Peu de chemins sont indépendants des autres dans le manuscrit de Voynich (page 276). Les chemins sont remarquablement liés et seuls quelques rares structures de motifs se trouvent isolées.

Constat 69 Il existe très peu de couples de motifs indépendants du reste de la structure principale.

677-§ Nous distinguons des foyers[489] de motifs dont le plus important[490] est **[_40]** auquel s'oppose **[8G_]** à travers des termes moyens comme par exemple **[8G_40]** ; puis suivent quatre foyers, à peu près équivalents, moins importants, **[ODC], [AM_], [OE_], [G_O]**.

[486] Nous rappelons que le latin est la langue qui possèdent le plus de motifs symétriques (Figure 35).

[487] Comparer les graphes pages 445-448.

[488] « S_S, _N_, _D_, _S_, _T_, T_T, _O_ »

[489] Nous ne tenterons pas d'associer avec des motifs de langues naturelles car nous sommes toujours dans la partie *compréhension* de la structure du cryptogramme.

[490] Dans l'ordre d'apparition dans le paragraphe : _qw?, 89_, 89_qw?, olfc, aw?_, o8_, 9_o.

Constat 70 Les motifs [_40],[8G_] sont les foyers principaux de connections ; [ODC], [AM_], [OE_], [G_O] sont des foyers secondaires mais très polarisés.

Se poser la question : comment expliquer le pourquoi du Constat 69 et du Constat 70 revient à se demander pourquoi il existe des motifs isolés dans les graphes de langues naturelles ?

678-§ En premier, il faut nous rappeler qu'un motif est représenté dans un graphe connexe si il est un constituant d'un chemin de motifs ; il y a cheminement dès lors qu'un motif est composé à partir d'un motif plus petit que lui (page 237) ; les motifs uniques ne sont donc pas présents dans le graphes.

679-§ Le plus petit chemin de motifs est composé de deux motifs. Si aucun des deux motifs ne participe à l'élaboration d'un autre chemin alors ce petit chemin est unique et constitue un groupe à lui tout seul.

Quand la diversité de motifs est totale il n'existe pas de connexion entre chemins de motifs.

680-§ Pour que des chemins soient interconnectés il est nécessaire qu'ils partagent un motif. Ce point commun est un terme moyen —peu courant dans les langues naturelles— qui est de plus en plus présent quand le niveau d'encryptage grandit ou lorsque plusieurs langues figures dans un même document. En d'autres termes, un graphe composé d'une seule structure n'est pas le graphe d'une langue naturelle puisque tous les chemins sont interconnectés par des termes moyens.

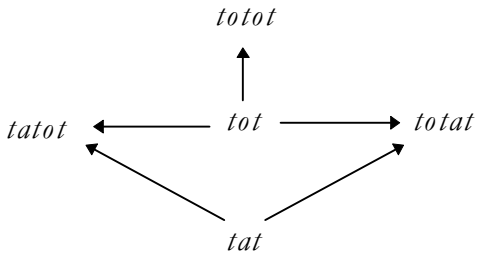
Aussi dans quel cas aboutissons-nous à un graphe composé d'une seule structure ?

681-§ La connexion des structures en une seule structure nécessite la modification des termes moyens d'une langue naturelle, créant quelques structures, en termes absolus reliant toutes les structures de motifs. Cette modification implique la substitution d'un élément[491] constitutif de ces termes.

682-§ Par exemple, considérons les trois motifs présents un certain nombre de fois : *x(totot), y(tatat)* et *z(tot),* seuls *totot* et *tot* sont liés mais *tatat* est un motif unique, qui si l'on désire qu'il participe au chemin *totot⊃tot,* il faut qu'une lettre du motif se modifie par substitution à représentation multiple en une autre lettre et permette ainsi l'apparition d'un nouveau motif : *(x-1)(totot), (totot), (y-1)(tatat), (tatat), (z-1)(tot) (tot)* devient *(x-1)(totot), (totat), (y-1)(tatat), (tatot), (z-1)(tot) (tat)* dont la représentation des connexions

[491] Au moins une lettre.

montre une seule structure.



Nous constatons donc que le manuscrit est issu d'un processus[492] qui utilise la variation du mode de représentation de ses éléments.

683-§ L'explication de la combinatoire d'entités en variation avec un contexte est plausible ; en cryptographie, nous appelons cela une substitution à représentations multiples cycliques dont la période peut être, comme les substituants, la variable du processus.

> **Constat 71 La structure unique du graphe connexe du manuscrit indique l'utilisation d'une représentation multiple cyclique : la notion de cycle[493] reste à définir.**

684-§ Dans tous les cas, l'opposition des deux foyers principaux **[8G_]** et **[_40]** est la démonstration de l'existence de deux langages. Elle conforte l'étude de CURRIER qui (page 162) avait été interpellé par le comportement du digramme **[8G]** et lui avait suggéré l'existence des langages *Hand A* et *Hand B*. Cependant, nous avons mis en exergue que le manuscrit contenait six types d'alphabets distincts, et que dans cette expectative, il existerait effectivement deux langages distincts —en premier repérables— mais qu'entre eux deux près de quatre autres langages seraient des déclinaisons —par représentations multiples— des deux langages *Hand A* et *Hand B*.

685-§ Or, « représentation multiple » ne signifie pas systématiquement encryptage par « représentation multiple » comme cela est le cas dans le code d'Henri III. La représentation multiple est présente dans la langue naturelle à différents niveaux.

686-§ Un document qui relate une classification numérique (Hypothèse 29) d'objets est enclin à être pourvu de nombreux éléments à représentations multiples. L'indexation

---

[492] Mode d'écriture ou d'encryptage.

[493] Nous avons vu qu'il n'existait pas de période d'encryptage liée à l'utilisation d'une clé d'encryptage de longueur fixe et de telle façon que cette clé soit répétée continuellement tout au long du texte (pages 157, 166 et 168). Cependant, l'utilisation de plusieurs clés de longueur variable et de répétitions variables sont difficilement détectables du fait même que les indices de leur présence s'entrecroisent.

numérique serait en ce cas la cause des nombreux termes moyens qui favorisent la connexion des chemins de motifs. En ce sens que le procédé de « représentation multiple » n'exclut pas l'hypothèse de la langue synthétique.

Tables des hypothèses, des constats et des conclusions intermédiaires

14 novembre 1998 —Première édition

Hypothèses

Constats

Conclusions intermédiaires

Conclusion

14 novembre 1998 —Première édition

Conclusion

•

L'APPLICATION de notre *artefact* cryptanalytique sur l'énigme du manuscrit de Voynich nous a conduit dans un dédale d'hypothèses, de constats, et de conclusions intermédiaires. Nous savions qu'une telle étude pouvait nous amener à l'incapacité de formuler une solution et nous ne prétendons pas être l'Oedipe attendu par un sphinx qui, frappé de mutisme, avait choisi l'écriture pour poser sa question. Cependant, nous énonçons trois conclusions générales répondant aux questions essentielles de la nature, sous-jacente et cryptée de ce texte.

La nature du texte

687-§ Le texte de VOYNICH fut considéré —dès le seizième siècle— comme un des ouvrages érudits de Roger BACON ; et de ce fait, de nombreuses hypothèses et conclusions se sont construites autour de ce qui apparaissait comme une évidence. John DEE proclamait sa parenté et son fils rapportait le fait que son père avait étudié un tel texte peu de temps avant qu'il se soit déplacé à Prague pour prétendument le vendre à Rudolph II de Bohème. Ce recoupement d'événements ne laissait aucun doute[494] aux analystes qui redécouvraient le manuscrit au début de notre vingtième siècle.

688-§ Partant de ce qui devenait une certitude, NEWBOLD induisait que le manuscrit datait du treizième siècle et qu'alors ce moine franciscain avait dû utiliser le latin pour rédiger le texte sous-jacent, et effectivement, les statistiques monogrammiques confirmaient cette supposition. Cette dynamique de recherche où l'hypothèse se confirme par des faits fut fatale à l'analyse de NEWBOLD qui ne concevait aucune autre solution que celle qui se lie à Roger BACON et à son siècle. Plus tard, FEELY remarque que le style d'écriture du *Docteur admirabilis* est un latin très abrégé et montre une différence avec le latin classique.

689-§ Ce début de remise en cause —de l'hypothèse devenue certitude— se confirma avec l'étude des digrammes de lettres du manuscrit qui révéla son inadéquation avec le latin. Cependant, comme pour contrecarrer cette nouvelle évidence, l'étude des digrammes du texte omis du caractère espace se trouvait proche de celle d'un texte latin. Voilà donc que la nature sous-jacente du texte n'était plus assurément latine **(P1)** et par conséquent l'auteur avait pu utiliser une autre langue —voire plusieurs— pour s'exprimer. Ce fut là encore une occasion de faire rejaillir Roger BACON comme

494 Complété par la lettre qui accompagnait le manuscrit (page 30) et indiquait que l'auteur probable était le « docteur *admirabilis* ».

titulaire de cette énigme : « n'avait-il pas écrit les sept méthodes pour dissimuler les écritures et en particulier de l'utilisation des langues grecques et sémitiques ? » ; aussi de nouvelles cryptanalyses furent faites mais sans succès **(P2)**.

Le problème de la détermination de la langue sous-jacente devenait la source d'hypothèses de plus en plus complexes qui impliquaient de visiter à nouveau la nature probable de l'encryptage du manuscrit.

690-§ Le pressentiment de FRIEDMAN et de TILTMAN évoluait vers l'hypothèse d'un système d'écriture basé sur la codification d'un langage universel synthétique **(P3)**. Il est vrai que Marcus MARCI avait envoyé le manuscrit à Athanasius KIRCHER qui lui-même venait d'écrire un ouvrage sur la langue universelle ; cependant, ce serait pure supposition que de dire : « MARCI le lui a transmis pour cette raison » et le fait que KIRCHER ait décrypté les hiéroglyphes égyptiens serait certainement le réel motif de l'allusion aux « sphinx ».

691-§ TILTMAN avait remarqué des structures de symboles qu'il catégorisait en trois positions dans les mots et il exprima l'idée qu'il existait des analogies avec le système de Cave BECK que les folios de « cercles concentriques » —aux apparences Lulliennes— confortent ; seulement , ils ne décrivent pas de relation entre les symboles du manuscrit et des éléments propositionnels de textes clairs. La recherche de règles de fonctionnement de cette hypothétique langue synthétique est donc fondamentale pour la poursuite du travail de TILTMAN.

692-§ L'étude trigrammique se montra riche en enseignements et permit de mettre en valeur des comportements particuliers liés à des syntaxes de positionnement dans les mots. La nature bivalente des trigrammes —rigoureusement internes et distants des deux extrémités des mots— révèle quatre familles[495] commençant respectivement par la lettre , la lettre  , la lettre  et la lettre  . Ce constat est intriguant, existe-t-il un lien réel entre ces lettres, entre nos trigraphes et les trigraphes spéciaux de Cave BECK dont la première lettre est soit « s » ou soit « t » ? La tentation est forte mais cette coïncidence a peut-être autant de valeur que celle qui montre une coïncidence entre les statistiques monogrammiques du manuscrit et celles du latin.

693-§ Nous ne détachons pas notre analyse des autres méthodes probablement utilisées pour l'encryptage de cette énigme. Nous pratiquons donc une recherche de périodicité qui nous amène à observer une lettre excessivement représentée dont l'attitude est d'occuper des positions communes dans des pages successives ; mais cette périodicité n'est pas celle que nous observons dans le système de VIGENÈRE, ou de PORTA, et nous ne concevons pas que « ces coïncidences » soient fortuites : quelles

[495] Sur l'ensemble des deux transcriptions de CURRIER et de FRIEDMAN.

qu'elles soient, elles sont l'expression de la méthodologie employée pour la rédaction du manuscrit. Nous savons que la langue de Raymond LULLE —alors contemporain de Roger BACON— emploie une lettre particulière comme un indicateur de changement de référence. Cet artifice mnémotechnique prend la même attitude d'une excessive représentation, seulement notre lettre **o** se place en quelque endroit du mot et ne correspond pas alors à cette lettre particulière de LULLE. Pourtant, il y a ces « cercles concentriques » dont les dimensions et leurs fonctionnalités apparentes ressemblent aux cercles des combinatoires d'entités Lulliennes. Or, ces cercles représentent des moyens de substitutions à représentations multiples que nous retrouverons dans les siècles suivants.

Nous décidons d'appliquer notre méthode de recherche en représentations multiples et, dans le cas favorable, de reconstituer les dictionnaires de substitutions.

694-§ Sur l'ensemble du manuscrit nous ne détectons pas plus d'une famille de codes à représentation multiple, mais lorsque nous étudions chacune des pages du manuscrit alors, nous découvrons qu'en chacune des positions p_i des vocables, il existe un alphabet de substitution de dimension variable et fonction de p_i, de telle sorte qu'un alphabet de substitution, pour une position p_i d'un mot m_i, se crée à partir de l'alphabet du mot m_{i-1} à la position p_{i-1}. La conséquence est que la transition des symboles de VOYNICH entre positions d'un même mot est réglementée par des jeux de substitutions remarqués dans un folio mais indécelables sur l'ensemble du manuscrit : il existe donc des comportements locaux très forts de représentations multiples.

695-§ A présent, si l'on considère les relations entre les mots du manuscrit alors notre surprise est encore plus grande. Nous constatons que les positions p_i —sur lesquelles s'effectuent les substitutions— sont diversifiées en symboles de VOYNICH selon un principe de construction basé sur un accroissement logique du mot. L'initiation de la construction est faite ainsi : la première position du mot est une position plus diversifiée que la deuxième position de ce mot. La deuxième position du mot est moins diversifiée que la troisième position ; puis la dernière position du mot est régie par la règle suivante : lorsqu'une position n est au moins égale à 4, elle est plus diversifiée que la position $n-1$, si le mot est de n lettres sinon, elle est moins diversifiée que la position $n-1$.

SYNTHESE* —La nature sous-jacente du texte manuscrit repose sur un processus d'élaboration synthétique qui admet des propositions de dimensions différentes et dont les alphabets utilisés dépendent de fonctions locales.

Nature de la substitution

696-§ La croyance que Roger BACON était l'auteur du manuscrit influait sur les

hypothèses de la technique d'encryptage employée. Dans son traité, *de la pierre philosophale et de la puissance de la nature,* BACON détaille ses moyens de sécurisation qui reposent sur la méthodologie de la substitution monoalphabétique, et, par conséquent, elle ne devait pas présenter de complexité à l'analyste **(E1)**. L'enthousiasme fut d'autant plus grand que les statistiques monogrammiques du manuscrit n'infirmaient pas cette supposition. Cependant, l'analogie avec le latin ne se présentait qu'à travers l'étude des lettres prises une à une et leurs associations avec des entités claires ne permettait pas —quelles que soient les langues naturelles connues de Roger BACON— d'obtenir le texte original. Une bribe, « *multos...portas »,* placée en fin de document laissa NEWBOLD penser que le procédé cryptographique était une succession d'opérations.

Bien que les tentatives de NEWBOLD échouèrent, il restait les hypothèses de la substitution multigraphiques.

697-§ Une première façon de faire consiste à considérer le manuscrit comme le résultat d'une substitution d'une lettre claire par deux ou trois symboles de VOYNICH **(E2)**. La conséquence directe de cette manipulation est de provoquer une multiplication de la dimension du cryptogramme, nous ne le constatons pas dans notre analyse de la diversité de ses motifs symétriques et redondants, nous constatons le phénomène inverse ; c'est-à-dire, le manuscrit se présente sous une forme « condensée » plutôt « qu'expansée » **(E3)**. Il y aurait alors une tendance à ce qu'un symbole de VOYNICH corresponde à plusieurs lettres claires. L'hypothèse selon laquelle deux à trois symboles de VOYNICH seraient substitués à deux à trois lettres claires ne peut donc être envisagée **(E4)**.

698-§ Le système présent dans le manuscrit rejette les substitutions monographiques et multigraphiques aussi sommes-nous tentés de croire —comme TILTMAN— que la substitution est un amalgame de genres différents de substitutions **(E5)**. Les variations d'écarts entre mots et la mise en évidence de cinq types de dictionnaires de substitution plaideraient pour un encryptage à options multiples. Est-ce que la substitution polyalphabétique correspond à ces constats ? Nous ne le pensons pas. Bien que le manuscrit ait les attributs symétriques d'une polysubstitutions, la proportion de motifs redondants est trop différente, de même, la recherche d'une période d'encryptage nous a conduit à l'impossibilité de prouver sa présence **(E8)**.

699-§ Aussi, l'indétermination d'une période constante nous suggère la probable existence d'une évolution de la substitution par une modulation des alphabets utilisés **(E6)**-**(E7)**. En effet, l'étude du manuscrit dans sa globalité montre qu'un alphabet de trente symboles est utilisé, pourtant, lorsque nous étudions le manuscrit page après page, nous remarquons qu'il existe six alphabets aux modes statistiques différents et qu'une page comporte au moins seize symboles et au plus vingt-sept symboles : ce qui signifie que la totalité des symboles mis à la disposition du rédacteur n'est pas utilisée localement. Ce dernier point corrobore la découverte de dictionnaires de

substitutions. De plus, l'étude de la connexion des motifs symétriques et redondants du manuscrit révèle l'utilisation de termes moyens —alphabets à représentations multiples— comme agents de médiation entre chemins de motifs qui normalement sont des structures autonomes. L'aspect monolithique du graphe connexe de ces motifs est l'expression d'une représentation multiple dont la substitution est dépendante de règles indéterminées.

> **SYNTHESE* —Le manuscrit n'est pas un cryptogramme construit à partir d'une substitution multigraphique. L'étude locale de ce texte montre un emploi d'alphabets différents propres à la substitution évolutive par représentation multiple. Les langages *Hand A* et *Hand B* sont donc la partie visible de cette énigme et dont la partie immergée est constituée des déclinaisons de ces deux langages.**

Autres natures

700-§ La représentation multiple a pour incidence d'offrir une palette de symboles bien plus importante que nécessaire. Cette abondance se ressent comme un surplus qui pourtant ne peut être pris pour inutile. Les trente symboles du manuscrit sont *a priori* nombreux quand ils sont utilisés dans un même cryptogramme ; cependant, nous savons que le nombre maximal de lettres de cet alphabet nécessaire à l'écriture d'une page de ce manuscrit est de vingt-trois lettres de VOYNICH[496] **(T1)**, l'ajout de ces lettres ne signifie pas « ajout de signifiant » et plus insidieusement cette profusion de symboles peut dissimuler la suppression de lettres habituellement détectables par leurs implications dans la construction des vocables **(T2)**. La diversité de motifs symétriques et redondants d'après la dimension du manuscrit nous signale une représentation excessive de cette diversité comme si il avait été diminué de la moitié de ses symboles —compensée par des alphabets multiples— et qu'alors, il est envisageable qu'une des opérations cryptographiques concerne la suppression d'une partie des lettres. Peut-on avoir idée de la nature de ces lettres ? Le premier indice dit que le texte clair s'est vu ôter près de la moitié de ses lettres, il est probable que cette proportion corresponde globalement à celle des voyelles.

701-§ L'étude de la diversité de motifs symétriques et redondants place le manuscrit de Voynich dans la situation d'un texte dépourvu de voyelles ; mais aussi, la proportion de chemins d'inclusion de motifs et leur degré d'inclusion sont très au-dessus de ceux constatés pour un texte pourvu de voyelles, tandis que cette proportion de chemins et de degrés d'inclusion s'intègre parmi celles des textes sémitiques. L'expérience faite sur le texte *Gaudeamus Igitur* —en latin médiéval— montre en effet que la suppression de ses voyelles tend à le rapprocher du manuscrit de Voynich. Seulement, peut-on pour autant conclure que nous avons affaire à un texte consonantique ? Oui, si nous

[496] Transcription de FRIEDMAN.

remettons en cause notre conclusion sur la nature du texte, non si l'on considère la proportion de motifs symétriques qui, même dans une version consonantique conjuguée de substitutions à représentations multiples, ne suffit pas à expliquer la surabondance de motifs redondants : or, aucun système classique d'encryptage ne correspond à ce comportement si ce n'est celui qui implique la condensation de groupe de lettres en symbole.

> **SYNTHESE* —Les analogies consonantiques sont les expressions d'une forme particulière d'énonciation qui procède de la condensation de l'information.**

702-§ Or, cette réduction s'explique aussi par l'utilisation d'apostrophismes, mais mis à part le comportement de la lettre **o** qui s'intercale avec une agaçante véhémence, nous n'affirmons rien **(T3)**. Est-elle une lettre nulle ? Nous constatons effectivement qu'elle est représentée dans une proportion anormale comparable à la lettre mnémotechnique « T » de la langue philosophique de Raymond LULLE, et équivalente à la présence du caractère espace d'un texte. Ces remarques montrent effectivement que la lettre **o** a le comportement d'une lettre dispensable[497]. Cependant, lorsque nous pratiquons une étude locale, nous constatons qu'il existe quatre autres lettres **c, cr, 9, a,** susceptibles d'être assimilées à des lettres nulles **(T4)**.

> **SYNTHESE* —Il existe potentiellement cinq symboles capables de jouer le rôle de la lettre nulle si l'on considère le manuscrit comme un assemblage de cryptogrammes, sinon seule la lettre o peut jouer ce rôle.**

703-§ La dernière problématique essentielle concerne l'hypothèse de la construction anagrammatique **(T5)**. Nous n'avons pas observé d'inversion périodique des lettres des mots. Pour FRIEDMAN et TILTMAN, le manuscrit n'en est pas doté. En fait, l'hypothèse anagrammatique ne pourrait pas expliquer les règles de construction des mots que nous avons mis en exergue, elle n'expliquerait guère plus le principe des substitutions à représentations multiples, par contre, son seul emploi autoriserait le déploiement du champ incertain de la reconstruction anagrammatique.

Perspectives

704-§ Nous n'avons pas abouti à la solution du manuscrit de Voynich. Notre quête nous a toutefois permis d'étayer les trois principaux axes sur lesquels nous devrons

[497] La suppression d'une lettre dispensable améliore la lisibilité du texte : c'est le cas de la suppression d'une lettre nulle.

poursuivre notre cryptanalyse.

705-§ La première orientation concerne l'étude des langues synthétiques développées — aux cours du XIII^{ème}, XIV^{ème}, XV^{ème} et XVI^{ème} siècle— en privilégiant les langues qui expriment l'idée de classification proche de celle de Cave BECK et d'Athanasius KIRCHER. Seulement, leur étude nécessitera la transcription de textes médiévaux — issus de la construction propositionnelle de ces langues— en textes interprétables par nos outils d'analyse et qui nous permettront, comme nous l'avons déjà fait sur le manuscrit de Voynich, d'évaluer les conséquences sur leurs énonciations en répondant aux trois questions :

- Est-ce que cette langue synthétique procède d'une condensation de l'information similaire à celle constatée dans l'approche consonantique des textes de langues naturelles ?

- Est-ce que les règles de construction des vocables du manuscrit se retrouvent dans la langue synthétique étudiée ?

- Est-ce que les lettres que nous estimons être à « caractère nul » sont assimilables à certaines lettres de la langue synthétique étudiée ?

706-§ Le deuxième axe que nous exploiterons sera celui d'une étude approfondie de la notion de « cycle » ou de « variabilité » de l'utilisation des substitutions à représentations multiples. Il nous faudra tenter de dissocier les différents langages qui interviennent dans la rédaction du manuscrit que nous savons être, plus de deux et, pas plus de six.

707-§ Finalement, le troisième axe est un chemin sur lequel nous n'avons pas voulu émettre d'interprétation pour ne pas nous placer dans la situation indélicate de FEELY, STRONG et LEVITOV, qui associèrent le dessin au discours du texte. Nous aborderons l'étude des représentations multiples des figures —comme celle que nous avons déjà hypothéquée en Hypothèse 5— et surtout, celles dont l'inspiration semble être issue d'un procédé de langue synthétique que nous retrouvons sous formes de « réseaux de rosettes » ou de « cercles concentriques ».

708-§ La synthèse de ces trois axes de recherche sera la mise en adéquation du fonctionnement d'une langue synthétique —avec celui des « rosettes » et en fonction des différents langages— de structure analogue au manuscrit de Voynich.

E q u a t i o n s

F i g u r e s

T a b l e a u x

Bibliographie

14 novembre 1998 —Première édition

Bibliographie

•

Pour conduire l'étude du manuscrit de Voynich nous avons établi trois catégories de documents. Nous avons recueilli les enseignements de la cryptanalyse dans les ouvrages que nous réunissons sous l'intitulé « Artefact ». Une seconde catégorie d'ouvrages concerne, « Les mots du langage », leur utilisation. Enfin, le troisième groupe est une collection d'ouvrages abordant, chacun sous un angle différent, la problématique de la reconnaissance et de la mesure des structures de motifs.

Artefact

[AENE1990] AENEAS Le Tacticien, How to Survive under Siege, Oxford University Press, 1990.

[BACO1557] BACON Roger, De l'admirable pouvoir et puissance de l'art, & de nature, ou eft traicté de la pierre philofophale, Traduit par Jacques Girard de Tournus, édité par Macé Bonhomme, Lyon, 1557.

[BARK1995] BARKER Wayne G., Cryptanalysis of the double transposition cipher, Aegean Park Press, n°69, 1995.

[BECK1657] BECK Cave, The Universal Character, Londres, 1657.

[CALL1985a] CALLIMAHOS Lambros, FRIEDMAN William, Military cryptanalytics, n°42, Part I-Vol n°1, Aegean Park Press, 1985.

[CALL1985b] CALLIMAHOS Lambros, FRIEDMAN William, Military cryptanalytics, n°43, Part I-Vol n°2, Aegean Park Press, 1985.

[CALL1985c] CALLIMAHOS Lambros, FRIEDMAN William, Military cryptanalytics, n°44, Part II-Vol n°1, Aegean Park Press, 1985.

[CALL1985d] CALLIMAHOS Lambros, FRIEDMAN William, Military cryptanalytics, n°45, Part II-Vol n°2, Aegean Park Press, 1985.

[CASA1994] CASANOVA Antoine, Cryptanalyse de textes chiffrés, Université PARIS 8, 1994, Caractérisation des relations textuelles entre ADNc et protéines, Université PARIS 8 et PARIS 7, 1995.

[CESA1964] CESAR Jules, La guerre des Gaules, G-F Flammarion, 1964.

[CURR1976] CURRIER Prescott H., Some Important New Statistical Findings, edited by Mary D'IMPERIO Seminar on 30th November in Washington D,C, 1976.

[DAVI1995] DAVIES Donald Watts, La sécurité dans les réseaux informatiques, AFNOR, page 68—71, Paris, 1995.

[DELA1902] DELASTELLE Felix Marie, Traité élémentaire de cryptographie, Gauthier-Villars, Paris, 1902.

[DUCL1992] DUCLOUX Gérard, Sécurité des réseaux et cryptographie, Centre solutions SystemView et sécurité Stratégie et marketing réseaux Tour Descartes IBM France, octobre 1992.

[FEEL1943] FEELY Joseph M., Roger Bacon's cipher : The right key found, Rochester, New York, 1943.

[FRIE1922] FRIEDMAN William Friedriech, The index of coincidence and its applications in cryptanalysis, Aegean Park Press, réimpression de l'édition de 1922, 1976.

[FRIE1959] FRIEDMAN William, FRIEDMAN Elizabeth, Acrostics Anagrams and Chaucer, Philological Quarterly, n°38, page 1—20, 1959.

[FRIE1962] FRIEDMAN Elizabeth, The most mysterious MS -Still an Enigma, Washington DC, Port, 5 août 1962.

[GURN1789] GURNEY Thomas, Brachygraphy or an easy and compendious system of short-hand, London Acts Directs, Londres, 1789.

[HODG1988] HODGES Andrew, Alan Turing : the enigma of intelligence, Payot, Paris, 1988.

[IMPE1980] IMPERIO Maria d', The Voynich manuscript, an elegant enigma, Aegean Park Press, n°27, 1980.

[KAHN1980] KAHN David, La guerre des codes secrets, InterEditions, 1980.

[KASI1863] KASISKI Friedrich W., Die geheimschriften und die dechiffrier kunst, Berlin, 1863.

[KULL1977] KULLBACK Solomon, Statistical methods in cryptanalysis, Aegean Park Press, n°4, 1977.

[LAND1997] LANDINI Gabriel, Adresse Internet http://sun1.bham.ac.uk/G.Landini/evmt/, Projet Européen pour le décryptement de MS408, 1997.

[LERV1976] LERVILLE Edmond, Les cahiers secrets de la cryptographie, Edition du Rocher, Monaco, 1976.

[LEVI1987] LEVITOV Leo, Solution of the Voynich manuscript, a liturgical manual for the Endura rite of the Cathari Heresy, the cult of Isis, Aegean Park Press, Laguna Hills, 1987.

[NEIL1944] O'NEIL Hugh, Botanical Observations of the Voynich MS, Speculum, page 126, 19 janvier 1944.

[NOLA1902] NOLAN Edmond, HIRSCH S., A., The greek grammar of Roger

Bacon, The Cambridge University Press, 1902.

[PORT1563] PORTA Jean-Baptiste, Magia naturalis, Naples, 1558, De furtivis litterarum notis, vulgo de ziferis, Naples, 1563.

[PRAT1940] PRATT Fletcher, Histoire de la cryptographie, Bibliothèque historique, Payot, Paris, 1940.

[SEBE1989] SEBERRY J., PIEPRZYK J., Cryptography, an introduction to computer security, Prentice Hall, 1989.

[SEST1710] SESTRI Jean, Metodo brevissimo e assoluto per scrivere in cifra, Rome, 1710.

[SGDN1991] SGDN, Secrétariat Général de la Défense Nationale, DISSI/SCSSI, n°400 & n°480, 1991.

[SHAN1949b] SHANNON Claude Eduard —Secrecy, Communication theory of secrecy systems, Bell Syst, Tech, J,, Vol n°28, page 656—715, 1949.

[SINK1968] SINKOV A., Elementary Cryptanalysis, Mathematical Association of America, a mathematical approach, Random House, New York, 1968.

[STAL1998] STALLINGS Dennis J., Understanding the second-order entropies of Voynich text, compte-rendu EVMT, 27 avril 1998.

[STRO1945] STRONG Leonell C., Anthony Askham : the author of the Voynich MS, Science, Vol n°101, pp 608—609, 15 juin 1945.

[TILT1951] TILTMAN John H., Interim report on the Voynich MS : personal communication to W. F. Friedman, 5 mai 1951.

[VIGE1586] VIGENERE Blaise de, Traictés des chiffres ou secrètes manières d'escrire, Paris, 1586.

Les mots du langage

[AFL1998] AFL, Association Française pour la Lecture, Intervention aux cours d'apprentissage à la lecture flexible, IUT-Montreuil, 1998.

[AROM1996] AROMATICO Andrea, Alchimie, le grand secret, découverte Gallimard, 1996.

[BACK1932] DE BACKER Augustin, SOMMERVOGEL Carlos, Bibliothèque de la Compagnie de Jésus, Première partie: Bibliographie par les Pères Augustin et Aloys De Backer, Seconde partie : Histoire par le Père Auguste Carayon, Nouvelle édition par Sommervogel Carlos, Picard, Paris, 1890-1932.

[BEAU1986] BEAUME Edmond, La lecture, Préalables à sa pédagogie, Association Française pour la lecture, 1986.

[CHAM1823] CHAMPOLLION Lejeune J-F., Panthéon Egyptien, Collection des personnages mythologiques de l'ancienne Egypte, 1823, inter-livres, Paris, 1992.

[CHAM1841] CHAMPOLLION Lejeune J-F., Les Principes généraux de l'écriture sacrée égyptienne appliquée à la représentation de la langue parlée ou Grammaire égyptienne, Institut d'Orient, Paris, 1984 de 1841.

[CHAM1989] CHAMPOLLION Hervé, L'Egypte de J-F. CHAMPOLLION, Lettres et Journaux de voyage, Image & Magie, 1989.

[ECO1994] ECO Umberto, La recherche de la langue parfaite dans la culture européenne, SEUIL, 1994.

[ETHN1986] ETHNOMETHODOLOGIES, Pratiques de Formation, Université PARIS 8, Saint-denis, n°11—12, octobre 1986.

[FISC1986] FISCHER Henry George, L'écriture et l'art de l'Egypte ancienne, Collège de France, Essais et Conférences, Presses Universitaires de France, 1986.

[FOUC1994] FOUCAMBERT Jean, La manière d'être lecteur : apprentissage et enseignement de la lecture, Albin Michel, Paris, 1994.

[GUIR1963] GUIRAUD Pierre, Les mots français, Cité par Henri MITTERAND, Que sais-je ?, n°270, Presses Universitaires de France, 1963.

[JAUS1893] JAUSSEN Tepano, L'ile de Pâques, historique et écriture, Bulletin de Géographie Historique et Descriptive, n°2, Paris, 1893.

[JEAN1987] JEAN Georges, L'écriture mémoire des hommes, découvertes Gallimard, 1987.

[JERP1989] JERPHAGNON Lucien, Histoire de la pensée —Antiquité et Moyen âge, TALLANDIER, 1989.

[LEIB1690] LEIBNIZ Gottfried Wilhelm —Essai, Nouveaux essais sur l'entendement humain, GF-Flammarion, 1990 réédition de 1690.

[LEVY1987] LEVY Pierre, La machine univers, La découverte, collection Sciences, 1987.

[MAND1965] MANDELBROT Benoît, Information theory and psycholinguistics, in Wolfmam B, B, and Nagel E, Scientific psychology Basic Books, 1965.

[MARL1977] MARLER P., R., PETERS S., Selective vocal learning in a sparrow, Science, Vol n°198, page 519—521, 1977.

[MOLE1971] MOLES Abraham, La communication, Retz, Paris, 1971.

[MULL1968] MULLER Charles, Initiation à la statistique linguistique, Larousse, Paris, 1968.

[ORL1988] ORLIAC Catherine, ORLIAC Michel, Des dieux regardent les étoiles, les derniers secrets de l'ile de Pâques, Découverte Gallimard Histoire, 1988.

[PAUL1937] PAUL Guillaume, La psychologie de la forme, Flammarion, Paris, 1937.

[PIER1966] PIERCE John-Robinson, Symboles, signaux et bruit, MASSON, sofradel, Paris, 1966.

[RUES&BATE1988] RUESCH Jurgen, BATESON Gregory, Communication et Société, Paris, SEUIL, 1988.

[SALT1991] SALTON Gérard, Developments in automatic text retrieval, Science, Vol n°253, page 974—980, août 1991.

[TERS1968] TERS François, Co-auteur MAYER & REICHENBACH, Vocabulaire orthographique de base, O.C.D.L., Paris, 1968.

[VIVA1967] VIVARAIS, Architecture des églises romanes du Vivarais, Edition FERN, 1967.

[WATZ1980] WATZLAWICK Paul, Le langage du changement, éléments de communication thérapeutique, SEUIL, 1980.

[WITT1961] WITTGENSTEIN Ludwig, Tractatus logico-philosophicus & Investigations philosophiques, Gallimard, 1961.

[ZIPF1935] ZIPF George Kingsley, The psycho-biology of language, Hought Mifflin Co, Boston, 1935.

[ATLA1992] ATLAN Henri, L'organisation biologique et la théorie de l'information, Hermann, 1992.

[BENN1976] BENNET William Ralph, Scientific and Enginneering Problem Solving with the Computer, Englewwood Cliffs, PRENTICE-HALL, 1976.

[BRISS1991] BRISSON Luc, Inventer l'univers, le problème de la connaissance et les modèles cosmologiques, Les belles lettres, Collection L'âne d'or, 1991.

[CHOM1957] CHOMSKY Noahm, Syntactic structures, Mouton & Co, La Haye, 1957.

[DAMA1995] DAMASHEK Marc, Gauging Similarity with n-Grams : Language-Independant Categorization of Text, Science, Vol n°267, page 843—848, février 1995.

[KINC1957] KINCHIN A. I., The mathematical foundations of information theory, Dover New-York, 1957.

[LEGR1994] LEGRAS Bernard, Eléments de statistique, Collection « Outils et Méthodes », Presses Universitaires de Nancy, 1994.

[LEIB1714] LEIBNITZ Gottfried Wilhelm, La Monadologie, Le livre de poche, réédition de 1714, 1991.

[LIND1968] LINDENMEYER Aristid, Mathematical models for cellular interaction in development I-II, Journal of theorical Biology, n°18, page 280—315, 1968.

[LOCH1994] LOCHAK Georges, La géométrisation de la physique, Flammarion, Nouvelle bibliothèque scientifique, Paris, 1994.

[MALL1989] MALLAT Stéphane, A theory for multiresolution signal decomposition, The wavelet representation, IEEE PAMI, Vol n°11, n°7, page 674—693, 1989.

[MAND1997] MANDELBROT Benoît — FHF, Fractales, Hasard et Finances, Champs Flammarion, 1997.

[MARK&PETR1981] MARKOV Andreï Andreïevitch, Etude des chaines linguistiques du roman Russe en vers d'A,S Puskin: 'Evgenij onegin', PETRUSZEWYCZ Micheline, Les chaînes de Markov dans le domaine linguistique, Slatkine, Genève & Paris, 1981.

[MEYE1987] MEYER Yves, L'analyse par ondelettes, Pour la Science, page 28—37, septembre 1987.

[MONI1996] MONIER Jean-Marie, Algèbres, DUNOD, 1996.

[OSWA1986] OSWALD Jacques, Theorie de l'information ou analyse diacritique des systèmes, Masson, Paris, 1986.

[PAIR1988] PAIR Claude, MOHR Roger, SCHOTT René, Construire les algorithmes, DUNOD Informatique, Paris, 1988.

[PRUS1989] PRUSINKLEWICZ Przemyslaw, Lindenmayer systems, fractals and plants, Lecture notes in biomathematics, Springer-Verlag New-York, n°79, 1989.

[RUBE1993] RUBENKING Neil, Programmeur Turbo Pascal, Ziff-Davis Press & DUNOD Tech, 1993.

[SALO1985] SALOMAA Arto, Computation and automata, Cambridge University Press, 1985.

[SCIE1998] POUR LA SCIENCE, Les symétries de la nature, Dossier Hors-série, Juillet 1998.

[SHAN1949a] SHANNON Claude Edouard —Theory, The mathematical theory of communication, Université de l'Illinois, 1949.

[SHAN1951] SHANNON Claude Edouard —Prediction, Prediction and entropy of printed English, Bell Syst, Tech, J, Vol n°30, page 50—64, 1951.

[VOLL1989] VOLLAT Patrick, Calculabilité effective et algorithme théorique, EYROLLES, Paris, 1989.

[WEYL1952] WEYL Hermann, Symmetry, Princeton University Press, 1952.

[WIRT1987] WIRTH Niklaus, Algorithmes et structures de données, EYROLLES, 1987.

14 novembre 1998 —Première édition

Index

14 novembre 1998 —Première édition

Index

A

B

C

14 novembre 1998 —Première édition

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

UNIVERSITE PARIS 8

U.F.R. LANGAGE, INFORMATIQUE, TECHNOLOGIE

ANNEXE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE PARIS 8

Discipline : science de l'information et de la communication

présentée et soutenue publiquement

par

Antoine CASANOVA

Titre : méthodes d'analyse du langage crypté : Une contribution à l'étude du manuscrit de Voynich

---

Directeur de thèse : M. LEPERS Jean-Marc

---

14 novembre 1998 —Première édition

Avertissements

●

709-§ Le travail d'analyse de textes cryptés nécessite de nombreux calculs quantitatifs et qualitatifs sur lesquels les autres membres cryptologues peuvent se baser pour pratiquer leurs propres expériences d 'analyses.

710-§ Ce second volume intitulé *Annexe* est fondamental dans la *pratique de terrain* du cryptanalyste. C'est un précieux index rempli de données référencées, qui ouvre d'autres voies d'exploration par la combinatoire que chacun peut appliquer aux données, dans lequel nous puisons l'information utile à la validation ou à la réfutation d'hypothèses.

711-§ Nous y trouvons trois parties spécifiques. La première partie est classique, elle fournit des précisions sur les textes utilisés pour positionner notre analyse ainsi que les informations[498] recueillies à leur propos. La deuxième partie est consacrée aux informations intrinsèques au manuscrit de Voynich. La troisième et dernière partie comprend les graphes connexes des motifs symétriques et redondants du manuscrit et de textes en langues naturelles.

[498] Calculs statistiques, probabilistes, markoviens, symétries, redondances et contextes.

Table des matières

Annexe

Références & Résultats

•

Références & Résultats sur des textes de langues naturelles

Sources et références du manuscrit de Voynich

Graphes connexes des motifs symétriques et redondants

Annexe

Références & Résultats

14 novembre 1998 —Première édition

Références & Résultats sur des textes de langues naturelles

•

14 novembre 1998 —Première édition

Textes anglais et français classés par titre

TEXTE	AUTEUR	TITRE
carol.txt	Dickens Charles	A christmas carol
alice.txt	Carrol lewis	Alice's adventures wonderland
antigo.txt	Sophocles	Antigone
eighty.txt	Verne Jules	Around the world in 80 days
athene.txt	Aristotle	Athene
atlan.txt	Bacon Francis	Atlantis
cand.txt	Voltaire	Candide
criton1.txt	Platon	Criton partie 1
criton2.txt	Platon	Criton partie 2
criton3.txt	Platon	Criton partie 3
opi.txt	Plutarque	Des opionions des philosophes
dracu10.txt	Stoker Bram	Dracula
plur.txt	Fontenelle	Entretiens sur la pluralite des mondes
fables.txt	Aesop	Fables
frank10.txt	Wollstonecraft Mary	Frankeinstein
moon.txt	Verne Jules	From the Earth to the moon
lastbo.txt	Doyle Conan	His last bow
histoir.txt	Aristotle	History of animals
hound.txt	Doyle Conan	Hound of Baskervilles
ilia01.txt	Homer	Illiad
jabber.txt	Carroll lewis	jabber wocky
meth.txt	Descartes René	Le discours de la methode
augle.txt	Saint Augustin	Les lettres de Saint Augustin
miser.txt	Hugo Victor	Les misérables
rev.txt	Rousseau	Les reveries du promeneur solitaire
odys1.txt	Homer	L'odyssée
lordji.txt	Conrad joseph	Lord Jim
manuel.txt	Criton	Manuel
guer.txt	Tayac CIA	Manuel de guerrilla CIA
hum.txt	Malebranche	Meditations sur l'humilite et la penitence
micro.txt	Voltaire	Micromegas
oed1.txt	Sophocles	Oedipus the king vol 1
oed2.txt	Sophocles	Oedipus the king vol 2
libert.txt	Stuart Mill John	On liberty
darwin.txt	Darwin Charles	Origin of species
parlos.txt	Milton John	Paradise lost
pargai.txt	Milton John	Paradise regained
pd_2.txt	Un Docteur de la Sorbonne	Pensées diverses, comete de décembre 1680
dgray.txt	oscar wilde	Picture of Dorian Gray
rhetor.txt	Aristotle	Rhetoric
round.txt	Verne Jules	Round the moon
signfo.txt	Doyle Conan	Sign of four
snark.txt	Carroll Lewis	Snark
study.txt	Doyle Conan	Study in scarlet
opar.txt	Burroughs Edgar rice	Tarzan and the Jewels of Opar
tarzan.txt	Burroughs Edgar Rice	Tarzan of the Apes
advent.txt	Doyle Conan	The adventures of sherlock holmes
sunzu.txt	Sun Tzu	The art of war
callwi.txt	London Jack	The call of the wild
casebo.txt	Doyle Conan	The case book of sherlock holmes
chimes.txt	Dickens Charles	The chimes
crick.txt	Dickens Charles	The cricket on the heart
godsma.txt	Burroughs Egdar Rice	The gods of mars
darkne.txt	Conrad Joseph	The heart of darkness
invism.txt	Wells herbet george	The invisible man
jungle.txt	Burroughs Egdar rice	The jungle tales of Tarzan
lostwo.txt	Doyle Conan	The lost world
ozland.txt	Bum Frank	The marvelous land of Oz
pit.txt	Poe Egdar Allan	The pit and the Pendulum
sharer.txt	Conrad Joseph	The secret sharer
hydea10.txt	Stevenson Robert Louis	The strange case of Dr Jekyll and Mr Hyde
women.txt	Stuart Mill John	The subjection of women
timema.txt	Wells Herbet George	The time machine
beagle.txt	Darwin Charles	The voyage of beagle
warwo.txt	Wells Herbet George	The war of the worlds
wizoz.txt	Baum Frank	The wonderful wizard of Oz
world90.txt	CIA	The world factbook 1990
worl9.txt	CIA	The world factbook 1992
look.txt	Carroll lewis	Through the looking glass
twocity.txt	Dickens Charles	Two city

Textes anglais et français classés par Auteur

TEXTE	AUTEUR	TITRE
fables.txt	Aesop	Fables
athene.txt	Aristotle	Athene
histoir.txt	Aristotle	History of animals
rhetor.txt	Aristotle	Rhetoric
atlan.txt	Bacon Francis	Atlantis
wizoz.txt	Baum Frank	The wonderful wizard of Oz
ozland.txt	Bum Frank	The marvelous land of Oz
opar.txt	Burroughs Edgar rice	Tarzan and the Jewels of Opar
tarzan.txt	Burroughs Edgar Rice	Tarzan of the Apes
godsma.txt	Burroughs Egdar Rice	The gods of mars
jungle.txt	Burroughs Egdar rice	The jungle tales of Tarzan
alice.txt	Carrol lewis	Alice's adventures wonderland
jabber.txt	Carroll lewis	jabber wocky
snark.txt	Carroll Lewis	Snark
look.txt	Carroll lewis	Through the looking glass
world90.txt	CIA	The world factbook 1990
worl9.txt	CIA	The world factbook 1992
lordji.txt	Conrad joseph	Lord Jim
darkne.txt	Conrad Joseph	The heart of darkness
sharer.txt	Conrad Joseph	The secret sharer
manuel.txt	Criton	Manuel
darwin.txt	Darwin Charles	Origin of species
beagle.txt	Darwin Charles	The voyage of beagle
meth.txt	Descartes René	Le discours de la methode
carol.txt	Dickens Charles	A christmas carol
chimes.txt	Dickens Charles	The chimes
crick.txt	Dickens Charles	The cricket on the heart
twocity.txt	Dickens Charles	Two city
lastbo.txt	Doyle Conan	His last bow
hound.txt	Doyle Conan	Hound of Baskervilles
signfo.txt	Doyle Conan	Sign of four
study.txt	Doyle Conan	Study in scarlet
advent.txt	Doyle Conan	The adventures of sherlock holmes
casebo.txt	Doyle Conan	The case book of sherlock holmes
lostwo.txt	Doyle Conan	The lost world
plur.txt	Fontenelle	Entretiens sur la pluralite des mondes
ilia01.txt	Homer	Illiad
odys1.txt	Homer	L'odyssée
miser.txt	Hugo Victor	Les misérables
callwi.txt	London Jack	The call of the wild
hum.txt	Malebranche	Meditations sur l'humilite et la penitence
parlos.txt	Milton John	Paradise lost
pargai.txt	Milton John	Paradise regained
dgray.txt	oscar wilde	Picture of Dorian Gray
criton1.txt	Platon	Criton partie 1
criton2.txt	Platon	Criton partie 2
criton3.txt	Platon	Criton partie 3
opi.txt	Plutarque	Des opionions des philosophes
pit.txt	Poe Egdar Allan	The pit and the Pendulum
rev.txt	Rousseau	Les reveries du promeneur solitaire
augle.txt	Saint Augustin	Les lettres de Saint Augustin
antigo.txt	Sophocles	Antigone
oed1.txt	Sophocles	Oedipus the king vol 1
oed2.txt	Sophocles	Oedipus the king vol 2
hydea10.txt	Stevenson Robert Louis	The strange case of Dr Jekyll and Mr Hyde
dracu10.txt	Stoker Bram	Dracula
libert.txt	Stuart Mill John	On liberty
women.txt	Stuart Mill John	The subjection of women
sunzu.txt	Sun Tzu	The art of war
guer.txt	Tayac CIA	Manuel de guerrilla CIA
pd_2.txt	Un Docteur de la Sorbonne	Pensées diverses, comete de décembre 1680
eighty.txt	Verne Jules	Around the world in 80 days
moon.txt	Verne Jules	From the Earth to the moon
round.txt	Verne Jules	Round the moon
cand.txt	Voltaire	Candide
micro.txt	Voltaire	Micromegas
invism.txt	Wells herbet george	The invisible man
timema.txt	Wells Herbet George	The time machine
warwo.txt	Wells Herbet George	The war of the worlds
frank10.txt	Wollstonecraft Mary	Frankeinstein

Textes latins de l'époque médiévale

TEXTE	TITRE–AUTEUR
Anonev.txt	Anonymus Neveleti
Apolog.txt	Apologia Apulcii
Dante1.txt	Dantes Alagherii Iohanni de Virgilio
Danter.txt	Dantis Alagherii de Vulgari Eloquentia Liber Primus
Dante2.txt	Dantis Alagherii de Vulgari Eloquentia Liber Secundus
Dante13.TXT	Dantis Alagherii Epistola a Cangrande della Scala
aroath.txt	Declaratio Arbroathis
Ein.txt	Einhardi vita Karoli Magni
Gaud.txt	Gaudeamus Igitur
Septsap.txt	Historia Septem Sapientum
Stone.txt	Martyrium Ricardi Archiepiscopi Clement Maidstone

Diversité des motifs sans voyelles

Texte	Taille	Diversité
GAUD	681	14
JABBER	785	16
DEGRE	1110	6
DANTE1	2996	67
CRITON1	6522	93
CRITON2	9194	101
CRITON3	11549	115
PD_2	17192	193
ODYS1	17212	178
DANTE13	21472	194
SNARK	22650	212
ILIAD01	24762	130
PIT	28112	230
MICROMEG	31785	239
MANUEL	32271	246
DANTE2	34006	253
DANTER	36201	268
SEPTSAP	41586	291
ANTIGONE	46242	251
EIN	47524	307
OEDIPU1	56911	389
OEDIPU2	63579	414
ATLANTIS	68557	218
SHARER	72041	394
PARGAIN	73826	396
GUERILLA	80865	245
VMS408C	99777	556
CANDIDE	107293	290
HYDEA10	112645	326
ALICE	115997	339
ATHENE	116569	288
CAROL	127374	361
LOOKING	129347	556
APOLOG	131894	538
CHIMES	136980	464
CALLWILD	143022	353
CRICKET	143142	407
TIMEMACH	146290	574
WIZOZ	166484	575
DARKNESS	172821	461
FABLES	179031	418
VMS408F	184261	825
SIGNFOUR	187468	687
OZLAND	194250	619
STUDY	194607	715
MOON	199560	656
WOMEN	214571	583
INVISM	222147	459
LIBERTY	234090	614
SUNZU10	250726	769
ROUND	251192	688
HOUND	257264	451
LASTBOW	263651	475
WARWORLD	276446	774
EIGHTY	301040	496
OPAR	304083	739
RHETO	312055	785
JUNGLE	338634	476
LOSTWO	342971	845
FRANK10	343059	480
DGRAY10	348524	527
CASEBOOK	362504	537
GODSMARS	365707	503
PARLOST	378546	819
TARZAN	390857	870
ADVENTUR	455140	590
DARWIN	462546	477
TWOCITY	515159	1107
LORDJIM	579350	1288
HISTOI	582214	556
DRACU10	667152	785
BEAGLE	786267	740
W90	1596297	2099
W92	1878194	2139
MISERAB	2627133	2507

Motifs les plus longs des textes références (page 250)

En appliquant la méthode de recherches de motifs symétriques et redondants, nous avons obtenu les listes de ci-dessous ou la première colonne indique le nom du texte (page 351) suivi, dans la colonne suivante, du motif, et finalement de sa dimension réelle en nombre de lettres (espace '_' compris).

Avec voyelles

FABLES	#2#(#2#_THE_LION_THE_FOX_AND_THE_A#2#S)	60
MICROMEG	#2#(_LES_ETRES_$ETE !NDUS_QUI_S#2#(ENT))	60
TWOCITY	#2#(FIVE_PACES_BY_FOUR_AND$_A_ !HALF_)	60
HISTOI	#2#(_IN_MARINE_CREATURES_ALS$O_O !NE)	58
FABLES	#2#(#2#_THE_NORTH_WIND_AND_THE_SUN)	56
LORDJIM	#2#(I_WANTED_TO_GET_A$T_T !HE_BOATS)	56
PARLOST	#2#(_THAT_MAN_SHOULD_FIND_GRACE_)	56
W90	#2#(_CO#2#LECTIVE_S$TAT !E_PRESIDENCY)	56
W92	#2#(_ARMED_FORCES_RULING_COUNCIL)	56
MISERAB	#3#(_MY_MOTHER_IS_DEAD)	54
W90	#2#(ARMED_FORCES_RULING_COUNCIL)	54
ALICE	#2#(P#8#_BEAU#2#OTIFUL_S#4#O)	52
FABLES	#2#(#2#_THE_SWA#2#LOW_AND_THE_CROW)	52
FABLES	#2#(#2#_THE_GE$ESE !_AND_THE_CRANES)	52
MISERAB	#2#(_MONSEIGNEUR_SAINTEUSEBIUS)	52
W90	#2#(_NATIONAL_PEOPLES_CONGRE#2#S)	52
W90	#2#(_NATIONAL_PEOPLES_A#2#SEMBLY)	52
FABLES	#2#(#2#_THE_FOX_AND_THE_LEOPARD)	50
LASTBOW	#2#(_THE_TIGER_OF_SAN_PEDRO_)	48
LOOKING	#2#(#3#(ONE_AND_))	48
LOOKING	#2#(_THE_CAUSE_OF_LIGHT$NIN !G_)	48
LORDJIM	#2#(BEFORE_TH$E_E !ND_IS_TOLD#2#_)	48
LORDJIM	#2#(THE_MAKING_OF_QU#2#ENSLAND)	48
MISERAB	#2#(_MONSEIGNEUR_SAINTJULIEN)	48
MISERAB	#2#(THE_CO#2#MI#2#SARY_OF_POLICE)	48
MISERAB	#2#(_THOSE_WHO_ARE_DEPARTING)	48
TWOCITY	#2#(THOUGH_ITS_NOT_IMPORTANT)	48
INVISM	#2#(KNOCKED_HIM_ON_THE_HEAD)	46
LORDJIM	#2#($_I_ !CAN_O#2#FER_N$O_O !P$INI !ON)	46
MISERAB	#2#(_DEVRAIT_DU$RER !_TOUJOURS)	46
TWOCITY	#2#(WORTH_NO_MORE_THAN_THAT)	46
TWOCITY	#2#(IN$_A_ !QUARTER_OF_AN_HOUR)	46
W92	#2#(_ROYAL_ADVISORY_COUNCIL)	46
CANDIDE	#2#(_IL_NEST_POINT_JESUITE)	44
EIGHTY	#2#(DIRECTLY_FROM_BRIND$ISI !)	44
INVISM	#2#(#2#_THE_THINGS_HE_MAY_DO)	44
INVISM	#2#(TIED_HIM_UP_IN$_A_ !SH#2#ET)	44
LORDJIM	#2#(_HE_WAS_COMING_TO_THAT)	44
LORDJIM	#2#(_THE_BEST_DISPOS$ITI !ONS)	44
LORDJIM	#2#(COME_AND_S#2#E_THE_GIRL_)	44
MISERAB	#2#(_WHAT_ARE_WE_COMING_TO)	44
MISERAB	#2#(_IN_ORDER_TO_BE_HA#2#PY_)	44
TWOCITY	#2#(FOR_THR#2#E_HEAVY_HOURS_)	44
W90	#2#(ROYAL_ADVISORY_COUNCIL)	44
W92	#2#(AFGHANISTAN_GOVERNMENT)	44
ANTIGONE	#2#(#13#_ANTIGONE)	42
CHIMES	#2#(_FU#2#L_OF_OBSERWATIONS)	42
DRACU10	#2#(THE_BL#2#OD_IS_THE_LIFE)	42

Sans voyelles

LOSTWO	#2#(TH_MST_WNDRFL_THNGS_HV_H#2#PND)	56
CHIMES	#2#(#2#(_TB_VCK)KP#2#_GD_HR$T_T !B)	54
CHIMES	#2#(_TBVCK_TB_VCK_JB_CMNG_SN_TB)	54
DGRAY10	#2#(TH_SM_FLSH_ND_BLD$_S_ !N$S_S !LF)	52
STUDY	#2#(_TH_SC$RTR !_MR_JSPH_STNGRSN_)	52
CHIMES	#2#(#2#(TB_VCK_)WTNG_FR#2#_TB)	50
W90	#2#(S#2#T_LW_ND$_RDR_ !RS$TRT !N_$CNC !L)	50
ALICE	#2#(P#4#_SP$_F_ !TH_V#2#NG_BTFL_S)	48
CALLWILD	#2#(#5#_TH_DM#2#NT_P$RMR !DL_BST)	48
ATHENE	#2#(LSMCHS_ND_THMSTCL$S_S !N_F)	46
CAROL	#2#(_TH_BKRS_T$H_H !D_SML$T_T !H)	44
FABLES	#2#(#2#_TH_LN_TH_FX_ND_TH_#2#S)	44
FABLES	#2#(#2#_TH_NRTH_W#2#(ND_)TH_SN)	44
DRACU10	#2#(ST_PLS_TH$R_R !LTV$S#2#_S !#2#P)	42
PARLOST	#2#($_THT_ !MN_SHLD_FND_GRC_)	42
W92	#2#(NWL_NDSTRLZNG_CNMS_NS)	42
FABLES	#2#(#2#_TH_S$W#2#LW !_ND_TH_CRW)	40
MICROMEG	#2#(_LS_TRS_TND$S_Q_S !$NTN !T)	40
TWOCITY	#2#(_RMND_#2#MVBL_CLS$_T_ !HM)	40
TWOCITY	#2#(FV_PCS$_B_ !FR_ND#2#_HLF_)	40
LORDJIM	#2#(_WNTD$_T_ !G$T_T_T !H_BTS)	38
W92	#2#(_RMD_FRCS_RLNG_$CNC !L)	38
CAROL	#2#(#5#_BCS#2#_FL$L_N_L !V)	36
FABLES	#2#(#2#_TH_FX_ND_TH_LPRD)	36
FABLES	#2#(#2#_TH_GS_ND_TH_CRNS)	36
MISERAB	#2#(ND$_THT_ !T_SH#2#L_PLS_)	36
MISERAB	#3#($_M_ !MTHR$_S_ !#2#D)	36
W90	#2#(RMD_FRCS_RLNG_$CNC !L)	36
W90	#2#(_$C#2#LC !TV_S#2#T_PRSDNC)	36
ANTIGONE	#2#(#13#_NTGN)	34
DARWIN	#2#(_STR#2#GL_FR_XSTNC_)	34
HISTOI	#2#($_N_ !MRN_C$RTR !S_LS_N)	34
HISTOI	#2#($_N_ !MRN_C$RTR !S_LS_N)	34
LASTBOW	#2#(_TH_TGR$_F_ !SN_PDR_)	34
LOOKING	#2#(_TH_CS$_F_ !LGHT#2#NG_)	34
LORDJIM	#2#(BFR_TH_ND$_S_ !TLD#2#_)	34
TWOCITY	#2#(WRTH$_N_ !MR_THN_$THT !)	34
TWOCITY	#2#(T$HGH !_TS_NT_MPR$TNT !)	34
W90	#2#(_$NTN !L_#2#PLS_CNGR#2#S)	34
HOUND	#2#(#2#_MR_SHRLCK_HLMS)	32
INVISM	#2#(_#2#(_TH)NGS$_H_ !M_D)	32
INVISM	#2#(KNCKD_HM$_N_ !T$H_H !D)	32
LORDJIM	#2#($_H_ !WS_CMNG$_T_ !$THT !)	32
LORDJIM	#2#(TH_MKNG$_F_ !QNSLND)	32
MISERAB	#2#(#12#_#2#L#2#T)	32
MISERAB	#2#($_#2#L_ !THS_RCH_FLKS)	32
MISERAB	#2#(_THS_WH$_R_ !DPRTNG)	32
W90	#2#(_$NTN !L_#2#PL$S_S !SMBL)	32

Extraits : les cinq motifs les plus

grands par texte (page 250)

La liste que nous vous donnons est un extrait de la liste principale contenant les motifs de dimension supérieure à dix. Il n'est pas possible de fournir entièrement cette liste sur papier car sa taille est dix fois supérieure à la liste présentée ici. Or il est remarquable qu'un texte ne soit pas entièrement déductible de cinq seuls motifs.

ADVENTUR	#2#(_MY_DEAR_YOUNG_LADY)	38
ADVENTUR	#2#(_THE_RIGHT_SIDE_)	32
ADVENTUR	#2#(_NO$T_T !HE_SOLE)	26
ADVENTUR	#2#(_TO_AN_END_)	22
ADVENTUR	#2#(_THE_CE#2#LAR)	22
ALICE	#2#(P#8#_BEAU#2#OTIFUL_S#4#O)	52
ALICE	#2#(_WOULD_NOT_COULD_NOT)	40
ALICE	#2#(_DO_CATS_EAT_BATS_)	36
ALICE	#2#(WI#2#L_YOU_WONT_YOU_)	36
ALICE	#2#(_WI#2#L_YOU_WONT_YOU)	36
ANTIGONE	#2#(#13#_ANTIGONE)	42
ANTIGONE	#2#(SECOND_M$E#2#SE !NGER)	32
ANTIGONE	#2#(_AND_TURNED)	22
ANTIGONE	#2#(COME_FORTH)	20
ANTIGONE	#2#(TEIRESIAS)	18
ATHENE	#2#(_THE_ARBITRATORS)	32
ATHENE	$T#27#_T !	29
ATHENE	#2#(_AS_THEY)	16
ATHENE	$IR_CIVIC_RI !	11
ATHENE	#2#(HEN_T)	10
BEAGLE	#2#(ONE_HUNDRED_AND_)	32
BEAGLE	#2#(TIE#2#RA_DEL_FUEGO)	32
BEAGLE	#2#(RIO_DE_JANEIRO)	28
BEAGLE	#2#(#4#_CONFINED_)	26
BEAGLE	#2#(#7#_TO_THE)	26
CALLWILD	#2#(_THATS_A#2#L_RIGHT)	32
CALLWILD	#2#(_AND_NUDGE)	20
CALLWILD	#2#(ACHED_AND_)	20
CALLWILD	#2#(_CHARLES)	16
CALLWILD	#2#(_GAD_SIR)	16
CANDIDE	#2#(_IL_NEST_POINT_JESUITE)	44
CANDIDE	#2#(_MANGEONS_DU_JESUITE)	40
CANDIDE	#2#(_CEST_UN_JESUITE)	32
CANDIDE	#2#(_BORTZM$EYE !R)	22
CANDIDE	#2#(_PANGLO#2#S_)	20
CAROL	#2#(SCR#2#OGES_NI$ECE !)	28
CAROL	#2#(_THROUGH_AND)	24
CAROL	#2#(_ROUND_AND)	20
CAROL	#2#(#2#_CAN_YOU)	18
CAROL	#2#(_CRATCHIT)	18
CASEBOOK	#2#($_I_ !WI#2#L_NOT_S#2#E_HIM)	38
CASEBOOK	#2#(_DO$_I_ !NOT_LOVE_HIM)	36
CASEBOOK	#2#(_PERHAPS$_I_ !HAVE)	30
CASEBOOK	#2#(_DE_MERVI#2#LE_)	26
CASEBOOK	#2#(_LOWENSTEIN_)	24
CHIMES	#2#(_FU#2#L_OF_OBSERWATIONS)	42
CHIMES	#2#(_THE_G#2#OD_OLD_TIMES)	38
CHIMES	#2#(_HAUNT_AND_HUNT_HIM)	38
CHIMES	#2#(BREAK_HI$S_S !LUMBERS_)	38
CHIMES	#2#(_S#2#EN_THE_ALDERMAN_)	38
CRICKET	#2#(_THE_OLD_GENTLEMAN_)	38
CRICKET	#3#(_CHI#2#RUP)	24
CRICKET	#2#(_H$ERE !_ALONE_)	24
CRICKET	#2#(_QUITE_GONE)	22
CRICKET	#2#(_G#2#ODNIGHT_)	22
CRITON1	#2#(_SOCRATE_)	18
CRITON1	#2#(_CRITON)	14
CRITON2	#2#(E_SOCRAT)	16
CRITON2	#2#(_SOCRATE)	16
CRITON2	#2#(E_QUE#2#L)	14
CRITON3	#2#(_TU_MEURS)	18
CRITON3	#2#(TE_SOCRA)	16
CRITON3	#2#(E_SOCRAT)	16
DARKNESS	#2#(_IT_IS_IMPO#2#SIBLE)	34
DARKNESS	#2#(T_HE_WAS_GREA)	26
DARKNESS	#2#(_NO_RESTRAINT)	26
DARKNESS	#2#(_HE_STRU#2#GLED)	26
DARKNESS	#2#($_I_ !LOVED_HIM_)	26
DARWIN	#2#(_NATURAL_S$ELE !CTION)	36
DARWIN	#2#(_TH$ESE !_TWO_BR#2#EDS)	34
DARWIN	#2#(E_RHOMBS_AND_TH)	30
DARWIN	#2#(_OTHER_SPECIES)	28
DARWIN	#2#(D_LARGER_AN)	22
DGRAY10	#2#(MA#2#RYING_SIBYL_VANE)	38
DGRAY10	#2#(HE_HAD_GOT_FROM_HER)	38
DGRAY10	#2#(_YOU_WI#2#L_F#2#EL_IT)	34
DGRAY10	#2#(HER_GRANDFATHER)	30
DGRAY10	#2#(F#2#OLISH_CHILD_)	28
DRACU10	#2#(THE_BL#2#OD_IS_THE_LIFE)	42
DRACU10	#2#(A_PRESAGE_OF_H$O#2#RO !R)	38
DRACU10	#2#(FOR_DEAR_LUCY$S_S !AKE)	38
DRACU10	#2#(#2#_WHAT_AM$_I_ !TO_DO)	34
DRACU10	#2#(#2#_IF_ONLY$_I_ !KNEW)	32
EIGHTY	#2#(DIRECTLY_FROM_BRIND$ISI !)	44
EIGHTY	#2#(THR#2#E_HUNDRED_POUNDS)	40
EIGHTY	#2#(FOR_TOM$O#2#RO !W_MONDAY)	38
EIGHTY	#2#(ROUND_THE_WORLD)	30
EIGHTY	#3#(EIMPO#2#SIBL)	30
FABLES	#2#(#2#_THE_LION_THE_FOX_AND_THE_A#2#S)	60
FABLES	#2#(#2#_THE_NORTH_WIND_AND_THE_SUN)	56
FABLES	#2#(#2#_THE_SWA#2#LOW_AND_THE_CROW)	52
FABLES	#2#(#2#_THE_GE$ESE !_AND_THE_CRANES)	52
FABLES	#2#(#2#_THE_FOX_AND_THE_LEOPARD)	50
FRANK10	#2#(_MY_FATHER_)	22
FRANK10	#2#(_BEAUTIFUL_)	22
FRANK10	#2#(_SAVE_ME_)	18
FRANK10	#2#(NO$T_T !HUS)	16
FRANK10	#2#(CURSED_)	14
GODSMARS	#2#(THE_DEAD_RETUR$N_N !OT_)	40
GODSMARS	#2#(_TH$ERE !_IS_NO_HOPE)	34
GODSMARS	#2#(I_AM_IN_TIME#2#_)	28
GODSMARS	#2#(_JOHN_CARTER_)	26
GODSMARS	#2#(AND_PA#2#RIED_)	24
GUERILLA	#2#(_DEMOCRACY)	20
HISTOI	#2#(_IN_MARINE_CREATURES_AL$$O_O !NE)	58
HISTOI	#2#(_AND_TH$E_E !XCRETIONS)	38
HISTOI	#2#(_THE_T$E#2#SE !#2#LATES)	32
HISTOI	#2#(_AND_THE_SEAMEW)	30
HISTOI	#2#(_$TET !RAPTEROUS)	26
HOUND	#2#(#2#_MR_SHERLOCK_HOLMES)	40
HOUND	#2#(_PROVE_I$T_T !O_ME)	30
HOUND	#2#(#2#_F#2#OTPRINTS)	24
HOUND	#2#(_SHAMEFU#2#LY_)	24
HOUND	#2#(_HIS_WIFE#2#_)	22
HYDEA10	#2#(_GOD_FORGIVE_US)	30
HYDEA10	$D#22#_D !	24
HYDEA10	#2#(LISTENS_AND)	22
HYDEA10	#2#(THE_MOR$NIN !G)	22
HYDEA10	#2#(_$AGA !IN_AND)	20
ILIAD01	#2#(_MOTHER)	14
INVISM	#2#(KNOCKED_HIM_ON_THE_HEAD)	46
INVISM	#2#(#2#_THE_THINGS_HE_MAY_DO)	44
INVISM	#2#(TIED_HIM_UP_IN$_A_ !SH#2#ET)	44
INVISM	#2#(THE_JO#2#LY_CRICK$ETE !RS)	40
INVISM	#2#($_A_ !REIGN_OF_TER$ROR !_)	38
JUNGLE	#2#(_TEN_FAT_GOATS)	28
JUNGLE	#3#(_WORKING)	24
JUNGLE	#2#(_TREMBLED)	18
JUNGLE	#2#(AND_$AGA !IN)	18
JUNGLE	#2#(_TARZAN_)	16
LASTBOW	#2#(_THE_TIGER_OF_SAN_PEDRO_)	48
LASTBOW	#2#(_D#2#EPLY_INT$ERE !STED_)	38
LASTBOW	#2#(#2#_VERY_INT$ERE !STING)	36
LASTBOW	#2#(_THE_NEXT_STEP_)	30
LASTBOW	#2#(_VERY_PAINFUL_)	28
LIBERTY	#2#(_THE_NATION)	22
LIBERTY	#2#(_$E#2#CE !NTRIC)	20
LIBERTY	#2#(_$ENE !RGY)	14
LIBERTY	#2#(_EXI$$TS !)	14
LIBERTY	#2#(_TRUTH)	12
LOOKING	#2#(#3#(ONE_AND_))	48
LOOKING	#2#(_THE_CAUSE_OF_LIGHT$NIN !G_)	48
LOOKING	#2#(T#2#_SHOULDNT_DO_THA)	36
LOOKING	#2#(_$NIN !E_FROM_EIGHT_)	34
LOOKING	#2#(_BRE$ADA !NDBU#2#TER)	30
LORDJIM	#2#(I_WANTED_TO_GET_A$T_T !HE_BOATS)	56
LORDJIM	#2#(BEFORE_TH$E_E !ND_IS_TOLD#2#_)	48
LORDJIM	#2#(THE_MAKING_OF_QU#2#ENSLAND)	48
LORDJIM	#2#($_I_ !CAN_O#2#FER_N$O_O !P$INI !ON)	46
LORDJIM	#2#(_HE_WAS_COMING_TO_THAT)	44
LOSTWO	#2#(MAPLE_WHITE_LAND)	32
LOSTWO	#2#(CA#2#NOT_A#2#LOW_IT)	30
LOSTWO	#2#(#2#_R$EGE !NT_STR#2#ET)	30
LOSTWO	#2#(_$_A_ !PROCE#2#SION)	28
LOSTWO	#2#(WORD_OF_H$ONO !R)	26
MICROMEG	#2#(_LES_ETRES_$ETE !NDUS_QUI_S#2#(ENT))	60
MICROMEG	#2#(_CUBAUD)	14
MICROMEG	#2#(_NOUS)	10
MICROMEG	#2#(_VOUS)	10
MICROMEG	#2#(EST_C)	10
MISERAB	#3#(_MY_MOTHER_IS_DEAD)	54
MISERAB	#2#(_MONSEIGNEUR_SAINTEUSEBIUS)	52
MISERAB	#2#(_MONSEIGNEUR_SAINTJULIEN)	48
MISERAB	#2#(THE_CO#2#MI#2#SARY_OF_POLICE)	48
MISERAB	#2#(_THOSE_WHO_ARE_DEPARTING)	48
MOON	#2#(REFLECTED)	18
MOON	#2#($_A_ !HERO)	14
MOON	#2#(ENOUGH_)	14
MOON	#2#(NOT_ONE)	14
MOON	#2#(NICHO#2#L)	14
OEDIPU2	#2#(_THE_WINGS)	20
OEDIPU2	#2#(POLYNEICES)	20
OEDIPU2	#2#(M$E#2#SE !NGER)	18
OEDIPU2	#2#(T#2#O_LONG_)	18
OEDIPU2	#2#(ANTIGONE)	16
OPAR	#2#(SHE$_DID_ !NOT_S#2#E)	30
OPAR	#2#(I_DO_NOT_KNOW_)	28
OPAR	#2#(_ANOTHER_AND)	24
OPAR	#2#(D_ANOTHER_AN)	24
OPAR	#2#(R$EVE !NGE#2#_)	18
OZLAND	#2#(_YOUR_MAJESTY_)	28
OZLAND	#2#(SOMETHING_ELSE)	28
OZLAND	#2#(THE_SAWHORSE)	24
OZLAND	#2#(SLOW_HIM_UP_)	24
OZLAND	#2#(HE_LIVES#2#_)	20
PARGAIN	#2#(SO_LATELY_FOUND)	30

PARGAIN	#2#(_INCREASED)	20
PARGAIN	#2#(_IS_LEFT)	16
PARGAIN	#2#(MY_CRIME)	16
PARGAIN	#2#(AND_EAT)	14
PARLOST	#2#(_THAT_MAN_SHOULD_FIND_GRACE_)	56
PARLOST	#2#(_G#2#OD_AND_OF_OUR)	32
PARLOST	#2#(_ON_EVIL_DAYS)	26
PARLOST	#2#(E_HIS_PRAIS)	22
PARLOST	#2#(_THY_PRAISE)	22
PIT	#2#(_DOWN_)	12
PIT	#2#(UNREAL)	12
PIT	#2#(_SICK)	10
PIT	#2#(M_THE)	10
PIT	#2#(_LONG)	10
RHETO	#2#(RATIONAL_CRAVING_)	34
RHETO	#2#(_ETHICAL_STUDIES)	32
RHETO	#2#(_FOR_THAT_REASON)	32
RHETO	#2#(_METAPHORICAL)	26
RHETO	#2#($T_T !$O_O !#2#FER_I)	24
ROUND	#2#(_NOTHING_BUT$_A_ !M$ETE !OR)	42
ROUND	#2#(_BECOME_S$ELE !NITES_)	36
ROUND	#2#(CULTIVATED_FIELDS)	34
ROUND	#2#(_WH$ERE !_ARE_THEY)	30
ROUND	#2#(THE_HYPERBOLA)	26
SHARER	#2#(_FAINTER_AND)	24
SHARER	#2#(_G#2#OD_FU#2#L_)	22
SHARER	#2#(_TE#2#RIBLE_)	20
SHARER	#2#(PERHAPS_)	16
SHARER	#2#(#4#_YOU)	14
SIGNFOUR	#2#(_MAJOR_SHOLTO)	26
SIGNFOUR	#2#(_THAT_IS_WE#2#L)	26
SIGNFOUR	#2#(S_BAD_BUSINES)	26
SIGNFOUR	#2#(_OH_DEAR)	16
SIGNFOUR	#2#(NAUGHTY_)	16
STUDY	#2#(#2#(_ON)_TO_ZION_)	30
STUDY	#2#(TO_FORGET_IT#2#_)	28
STUDY	#2#(_IVE_FOUND_IT)	26
STUDY	#2#(_ONE_HEARS_)	22
STUDY	#2#(_BEAUTIFUL)	20
SUNZU10	#2#(_SUPR$EME !_EXC$E#2#LE !NCE)	38
SUNZU10	#2#(_BON$APA !RTE_)	22
SUNZU10	#2#(_THE_RIGHT_)	22
SUNZU10	#2#(_BE_SUBTLE)	20
SUNZU10	#2#(_D$EFE !NSE_)	18
TARZAN	#2#(MOST_REPR$EHE !NSIBLE_)	38
TARZAN	#2#(PERFECTLY_W$I#2#LI !NG)	34
TARZAN	#2#(MOST_REMARKABLE_)	32
TARZAN	#2#(MOST_REMARKABLE)	30
TARZAN	#2#(CERTAINLY_SIR_)	28
TIMEMACH	#2#(_MY_POCKETS_)	24
TIMEMACH	#2#(_SLOWER_AND)	22
TIMEMACH	#2#(SILENT#2#_)	16
TIMEMACH	#3#(THUD)	12
TIMEMACH	#2#($ERE !_TH)	12
TWOCITY	#2#(FIVE_PACES_BY_FOUR_AND$_A_ !HALF_)	60
TWOCITY	#2#(THOUGH_ITS_NOT_IMPORTANT)	48
TWOCITY	#2#(WORTH_NO_MORE_THAN_THAT)	46
TWOCITY	#2#(IN$_A_ !QUARTER_OF_AN_HOUR)	46
TWOCITY	#2#(FOR_THR#2#E_HEAVY_HOURS_)	44
W90	#2#(_CO#2#LECTIVE_S$TAT !E_PRESIDENCY)	56
W90	#2#(ARMED_FORCES_RULING_COUNCIL)	54
W90	#2#(_NATIONAL_PEOPLES_CONGRE#2#S)	52
W90	#2#(_NATIONAL_PEOPLES_A#2#SEMBLY)	52
W90	#2#(ROYAL_ADVISORY_COUNCIL)	44
W92	#2#(_ARMED_FORCES_RULING_COUNCIL)	56
W92	#2#(_ROYAL_ADVISORY_COUNCIL)	46
W92	#2#(AFGHANISTAN_GOVERNMENT)	44
W92	#2#(_COUNCIL_OF_M$INI !STERS)	42
W92	#2#(_D$EVE !LOPING_COUNTRIES)	42
WARWORLD	#2#(_TO_DIE#2#_THEY_OUGHT)	38
WARWORLD	#2#(_$_I_ !CANT_G$O_O !N)	28
WARWORLD	#2#(#2#_K#2#EP_BACK)	22
WARWORLD	#2#($ETE !RNITY#2#_)	20
WARWORLD	#2#(#2#_$ETE !RNITY)	20
WIZOZ	#2#(#2#_DONT_CHASE_ME)	30
WIZOZ	#2#(_NOR_THE_NEXT)	26
WIZOZ	$T#20#_T !	22
WIZOZ	#2#(_THANK_YOU_)	22
WIZOZ	#2#(_COME_BACK_)	22
WOMEN	#2#($_A_ !RULE)	14
WOMEN	#2#(_GABER)	12
WOMEN	#2#(_FORCE)	12
WOMEN	#2#(_WOMEN)	12
WOMEN	$NEVERPREVEN !	11

Extraits de motifs dans leurs contextes (page 250)

The adventures of Sherlock Holmes

2(notthesole)

"I was a little startled at the nature of the child's amusement,but the father's laughter made me think that perhaps he was joking. " 'My sole duties, then,' I asked, 'are to take charge of a single child?' " 'No, no, not the sole, not the sole, my dear young lady,' he cried. 'Your duty would be, as I am sure your good sense would suggest, to obey any little commands my wife might give,provided always that they were such commands as a lady mightwith propriety obey. You see no difficulty, heh?' " 'I should be happy to make myself useful.'

Alice in wonderland

2(pSoupoftheeveningbeautifulSou)

The Mock Turtle sighed deeply, and began, in a voice sometimes choked with sobs, to sing this:`Beautiful Soup, so rich and green, Waiting in a hot tureen! Who for such dainties would not stoop? Soup of the evening, beautiful Soup! Soup of the evening, beautiful Soup! Beau--ootiful Soo--oop! Beau--ootiful Soo--oop! Soo--oop of the e--e--evening, Beautiful, beautiful Soup! `Chorus again!" cried the Gryphon, and the Mock Turtle had just begun to repeat it, when a cry of `The trial's beginning!' was heard in the distance.

2(Docatseatbats)

But do cats eat bats, I wonder?' And here Alice began to getrather sleepy, and went on saying to herself, in a dreamy sort ofway, `Do cats eat bats? Do cats eat bats?' and sometimes, `Dobats eat cats?' for, you see, as she couldn't answer eit her question, it didn't much matter which way she put it.

Antigone

2(SECONDMESSENGER)

CREON (Str. 2) By sorrow schooled. Heavy the hand of God,Thorny and rough the paths my feet have trod,Humbled my pride, my pleasure turned to pain;Poor mortals, how we labor all in vain! [Enter SECOND MESSENGER] SECOND MESSENGER Sorrows are thine, my lord, and more to come,One lying at thy feet, another yetMore grievous waits thee, when thou comest home.

2(MESSENGER)

Who dance before thee all night long, and shout, Thy handmaids we, Evoe, Evoe! [Enter MESSENGER] MESSENGER Attend all ye who dwell beside the hallsOf Cadmus and Amphion.

2(ANTIGONE)

ANTIGONE ANTIGONE and ISMENE before the Palace gates.

Athene

2(ofLysimachusandThemistoclesson)

The leaders of the people duringthis period were Aristides, of Lysimachus, and Themistocles, son of Lysimachus, and Themistocles, son of Neocles, of whom the latter appeared to devote himself to the conduct of war, while the former had the reputation of being a clever statesman and the most upright man of his time.

2(thenwhoisyourmo)

When they are examined, they are asked, first, 'Who isyour father, and of what deme? who is your father's father? who isyour mother? who is your mother's father, and of what deme?

The voyage of Beagle

2(onehundredand)

By the kindness of Dr. Smith, I am enabled to show thatthe case is very different. He informs me, that in lat. 24 degs.,in one day's march with the bullock-waggons, he saw, withoutwandering to any great distance on either side, between one hundred and one hundred and fifty rhinoceroses, whichbelonged to three species: the same day he saw several herdsof giraffes, amounting together to nearly a hundred; andthat although no elephant was observed, yet they are foundin this district.

2(wonderfullyas)

The relationship, though distant, between the Macraucheniaand the Guanaco, between the Toxodon and theCapybara, -- the closer relationship between the many extinctEdentata and the living sloths, ant-eaters, and armadillos,now so eminently characteristic of South American zoology,-- and the still closer relationship between the fossil andliving species of Ctenomys and Hydrochaerus, are mostinteresting facts. This relationship is shown wonderfully -- aswonderfully as between the fossil and extinct Marsupialanimals of Australia -- by the great collection lately broughtto Europe from the caves of Brazil by MM. Lund and Clausen.

2(ossessesso)

This volume contains, in the form of a Journal, a history ofour voyage, and a sketch of those observations in Natural Historyand Geology, which I think will possess some interest for thegeneral reader. I have in this edition largely condensed andcorrected some parts, and have added a little to others,

The call of the wild

2(thatsallright)

"Think it'll ride?" one of the men asked."Why shouldn't it?" Charles demanded rather shortly."Oh, that's all right, that's all right," the man hastenedmeekly to say. "I was just a wondering, that is all. Itseemed a mite top-heavy."

2(dwhenhecoul)

And through it all Buck staggered along at the head of theteam as in a nightmare. He pulled when he could; when hecould no longer pull, he fell down and remained down tillblows from whip or club drove him to his feet again.

Candide

#2#(EILNESTPOINTJESUIT)

Les Oreillons délièrent leurs deux prisonniers, leur firent toutes sortes de civilités, leur offrirent des filles, leur donnèrent des rafraîchissements, et les reconduisirent jusqu'aux confins de leurs États, en criant avec allégresse : « Il n'est point jésuite, il n'est point jésuite ! »

#2#(EMANGEONSDUJESUIT)et#2#(CESTUNJESUITE)

Ils étaient entourés d'une cinquantaine d'Oreillons tout nus, armés de flèches, de massues et de haches de caillou : les uns faisaient bouillir une grande chaudière ; les autres préparaient des broches, et tous criaient : « C'est un jésuite, c'est un jésuite ! nous serons vengés, et nous ferons bonne chère ; mangeons du jésuite, mangeons du jésuite ! »

#2#(ACHAL)

On détacha la chaloupe pour voir ce que ce pouvait être : c'était un de ses moutons.

#2#(ENTRE)

Partagé entre ces deux sentiments, il prend son or et ses diamants, et se fait conduire avec Martin à l'hôtel où Mlle Cunégonde demeurait. Il entre en tremblant d'émotion, son coeur palpite, sa voix sanglote ; il veut ouvrir les rideaux du lit, il veut faire apporter de la lumière.

#2#(PLACE)

Il volait déjà en prononçant ces paroles, et en criant en espagnol : « Place, place pour le révérend père colonel. »

#2#(QUISE)

Cependant l'abbé s'approcha de l'oreille de la marquise, qui se leva à moitié, honora Candide d'un sourire gracieux, et Martin d'un air de tête tout à fait noble ;

$CEDEMEDEC!

Cependant, à force de médecines et de saignées, la maladie de Candide devint sérieuse.

$E#2#TECE#2#TE!

« O mon cher Candide ! vous avez connu Paquette, cette jolie suivante de notre auguste baronne ; j'ai goûté dans ses bras les délices du paradis, qui ont produit ces tourments d'enfer dont vous me voyez dévoré ; elle en était infectée, elle en est peut être morte...

A christmas carol

2(Ihaveknownhimwalkwith)

They were very quiet again. At last she said, and in a steady, cheerful voice, that only faltered once: `I have known him walk with -- I have known him walk with Tiny Tim upon his shoulder, very fast indeed.' `And so have I,' cried Peter. `Often.' `And so have I,' exclaimed another. So had all.

The case book of Sherlock Holmes

2(Iwillnotseehim)

The woman turned her flushed and handsome face towardsme. "Where is my husband?" "He is below and would wish to see you." "I will not see him. I will not see him." Then she seemed towander off into delirium. "A fiend! A fiend! Oh, what shall I dowith this devil?" "Can I help you in any way?"

2(PerhapsIhave)

"I have no idea. Have you?" "Perhaps I have. Perhaps I haven't. I may be able to say moresoon. Anything which will define what made that mark willbring us a long way towards the criminal."

The chimes

3(factsonfigures)

'A man may live to be as old as Methuselah,' saidMr. Filer, 'and may labour all his life for the benefitof such people as those; and may heap up facts onfigures, facts on figures, facts on figures, mountainshigh and dry; and he can no more hope to persuade'em that they have no right or business to be mar-ried, than he can hope to persuade 'em that theyhave no earthly right or business to be born.

2(esFactsandFigures)

Still the Bells, pealing forth their changes, madethe very air spin. Put 'em down, Put 'em down!Good old Times, Good old Times! Facts and Fig-ures, Facts and Figures! Put 'em down, Put 'emdown. If they said anything they said this, untilthe brain of Toby reeled.

2(FactsandFigures)

Trotty had no portion, to his thinking, in the NewYear or the Old. 'Put 'em down, Put 'em down! Facts and Fig-ures, Facts and Figures! Good old Times, Goodold Times! Put 'em down, Put 'em down!' -- his trotwent to that measure, and would fit itself to noth-ing else.

The cricket on the heart

2(Plentyoftime)

'You are not married before noon ?' he said, 'Ithink?' 'No,' answered Tackleton. 'Plenty of time. Plentyof time.'

The heart of darkness

2(nomorethanjustice)

It is a difficult case.What do you think I ought to do -- resist? Eh? I wantno more than justice.' . . . He wanted no more thanjustice -- no more than justice. I rang the bell before amahogany door on the first floor, and while I waitedhe seemed to stare at me out of the glassy panel

Origin of species

2(NaturalSelection)

Chapter 4 - Natural Selection Natural Selection its power compared with man's selection its power on characters of trifling importance its power at all ages and on both sexes

2(erhombsandth)

then, if planes of intersection between the severalspheres in both layers be formed, there will result a double layer of hexagonal prismsunited together by pyramidal bases formed of three rhombs; and the rhombs and thesides of the hexagonal prisms will have every angle identically the same with the bestmeasurements which have been made of the cells of the hive-bee.

2(RARERAND)

From these several considerations I think it inevitably follows, that as new species inthe course of time are formed through natural selection, others will become rarer and rarer, and finally extinct.

2(otherspecies)

Several other singular rules could be given from Gartner: for instance, some species have a remarkable power of crossing with other species; other species of the samegenus have a remarkable power of impressing their likeness on their hybridoffspring:

Dorian Gray

2(youwillfeelit)

"No, you don't feel it now. Some day, when you are oldand wrinkled and ugly, when thought has seared your foreheadwith its lines, and passion branded your lips with itshideous fires, you will feel it, you will feel it terribly.

2(dontleaveme)

I should have shownmyself more of an artist. It was foolish of me, and yet Icouldn't help it. Oh, don't leave me, don't leave me."A fit of passionate sobbing choked her.

2(emomentth)

She heaved a deep sigh. It was a sigh of relief. The terrible moment,the moment that night and day, for weeks and months, she had dreaded,had come at last, and yet she felt no terror.

2(poisoning)

The Renaissance knew of strange manners of poisoning--poisoning by a helmet and a lighted torch, by an embroidered gloveand a jewelled fan, by a gilded pomander and by an amber chain.Dorian Gray had been poisoned by a book.

Dracula

2(Thebloodisthelife)

He was easily secured,and to my surprise, went with the attendants quite placidly,simply repeating over and over again, "The blood is the life!The blood is the life!"

Around the world in 80 days

2(Passepartout)

Passepartout, who had conscientiously studied the programme of his duties,was more than surprised to see his master guilty of the inexactnessof appearing at this unaccustomed hour; for, according to rule,he was not due in Saville Row until precisely midnight.Mr. Fogg repaired to his bedroom, and called out, "Passepartout!"Passepartout did not reply. It could not be he who was called;it was not the right hour."Passepartout!" repeated Mr. Fogg, without raising his voice.Passepartout made his appearance.

The gods of mars

2(thedeadreturnnot)

And then from the far corner of the great chamber a hollowvoice chanted: "There is no hope, there is no hope;the dead return not, the dead return not; nor is thereany resurrection. Hope not, for there is no hope."

Manuel de guerrilla CIA

2(ArmedPropagandaTeams)

4. Armed Propaganda Teams Armed Propaganda Teams (EPA) are formed through a careful selection ofpersuasive and highly motivated guerrillas who move about within thepopulation, encouraging the people to support the guerrillas and put upresistance against the enemy.

2(armedpropaganda)

7. Support of Contacts with Their Roots in Reality The support of local contacts who are familiar with the deep realityis achieved through the exploitation of the social and political weaknessesof the target society, with propagandist-combatant guerrillas, armedpropaganda, armed propaganda teams, cover organizations and mass meetings.

2(democracy)

Reduplication, when the phrase begins with the same word that ends theprevious one. For example: "We struggle for democracy, democracy and socialjustice." The concatenation is a chain made up of duplications. Forexample: "Communism transmits the deception of the child to the young man,of the young man to the adult, and of the adult to the old man."

History of animals

2(Inmarinecreaturesalsoone)

So much for the habits of birds. In marine creatures, also, one In marine creatures, also, onemay observe many ingenious devices adapted to the circumstances oftheir lives. For the accounts commonly given of the so-calledfishing-frog are quite true; as are also those given of the torpedo.

2(nearerand)

it hides itself; that the otheranimals come nearer and nearer, and that by this stratagem it cancatch even animals as swift of foot as stags.

Fables

#2#(#2#_the_lion_the_fox_and_the_a#2#s)

The Lion, the Fox, and the Ass The lion, the Fox and the Ass entered into an agreement to assist each other in the chase

#2#(_the_pigeons_)

The Hawk, the Kite, and the Pigeons. The pigeons, terrified by the appearance of a Kite, called upon the Hawk to defend them.

Sources et références du manuscrit de Voynich

14 novembre 1998 —Première édition

Alphabets de VOYNICH

Voynich caractère	Currier quantité	Voynich caractère	Friedman quantité
	95876		182072
y	1	J	1
t	1	V	2
c	1	7	3
5	2	Z	7
Y	41	Y	97
6	54	W	222
F	173	N	716
K	422	Q	957
P	592	I	1020
I	767	2	2106
2	1214	H	5008
S	2539	4	5197
H	2779	D	8757
D	4536	T	9962
T	5584	A	12839
8	6655	C	17285
G	9039	Espace	40782
Espace	20263	O	21299
O	11775	G	15614
C	8257	8	11574
A	5990	E	9131
E	4891	R	6486
R	3333	M	5133
4	2738	S	4193
M	1900	P	1256
N	811	K	1005
Q	644	X	934
X	496	F	336
L	186	L	131
W	137	6	10
7	47	9	6
q	2	3	3
p	2		
n	1		
a	1		
x	1		

Représentation multiple (page 223)

Pour chaque page du manuscrit nous avons établi les substitutions à représentations multiples sur les mots de dimensions supérieures ou égales à 3 lettres. A chaque position (P) de ces mots correspond un alphabet de lettres équivalentes.

—page 001
3 lettres
P1 28CDFGHPRST
P2 8ACDHORST
P3 28DEGMNOR
4 lettres
P1 2DFGHOPST
P2 8CDHTZ
P3 8ACORST
P4 2EGLMNR

—page 002
3 lettres
P1 8DEHPST
P2 AOT
P3 EGKMOR
4 lettres
P1 GHOST
P2
P3 8ADOS
P4 GO

—page 003
3 lettres
P1 28DGHPST
P2 8D
P3 EGLMNORS
4 lettres
P1 8DHO
P2 DT
P3 CD
P4

—page 004
3 lettres
P1 8ST
P2 CH
P3 EGOR
4 lettres
P1 DPT
P2
P3
P4 EMR

—page 005
3 lettres
P1 28ST
P2 AO
P3 EKMR
4 lettres
P1 ST
P2
P3
P4 EKR
5 lettres
P1 4S
P2 HPST
P3 28CDPT
P4 AO
P5 EKR

—page 006
3 lettres
P1 8DHST
P2 AO
P3 2EGKLMNR
4 lettres
P1 CHOT
P2 DHT
P3 AO
P4 EIKR

—page 007
3 lettres
P1 28ST
P2 AOTZ
P3 EKR
4 lettres
P1
P2
P3
P4 EK
5 lettres
P1 DT
P2
P3
P4 CT
P5

—page 008
3 lettres
P1 8DST
P2 AO
P3 EGMOR
4 lettres
P1 DOS
P2
P3 8ADO
P4 MR

—page 009
3 lettres
P1 8O
P2 SZ
P3 GMOR

—page 010
3 lettres
P1 8HST
P2
P3 EMNR
4 lettres
P1
P2
P3 EH
P4

—page 011
3 lettres
P1 8DHST
P2
P3 EKMR

—page 012
3 lettres
P1 28DEHOST
P2 ACHOT
P3 EKMNR
4 lettres
P1 8DG
P2
P3 8ACO
P4 2EKOR

—page 013
3 lettres
P1 ST
P2
P3 EMNR
4 lettres
P1 8DGST
P2 8CHT
P3 HT
P4 28

—page 014
3 lettres
P1 8HST
P2 CSTZ
P3 8EGMNR

—page 015
3 lettres
P1 28DHST
P2 ACDOTZ
P3 EGHIKMNOR
4 lettres
P1 28DEGPST
P2 2CSZ
P3 8HP
P4 EGKOR

—page 016
3 lettres
P1 28DHPRST
P2 AO
P3 EMNR
4 lettres
P1 8CDOST
P2 ADHO
P3 AO
P4 8ELMNR

—page 017
3 lettres
P1 28DGHOPST
P2 8ACOTZ
P3 EMR
4 lettres
P1 GO
P2 8HR
P3
P4 8EMR

—page 018
3 lettres
P1 8DHOST
P2 DHOPTZ
P3 EGR
4 lettres
P1 8FGPT
P2 8DH
P3 AEOR
P4 8EKMR

—page 019
3 lettres
P1 28DFGHOST
P2 8ADHO
P3 EGMOR
4 lettres
P1 8T
P2
P3 AO
P4 ER
5 lettres
P1
P2
P3 DH
P4
P5

—page 020
3 lettres
P1 28DHPST
P2
P3 EMNR

—page 021
3 lettres
P1 8FHPST
P2 2DST
P3 MN

—page 022
3 lettres
P1 8DHST
P2 8AOT
P3 KMNR
4 lettres
P1
P2 HPTZ
P3 DH
P4

—page 023
3 lettres
P1 8DPST
P2 AO
P3 EMR
4 lettres
P1 8DGOS
P2 DHOP
P3 ST
P4

—page 024
3 lettres
P1 8FGO
P2
P3 ELMNR
4 lettres
P1 4DGO
P2 DH
P3 AOST
P4 8R

—page 025
3 lettres
P1 8DHPST
P2
P3 8DEMNR
4 lettres
P1 24GHOST
P2 8CDEO
P3 8S
P4 ER

—page 026
3 lettres
P1 8DGHOT
P2 DHSTZ
P3 DKMR
4 lettres
P1 4GOT
P2 DH
P3 DHST
P4

—page 027
3 lettres
P1 28DHST
P2 8AO
P3 2EGKMNR
4 lettres
P1 DHORS
P2 8DH
P3
P4 MR

—page 028
3 lettres
P1 28DHRST
P2 AO
P3 EGLMR
4 lettres
P1 4T
P2
P3 8DH
P4 EMR

—page 029
3 lettres
P1 28DGST
P2 DT
P3 EGMT
4 lettres
P1 48HT
P2 DP
P3 DHSZ
P4

—page 030
3 lettres
P1 28T
P2
P3 EGLMR
4 lettres
P1 GT
P2 DGHO
P3 8HTZ
P4

—page 031
3 lettres
P1 248ST
P2 AOST
P3 EGKMNPR
4 lettres
P1 48GO
P2 DEP
P3
P4

—page 032
3 lettres
P1 28DHORST
P2 ACO
P3 EGMNOR
4 lettres
P1 DFGHOP
P2 8CDEHTZ
P3 AO
P4 EMNR
5 lettres
P1 DGOT
P2 DHT
P3 CZ
P4
P5 EKR

—page 033
3 lettres
P1 8ST
P2
P3 EKMNR
4 lettres
P1 DH
P2 DHTZ
P3 AO
P4 EMNR
5 lettres
P1 48ST
P2 GO
P3 CSTZ
P4
P5

—page 034
3 lettres
P1 28DST
P2 8AOST
P3 8KMR
4 lettres
P1 48GT
P2 DHT
P3
P4 EGKOR

—page 035
3 lettres
P1 8DHT
P2 AO
P3 EMR
4 lettres
P1 DGHOPS
P2
P3 AO
P4

—page 036
3 lettres
P1 28GOT
P2 DH
P3 EGMRT
4 lettres
P1 8DGO
P2 HT
P3 AO
P4 EGKMR

—page 037
3 lettres
P1 8HST
P2 AOT
P3 8EMR
4 lettres
P1 28GOS
P2 HTZ
P3 DP
P4 8GOR
5 lettres
P1 4T
P2 HP
P3
P4 CT
P5

—page 038
3 lettres
P1 28CFHOPST
P2 ACOZ
P3 2EMR
4 lettres
P1 GO
P2 DHP
P3 HOPT
P4 2EGMR

—page 039
3 lettres
P1 28DHST
P2 DH
P3 ER
4 lettres
P1 8DOPST
P2 DHP
P3 2R
P4 ER
5 lettres
P1
P2 HS
P3
P4
P5

—page 040
3 lettres
P1 8T
P2 ST
P3 EMR
4 lettres
P1 EH
P2 TZ
P3 8H
P4

—page 041
3 lettres
P1 8DFGHOS
P2 ADHOTZ
P3 EKMNR
4 lettres
P1 28DGO
P2 8ADHP
P3 TZ
P4 EMR

—page 042
3 lettres
P1 28DGHST
P2 DHTZ
P3 EKMR
4 lettres
P1 8FGHOT
P2 8DH
P3 8HT
P4 KM

—page 043
3 lettres
P1 8ST
P2 AEHO
P3 EKMNR
4 lettres
P1 GOT
P2 DEFHT
P3 ST
P4 MNR

—page 044
3 lettres
P1 28HST
P2 AO
P3 EKMNR
4 lettres
P1 CDHT
P2 DEH
P3
P4 2ELR

—page 045
3 lettres
P1 248DGHST
P2 AO
P3 8EKMR
4 lettres
P1 CHOPT
P2
P3 AO
P4 2EGKMNR

—page 046
3 lettres
P1 ST
P2
P3 8EGR
4 lettres
P1 8DGHOT
P2 8CDEHPR
P3
P4 EKMR

—page 047
3 lettres
P1 8T
P2 TZ
P3 LMN
4 lettres
P1 8S
P2
P3
P4
5 lettres
P1 4T
P2
P3
P4 ST
P5

—page 048
3 lettres
P1 8ST
P2
P3 EMR

—page 049
3 lettres
P1 28FO
P2
P3 EMR
4 lettres
P1 CST
P2
P3 8C
P4
5 lettres
P1 GO
P2 DH
P3
P4
P5
6 lettres
P1 GO
P2
P3
P4
P5 8T
P6

—page 050
3 lettres
P1
P2 CD
P3
4 lettres
P1 8DHST
P2 8COP
P3 8CDO
P4
5 lettres
P1 8DGHOPT
P2 HP
P3 CT
P4
P5 2E

—page 051
3 lettres
P1 8HPRST
P2 AO
P3 28EGKLMNOR

—page 052
3 lettres
P1 8DS
P2 8OST
P3 8EFGOR
4 lettres
P1
P2
P3 ST
P4

—page 053
3 lettres
P1 8DS
P2
P3 8EMR
4 lettres
P1 4OT
P2
P3 DH
P4 ER
5 lettres
P1 4GOT
P2 HP
P3 CDHT
P4

P5 ER

—page 054
3 lettres
P1 28ST
P2 CS
P3 ELMNR
4 lettres
P1
P2
P3 AEOR
P4 EMR

—page 055
3 lettres
P1 48DST
P2 DH
P3 2EGPR
4 lettres
P1 4HST
P2 GO
P3 CDEH
P4 8R

—page 056
3 lettres
P1 8DHOST
P2 8CSTZ
P3 2EGLMNR
4 lettres
P1 8DGHO
P2 8D
P3 8CHSZ
P4

—page 057
3 lettres
P1 248RST
P2 ACO
P3 EGLMNR
4 lettres
P1 248DRT
P2 CZ
P3 ACDO
P4 GO
5 lettres
P1 GR
P2 CT
P3 TZ
P4
P5

—page 058
3 lettres
P1 DHST
P2 AOTZ
P3 2EM
4 lettres
P1
P2 CDT
P3
P4

—page 059
3 lettres
P1 28RST
P2 AI
P3 8CEGMR
4 lettres
P1 8DST
P2
P3 8CDP
P4 8AEGO
5 lettres
P1 28GO
P2 DHT
P3
P4 8CT
P5 AG
6 lettres

P1 GO
P2
P3 DH
P4
P5 8C
P6 2EGR

—page 060
3 lettres
P1 28D
P2 AO
P3 2CMR
4 lettres
P1 28CGT
P2 DP
P3
P4 28EGKOR
5 lettres
P1 ADEOST
P2 CDHT
P3 CDFHTZ
P4 8C
P5 2ER

—page 061
3 lettres
P1 8DHRST
P2 AOTZ
P3 2EGKMNOR
4 lettres
P1 28OT
P2 ST
P3
P4

—page 062
3 lettres
P1 8DHORST
P2 AOST
P3 EMNR
4 lettres
P1 HPST
P2
P3
P4 ELR

—page 063
3 lettres
P1 28EFH
P2
P3 MR
4 lettres
P1
P2 CDHOR
P3 AO
P4 EKMNR
5 lettres
P1
P2
P3 DH
P4
P5

—page 064
3 lettres
P1 28HOST
P2 AO
P3 EKMNR
4 lettres
P1 ADGHOST
P2 CDEORSTZ
P3 8CDH
P4 EKMNR

—page 065
3 lettres
P1 248ADEHIOST
P2 8ACDEHO
P3 DEGKMR
4 lettres

P1 8DEGOST
P2 CDHOT
P3 28D
P4 EN
5 lettres
P1
P2 DH
P3 CDHT
P4 CZ
P5 ER

—page 066
3 lettres
P1 28DHORST
P2 8C
P3 EN
4 lettres
P1 2DHST
P2 CDHT
P3 8CDOT
P4 EKMNR
5 lettres
P1
P2 DEH
P3 CT
P4
P5 KMR

—page 067
3 lettres
P1 8DHOPST
P2
P3 ELMNR
4 lettres
P1 28DEHO
P2 ET
P3 DH
P4 EMO

—page 068
3 lettres
P1 8DHOST
P2 AO
P3 ELMNR
4 lettres
P1 8DGHT
P2 CDGO
P3 EH
P4

—page 069
3 lettres
P1 8HST
P2 TZ
P3 LMNR

—page 070
3 lettres
P1 8DGHOT
P2 ADHO
P3 EKM
4 lettres
P1 DGHO
P2 DHTZ
P3
P4 EMR
5 lettres
P1
P2
P3
P4 AO
P5

—page 071
3 lettres
P1 28DST
P2 8DH
P3 EMNR
4 lettres
P1 DFGHOST

P2 DH
P3 AO
P4 ER

—page 072
3 lettres
P1 28ST
P2 8AHO
P3 ELMNR
4 lettres
P1 GO
P2 ST
P3
P4 ER

—page 073
3 lettres
P1 8D
P2 DE
P3 AMNRZ

—page 074
3 lettres
P1 8DHOS
P2 AO
P3 EMNR

—page 075
3 lettres
P1 28DEFGST
P2 CDEF
P3 8EGMR
4 lettres
P1 8DHST
P2 8CDGHPST
P3 8CDO
P4 2EGKMNOR
5 lettres
P1 8EFGHPT
P2
P3
P4 8S
P5 EKMR

—page 076
3 lettres
P1 28DGHPST
P2 8ADO
P3 8EGKMNR
4 lettres
P1 DEGOST
P2 CDFHOPR
P3 8ADO
P4 EKMNR

—page 077
3 lettres
P1 28DGHOST
P2 8DR
P3 EKMNR
4 lettres
P1 DGOP
P2 DERST
P3 AO
P4 EGKMNOR
5 lettres
P1 4EGO
P2
P3
P4 AO
P5 ER

—page 078
3 lettres
P1 28DE
P2
P3
4 lettres
P1 4DOST
P2 DFR

P3 8D
P4 EKMR
5 lettres
P1 2DHP
P2 DF
P3 CO
P4
P5 MNR

—page 079
3 lettres
P1
P2
P3 KM
4 lettres
P1 28DGST
P2
P3 8D
P4
5 lettres
P1 GOT
P2 DH
P3 CS
P4
P5 8G
6 lettres
P1
P2
P3
P4
P5 8C
P6 8G

—page 080
3 lettres
P1 28
P2
P3 EGKMR
5 lettres
P1 EO
P2
P3 DH
P4 8ACO
P5
6 lettres
P1 GO
P2
P3
P4 CO
P5
P6

—page 081
3 lettres
P1 28DHRST
P2 AO
P3 2EGHKLMNOR
4 lettres
P1 4DHT
P2 CDFHOSZ
P3 8DEH
P4 ER
5 lettres
P1 48T
P2 CDHO
P3 8DHPR
P4 AOTZ
P5

—page 082
3 lettres
P1 28DHPRST
P2 AO
P3 DEGKLMNOR
4 lettres
P1 DGHT
P2 DEHTZ
P3
P4 EGMR
5 lettres
P1
P2
P3
P4
P5 LM

—page 083
3 lettres
P1 28DGORST
P2 8ADHO
P3 KMR
4 lettres
P1 GHOST
P2 CDHIO
P3 8CDH
P4
5 lettres
P1 DGO
P2 DFHPT
P3 CGT
P4
P5
6 lettres
P1
P2 8DH
P3 8DH
P4 CGO
P5
P6

—page 084
3 lettres
P1 OT
P2 8CD
P3 2FGMR
4 lettres
P1 4CGHOST
P2 CDHO
P3 8CDZ
P4 GKMOR
5 lettres
P1 DOST
P2 DHZ
P3
P4
P5 28E

—page 085
3 lettres
P1 ST
P2
P3 EKMR
4 lettres
P1 4GOT
P2 DH
P3 8D
P4

—page 086
3 lettres
P1 8DEHST
P2 DOSTZ
P3 AEGOR

—page 087
3 lettres
P1 8DGOST
P2 ADHO
P3 EKMNR
4 lettres
P1 4DEGHO
P2 DH
P3 DR
P4

—page 088
3 lettres
P1 8HOST
P2 DH
P3 8EKMR
4 lettres
P1 GO
P2 DH
P3
P4

—page 089
3 lettres
P1 28DERST
P2 8CD
P3 CEGKMOPR
4 lettres
P1 HOST
P2 CDHOSZ
P3 28ACDT
P4 2E
5 lettres
P1 DGOS
P2
P3 CT
P4
P5 KMR

—page 090
3 lettres
P1 8HST
P2 8C
P3 8GKMR
4 lettres
P1 28GHOPST
P2 8DEH
P3
P4 2KMR
5 lettres
P1 8CDEGOT
P2 DH
P3 CT
P4
P5

—page 091
3 lettres
P1 8DHST
P2 8COT
P3 EGKMNR

—page 092
3 lettres
P1 28DHPST
P2 AOSTZ
P3 EMR
4 lettres
P1
P2 CDGO
P3 8DHRT
P4 2G

—page 093
3 lettres
P1 8EHOST
P2 AO
P3 8EGMO
4 lettres
P1 DHOT
P2 8CEHS
P3 8C
P4 EKMN
5 lettres
P1
P2 DH
P3 DS
P4 8C
P5

—page 094
3 lettres
P1 EHST
P2 8C
P3 28EGR
4 lettres
P1 8GHOST
P2 CDHOTZ
P3 8CEHRZ
P4 EKNR
5 lettres
P1 8EFGO
P2 DHST
P3 CT
P4 8C
P5 NR

—page 095
3 lettres
P1 8DHRST
P2
P3 EGMOR
4 lettres
P1 8DHOPST
P2 EHT
P3 8ES
P4 EGHOR

—page 096
3 lettres
P1 28DOST
P2 ACO
P3 EGKMNOR
4 lettres
P1 8HO
P2 COTZ
P3 CDH
P4 EGOR
5 lettres
P1 48DST
P2 FH
P3 8DH
P4
P5 GKMO

—page 097
3 lettres
P1 8DOT
P2
P3 MR
4 lettres
P1 DHP
P2 28CDEHOP
P3 AI
P4 EKMR
5 lettres
P1 GO
P2
P3
P4
P5 NR

—page 098
3 lettres
P1 8DGH
P2
P3 MR
4 lettres
P1 DGOST
P2 8CDEFHOT
P3 8ACDO
P4 EMR
5 lettres
P1 8COT
P2 DE
P3 CDRTZ
P4 8C
P5

—page 099
3 lettres
P1 8DHORS
P2 AO
P3 EKMR

4 lettres
P1 4T
P2 DHSTZ
P3 8ADO
P4 EK
5 lettres
P1
P2
P3 DH
P4 CT
P5

—page 100
3 lettres
P1 248DT
P2
P3 8E
4 lettres
P1
P2
P3
P4 EK

—page 101
3 lettres
P1 8DGOST
P2 ADHO
P3 GKMR
4 lettres
P1
P2
P3 DFH
P4

—page 102
3 lettres
P1 28DHRST
P2 AO
P3 EGKMOR
4 lettres
P1 HPST
P2 OTZ
P3
P4 ER

—page 103
3 lettres
P1 8T
P2 8AHO
P3 28EGHRSZ
4 lettres
P1 8T
P2 HR
P3
P4 2E

—page 104
3 lettres
P1 8DST
P2 DH
P3 EKM
4 lettres
P1 DGHOST
P2
P3
P4
5 lettres
P1 HS
P2 ST
P3
P4
P5

—page 105
3 lettres
P1 28DGHOT
P2 ACO
P3 DEGKMR
4 lettres
P1 ST
P2 DH
P3 CH
P4 2E

—page 106
3 lettres
P1 28GHOT
P2
P3 EKMR
4 lettres
P1 DH
P2 DET
P3
P4 EKMR

—page 107
3 lettres
P1 28DOST
P2 8AD
P3 2EGKMNR
4 lettres
P1 GOT
P2 8CDHRS
P3 8ACOTZ
P4 8EMNR
5 lettres
P1
P2
P3
P4
P5 EKMR

—page 108
3 lettres
P1 8OT
P2 8CDR
P3 AG
4 lettres
P1 GO
P2 CDHRT
P3 8DMR
P4 EKLMNR

—page 109
3 lettres
P1 8DGHPST
P2 8ACO
P3 EGMR
4 lettres
P1 28CDHOT
P2 CDHTZ
P3 8ADEHO
P4 ER
5 lettres
P1 GO
P2 EH
P3 DT
P4 2T
P5

—page 110
3 lettres
P1 28DST
P2 ST
P3 8EGMOR
4 lettres
P1 DHO
P2
P3
P4
5 lettres
P1 4DHT
P2 CTZ
P3 HR
P4
P5 EGOR
6 lettres
P1 24T
P2
P3 DH
P4 CT
P5
P6

—page 111
3 lettres
P1 8H
P2
P3 EKM
4 lettres
P1 28DHST
P2 CT
P3 8CHT
P4 GO
5 lettres
P1 DST
P2
P3 COT
P4
P5
6 lettres
P1
P2
P3
P4
P5 CZ
P6

—page 113
3 lettres
P1 248DHOST
P2 8ACEHOP
P3 EKMR
4 lettres
P1 248ADGHOPST
P2 28ACDEHORS
P3 8ACDEHORT
P4 2EGKMR
5 lettres
P1 248CDGHOST
P2 CDHOT
P3 ACDER
P4 8ACEFORTZ
P5 2EGKMR
6 lettres
P1 GO
P2 8DEH
P3 DH
P4 ADEO
P5 AO
P6 ER

—page 117
3 lettres
P1 248ADEORST
P2 8ACDEO
P3 8EGMOR
4 lettres
P1 248ADEFGOPRST
P2 8ACDEO
P3 8CDEGHOR
P4 8EGMORZ
5 lettres
P1 2DEGPST
P2 CSTZ
P3 CDFHO
P4 8ACDOSTZ
P5 8EGR
6 lettres
P1 4EGOPST
P2 CDHOP
P3 CDHT
P4 COT
P5 28C
P6 2G

—page 118
3 lettres
P1 28DOT
P2 8ACO
P3 28EGMOR
4 lettres
P1 DHPT
P2 CDHOT
P3 8DH
P4 EKMR
5 lettres
P1 DST
P2 CO
P3 COT
P4
P5

—page 119
3 lettres
P1 8O
P2
P3 KMR

—page 121

—page 125

—page 126

—page 128

—page 129
3 lettres
P1
P2 8C
P3 EK
5 lettres
P1 OS
P2
P3
P4
P5

—page 131
3 lettres
P1 8HRST
P2 8CZ
P3

—page 134
3 lettres
P1 8DGHST
P2 8ACEO
P3 EKM
4 lettres
P1 OST
P2 CDEHR
P3
P4 EGKMO

—page 147
3 lettres
P1 248ADEORST
P2 AEHO
P3 EKMNR
4 lettres
P1 ADEGHOPST
P2 28CDEHSZ
P3 8CDEH
P4 AEGKMNR
5 lettres
P1 248DEGHPST
P2 CDEHRST
P3 8CDERT
P4 8ACDH
P5 28EGKLMNR
6 lettres
P1
P2 DEH
P3 ACDHOS
P4 CT
P5 28CS
P6

—page 148
3 lettres
P1 248DEHST
P2 ACOZ
P3 8EGMNR
4 lettres
P1 248DEGHRST
P2 8CDEHOPRST
P3 28ACDEHO
P4 8EGMNR
5 lettres
P1 248DEGOPST
P2 DEHPST
P3 CDHOSTZ
P4 8CDH
P5 8EGKMNR
6 lettres
P1 8GO
P2 8DEPT
P3 DHST
P4 CGT
P5 8CT
P6 28G

—page 149
3 lettres
P1 248DEORST
P2 28ACDEHMO
P3 28AEGMNPR
4 lettres
P1 8ADEGOST
P2 8ACDEHOPRST
P3 8ACDHOPT
P4 8AEGMNR
5 lettres
P1 8ADEOPST
P2 CDEHOPST
P3 8DEHRST
P4 8CDT
P5 28EGMNR
6 lettres
P1 EGOPST
P2 DEHPS
P3 DEHPST
P4 CTZ
P5 8CF
P6 8GO

—page 150
3 lettres
P1 248AEHORST
P2 8ACEHO
P3 2DEGMR
4 lettres
P1 28DEHOST
P2 DEHST
P3 8ACDHOT
P4 2CEGLMNR
5 lettres
P1 248DEHOST
P2 CDHSTZ
P3 DHP
P4 8CDHZ
P5 EKMNR
6 lettres
P1 48AEOST
P2 DEHPST
P3 8CDHT
P4
P5 8C
P6 28GR
7 lettres
P1
P2 DE
P3 CDH
P4 CSZ
P5
P6
P7

—page 151
3 lettres
P1 248EHPRST
P2 8ACO
P3 28EGKMNR
4 lettres
P1 4HST
P2 CDEHOST
P3 8CDH
P4 28EGR
5 lettres
P1 28CDEGPST
P2 CDGHOP
P3 DEH
P4 8ADHO
P5 EMNR
6 lettres
P1
P2
P3 CDHS
P4
P5 8C
P6
7 lettres
P1
P2 CO
P3 8DH
P4
P5
P6
P7

—page 152
3 lettres
P1 248DERST
P2 8ACOST
P3 28EGMR
4 lettres
P1 4EHOPST
P2 8D
P3 8CDEHRT
P4 2EGMR
5 lettres
P1 248CDEFGHOPST
P2 8CDHST
P3 DHR
P4 8ACOTZ
P5 28EGKMN
6 lettres
P1 8R
P2 CO
P3 DHST
P4
P5 8C
P6

—page 153
3 lettres
P1 248ADGHOR
P2 ADEHO
P3 28EKMNR
4 lettres
P1 DEGHOST
P2 2ACDEHTZ
P3 8CDE
P4 8EGMNR
5 lettres
P1 248DEGHOPST
P2 CDHPS
P3 CDHT
P4 CDHT
P5 ELMNR
6 lettres
P1 4EGOST
P2 DH
P3 DH
P4 CT
P5 8C
P6

—page 154
3 lettres
P1 248ACDEHORST
P2 8ACEHOR
P3 2AEGMPR
4 lettres
P1 8DEGHOST
P2 CDHST
P3 8ACHO
P4 EMR
5 lettres
P1 8DEGOPRS
P2 DHST
P3 CT
P4 8CHS
P5 EMNR
6 lettres
P1 GO
P2 DEFHP
P3 DHST
P4
P5 8C
P6

—page 155
3 lettres
P1 248EHOPST
P2 8AEHOR
P3 2DEGHKMOR
4 lettres
P1 48DEGHOPST
P2 8CDEHOST
P3 8ACDEHOZ
P4 AEGKMR
5 lettres
P1 DGHORST
P2 CDEHST
P3 CDEHST
P4 8ACOT
P5 2EMNR
6 lettres
P1 4T
P2 HP
P3 CDEFHST
P4 CST
P5 8C
P6

—page 156
3 lettres
P1 248DEGHOPRST
P2 DEHR
P3 AEGKMNOR
4 lettres
P1 28DEHOPRST
P2 CDEHOPRST
P3 8ACDEHOT
P4 AEGKMR
5 lettres
P1 48DEGHOPST
P2 CDEHST
P3 CDEHS
P4 8ACDOT
P5 2EGLMR
6 lettres
P1 GO
P2 DFHP
P3 CDHT
P4 CST
P5 8C
P6 2G

—page 157
3 lettres
P1 248CDEHOPRST
P2 ACDEHOR
P3 EGHMNOR
4 lettres
P1 8ADEGHOPRST
P2 DHRSTZ
P3 8ACDHO
P4 2AEGKMOR
5 lettres
P1 48EFHOPRST
P2 EHPR
P3 CDHT
P4 8ACDOT
P5 EKMNR
6 lettres
P1 EO
P2 EP
P3 DH
P4 ACZ
P5 8C
P6 ER
7 lettres
P1
P2
P3 DH
P4
P5
P6
P7

—page 158
3 lettres
P1 248DEHOPRST
P2 8ACDHOPT
P3 2AEGMNR
4 lettres
P1 248ADEHORST
P2 8ADEHPRT
P3 8ACDEGHOZ
P4 AEGMNR
5 lettres
P1 248DEFGHOPST
P2 DEST
P3 DHRST
P4 8ACDO
P5 2EGLMNR
6 lettres
P1 24AO
P2
P3 DHST
P4 CT
P5 8AC
P6 CG

—page 159
3 lettres
P1 248DEHRST
P2 ADEHORST
P3 2AEGMR
4 lettres
P1 8EGHOST
P2 8DEHR
P3 8CH
P4 EKMR
5 lettres
P1 8EGOPST
P2 DHST
P3 DHP
P4 8ACO
P5 EMR
6 lettres
P1 GO
P2 DEPS
P3 DHT
P4
P5 8C
P6

—page 160
3 lettres
P1 248DEGHOPRST
P2 8ACDOS
P3 DEGMPR
4 lettres
P1 8ADGHOPST
P2 ACDFH
P3 8CDHT
P4 EMNR
5 lettres
P1 8DEGOPRST
P2 CDHSTZ
P3 DEHN
P4 8CDHST
P5 AEGMNR

—page 161
3 lettres
P1 248DEGRST
P2 8ACEORT
P3 2EGKMR
4 lettres
P1 EHRST
P2 DHST
P3 8ACDEHOT
P4 8EGNR
5 lettres
P1 248EOPRST
P2 CDHST
P3 CDHZ
P4 8ACOTZ
P5 EMNR
6 lettres
P1 8D
P2 DHOT
P3 CDHST
P4 CT
P5 8C
P6

—page 162
3 lettres
P1 248DHOPRST
P2 8ACDHO
P3 2DEGMR
4 lettres
P1 4ADEHPST
P2 2CDHRST
P3 8ACDHO
P4 EMN
5 lettres
P1 48EGHOPRST
P2 DST
P3 DEH
P4 8ACO
P5 EMNR
6 lettres
P1 GO
P2 DEHP
P3 CDHST
P4 CST
P5 8C
P6

—page 163
3 lettres
P1 28DEHRST
P2 8ACDO
P3 8EGKMR
4 lettres
P1 CDGHOPRST
P2 8CDH
P3 8ACDHOPT
P4 EGLMR
5 lettres
P1 2EHORST
P2 CDEHOST
P3 CDHSTZ
P4 8ACGHOT
P5 EMR
6 lettres
P1 ER
P2 EH
P3 DH
P4 CTZ
P5 8C
P6 ER

—page 164
3 lettres
P1 248DEHST
P2 AO
P3 8EGMNR
4 lettres
P1 HST
P2 CDEH
P3 8ACDHO
P4 8EGMR
5 lettres
P1 8HST
P2 DEP
P3 DH
P4 8ACDO
P5 EMNR
6 lettres
P1
P2
P3 DH
P4
P5 8ACEO
P6 8G

—page 165
3 lettres
P1 248ADEHOPRST
P2 AEHOR
P3 AEGKMOR
4 lettres
P1 28GHOST
P2 4CDEHRSTZ
P3 8ACDHOT
P4 EMR
5 lettres
P1 8EGHOPRST
P2 DEFHPRST
P3 ACDHPTZ
P4 8ACEOTZ
P5 EMR
6 lettres
P1 AGO
P2 DEH
P3 CDHST
P4
P5 8C
P6

—page 166
3 lettres
P1 248ADEHOPRST
P2 8ACO
P3 2EGKMR
4 lettres
P1 248DEGHOST
P2 CDEHRST
P3 8ACDMOT
P4 EMR
5 lettres
P1 8DEGORST
P2 DHT
P3 ACT
P4 8ACEOS
P5 EMNR
6 lettres
P1 248GO
P2 EF
P3 CDEHST
P4 CGOT
P5 8C
P6 GR

—page 167
3 lettres
P1 28DEGHRST
P2 8ACEHOR
P3 28EFGKMR
4 lettres
P1 28ADEGHOPST
P2 8CDEFHOPRS
P3 8ACO
P4 28EGKMR
5 lettres
P1 48DGHOPST
P2 ACDHOPSTZ
P3 8CDEFHOPRST
P4 8ACOT
P5 EMR
6 lettres
P1 4EGOT
P2 DEHS
P3 CDFHPST
P4 COSTZ
P5 8CST
P6 GO

—page 168
3 lettres
P1 28H
P2
P3 MR
4 lettres
P1
P2
P3 AO
P4

—page 169
3 lettres
P1 28DEGHOPST
P2 8ACDEFHOSTY
P3 28EGKLMNR
4 lettres
P1 248AEGHOST
P2 8CDEFHOPRSZ
P3 8ACDHOTZ
P4 EGKLMOR
5 lettres
P1 48AGHOPST
P2 AOPR
P3 8DEHPTZ
P4 8ACO
P5 8EGKMR
6 lettres
P1 EG
P2 DFHPR
P3 CDHT
P4 CST
P5 8C
P6

—page 172
3 lettres
P1 28DHOST
P2 8ACDHOPZ
P3 8AEGKMNOR
4 lettres
P1 248ADEGHOPST
P2 28ACDHOPRST
P3 8ACDHOPS
P4 AEGKMNR
5 lettres
P1 4EGHOST
P2 DHPT
P3 8CDHOPSTZ
P4 8CDIMS
P5 2EGKMOR
6 lettres
P1
P2
P3 DH
P4
P5
P6 2G

—page 173
3 lettres
P1 28HRST
P2
P3 EKMR
4 lettres
P1 4DGHO
P2 8DHST
P3 8C
P4 KMR
5 lettres
P1 8DGH
P2 ST
P3 DH
P4 8C
P5 KM

—page 175
3 lettres
P1 28DHST
P2 AO
P3 2CEMOR
4 lettres
P1 DHST
P2 CTZ
P3
P4 2ER
5 lettres
P1 2DH
P2 AO
P3
P4
P5

—page 180
3 lettres
P1 248DHT
P2
P3 2DELM
4 lettres
P1 DS
P2 TZ
P3
P4 2R
5 lettres
P1 GP
P2
P3
P4
P5 EK

—page 181
3 lettres
P1 28DHOT
P2 AO
P3 2EKMR
4 lettres
P1 8GHPST
P2 CZ
P3 ACGO
P4 2EGKR
5 lettres
P1 4GOT
P2
P3
P4 AO
P5 ER
6 lettres
P1
P2

P3
P4 CZ
P5
P6 ER

—page 182
3 lettres
P1 28ST
P2
P3 2EKMR
4 lettres
P1 4ST
P2 8DEHR
P3 8CDO
P4 2EGR
5 lettres
P1 48ST
P2 CO
P3 CDHOT
P4
P5 EG
6 lettres
P1
P2
P3 DH
P4
P5
P6 EKR

—page 183
3 lettres
P1 28H
P2
P3 EKMNR
4 lettres
P1 2EHS
P2
P3 8P
P4 2KMR
5 lettres
P1 4ST
P2
P3 8D
P4 8D
P5 MR

—page 184
3 lettres
P1 248CDEHST
P2 8ADO
P3 2EGKMOR
4 lettres
P1 4DOST
P2 CDHORT
P3 8ACDGOZ
P4 EGKOR
5 lettres
P1 24GOST
P2 ADOT
P3
P4 8ADO
P5 AGO
6 lettres
P1 ST
P2 EP
P3 DHT
P4
P5 8C
P6

—page 185
3 lettres
P1 248DEHRST
P2 AO
P3 28EGKMNOR
4 lettres
P1 28CDGHST
P2 8CDFHO
P3 8AHO
P4 2EMR
5 lettres
P1 4GT
P2
P3
P4 CO
P5 2GKR

—page 186
3 lettres
P1 28DHRST
P2 8ACO
P3 2EGKMOR
4 lettres
P1 4DFHOPST
P2 8DH
P3 8ADO
P4 2EKMR

—page 187
3 lettres
P1 8DHT
P2 AO
P3 2ER
4 lettres
P1 4T
P2
P3 DEF
P4 8EKR
5 lettres
P1 4S
P2
P3
P4
P5 8ER

—page 188
3 lettres
P1 28ST
P2
P3 ER

—page 189
3 lettres
P1 28
P2 AO
P3 2EKMR
4 lettres
P1 DST
P2
P3
P4 EK

—page 190
3 lettres
P1 28DHRST
P2
P3 ER
4 lettres
P1 4DOST
P2
P3 CP
P4 2ER
5 lettres
P1 ST
P2
P3
P4
P5

—page 191
3 lettres
P1 28EHST
P2 AO
P3 EGKMNOR
4 lettres
P1 DFGHST
P2 8CHTZ
P3 8DS
P4 2ER
5 lettres
P1 DHST
P2 DH
P3
P4
P5 28EGKMR

—page 192
3 lettres
P1 28DHPST
P2 DEH
P3 AGMOR
4 lettres
P1 DHS
P2 CZ
P3
P4 2EK
5 lettres
P1 OT
P2
P3 CT
P4
P5

—page 193
3 lettres
P1 28DOST
P2 8ACO
P3 2EKMR
4 lettres
P1 4GOT
P2 28DEHR
P3
P4 EMR
5 lettres
P1
P2
P3 CO
P4 AO
P5 EM

—page 194
3 lettres
P1 28HRT
P2 DEH
P3 KMR
4 lettres
P1 4CDGHOT
P2 DH
P3 8ACDO
P4 EM
5 lettres
P1 GH
P2 CDHLOS
P3 8CDHOT
P4 8C
P5 MR

—page 195
3 lettres
P1 8DHOST
P2 8CDH
P3 ELMR
4 lettres
P1 GOT
P2 8DFH
P3 DH
P4 MR
5 lettres
P1
P2 ST
P3 DFH
P4
P5 MR

—page 196
3 lettres
P1 8DHOST
P2 8H
P3 EMR
4 lettres
P1 HOT
P2 28DFHO
P3
P4 EKMNR
5 lettres
P1 48DH
P2
P3 DH
P4 AO
P5 ER

—page 197
3 lettres
P1 28DEHOST
P2 AO
P3 2MR
4 lettres
P1 AO
P2 CDHO
P3 8D
P4 EMR

—page 198
3 lettres
P1 28CDFGHORT
P2 8ACHO
P3 EMR
4 lettres
P1 8DHOST
P2 8CDHORT
P3
P4 2EGMR
5 lettres
P1 8GHO
P2
P3 8CDHOT
P4
P5 EMNR

—page 199
3 lettres
P1 2EHT
P2
P3 2ER
4 lettres
P1 HST
P2
P3
P4 ER

—page 200
3 lettres
P1 2DT
P2 AO
P3
4 lettres
P1 DH
P2 8P
P3
P4

—page 201
3 lettres
P1 28DHRST
P2
P3 EMR
4 lettres
P1 DOST
P2 CERZ
P3 8ER
P4 2EGKMR
5 lettres
P1 DFGHOPT
P2
P3 CDHT
P4 AO
P5 ER

—page 202
3 lettres
P1 28GRT
P2 AO
P3 EM
4 lettres
P1 EG
P2 8DEH
P3 8AOS
P4 EMR
5 lettres
P1 4DGHOT
P2
P3
P4 ACOZ
P5 EGMOR

—page 203
3 lettres
P1 28GRST
P2
P3 2EIMR
4 lettres
P1 DS
P2
P3 AO
P4 8R
5 lettres
P1
P2 ST
P3
P4
P5
6 lettres
P1
P2
P3 DH
P4 CZ
P5
P6 2G

—page 204
3 lettres
P1 28ST
P2 2ACO
P3 8EGMOR
4 lettres
P1
P2
P3 ACDO
P4 ER
5 lettres
P1
P2
P3
P4
P5 ER

—page 205
3 lettres
P1 28DORST
P2 ACOT
P3 DEMR
4 lettres
P1 8DHOST
P2 CDEHTZ
P3 ACGO
P4 2EGR
5 lettres
P1 24DGHOPS
P2 CDHZ
P3 28ST
P4
P5 ER
6 lettres
P1 4T
P2 CO
P3
P4 CTZ
P5
P6 ER

—page 206
3 lettres
P1 4DEFOT
P2 CHP
P3 2DEGMORT
4 lettres
P1 CDHST
P2 CT
P3
P4 ER

—page 207
3 lettres
P1 ACHOST
P2 8CORZ
P3 EGMR
4 lettres
P1 28DHOT
P2 8R
P3
P4 EGMOR
5 lettres
P1 2T
P2 CT
P3 8E
P4
P5

—page 208
3 lettres
P1 28FST
P2 AO
P3 2EGMOR
4 lettres
P1 2D
P2 8AER
P3 CE
P4 MR
5 lettres
P1 4T
P2 DH
P3 CD
P4 CZ
P5 GO

—page 209
3 lettres
P1 28CHOPST
P2 8ACDO
P3 EGMOR
4 lettres
P1 DFHOST
P2 8CDEHP
P3 8CDOZ
P4 EGOR
5 lettres
P1 4GOST
P2 CDHTZ
P3 CD
P4 AO
P5 AG

—page 210
3 lettres
P1 28DPRST
P2 8ACDEGOZ
P3 2ACEGIMOR
4 lettres
P1 CDGHOST
P2 CPRZ
P3
P4 2EGORT
5 lettres
P1 GOST
P2 8DHRT
P3 CTZ
P4 AO
P5 EGOR

—page 211
3 lettres
P1 28DHOST
P2 AO
P3 EGKMOR
4 lettres
P1 4GOPRST
P2 28CDO
P3 2C
P4 2ER
5 lettres
P1 8GHOST
P2
P3 8CRZ
P4
P5 ER
6 lettres
P1 GO
P2 DH
P3 CDHT
P4 CZ
P5
P6 2ER

—page 212
3 lettres
P1 248DEHOPRST
P2 8ACDHOST
P3 DEGHKMNPR
4 lettres
P1 248ACDEHOPST
P2 8CDEHOPRST
P3 8ACDHOPTZ
P4 8DEGKMNR
5 lettres
P1 248DEGOPST
P2 DHST
P3 8CDHORT
P4 8ACOST
P5 EGMNOR
6 lettres
P1 24EGHOST
P2 8DEHPT
P3 CDHOST
P4 COT
P5 8ACGT
P6

—page 213
3 lettres
P1 248DEHPRST
P2 8ACDEHO
P3 8DEGHMR
4 lettres
P1 4ADEGHOST
P2 4CDEHOPRST
P3 8ACDHOZ
P4 EKLMR
5 lettres
P1 4DEFGHOPT
P2 DEHPST
P3 CDHST
P4 8ACHOS
P5 2EGKLMR
6 lettres
P1 AEGO
P2 DH
P3 CDHS
P4 CST
P5 8ACOS
P6 8G

—page 214
3 lettres
P1 248DEHRST
P2 8ACORS
P3 8ACEGKMOR
4 lettres
P1 48DEGHOPST
P2 28CDHOR
P3 8ACOTZ
P4 AEGMORZ
5 lettres
P1 4DOPST
P2 CDHOPRST
P3 8CDEHOPT
P4 8ACEIO
P5 8EGKMOR
6 lettres
P1 DEGOPT
P2 CDHPST
P3 CDHOSTZ
P4 8CEOTZ
P5 8CST
P6 EGMOR
7 lettres
P1
P2 HT
P3 DHPST
P4 CT
P5
P6 8T
P7

—page 215
3 lettres
P1 248CDEHPRST
P2 8ACEINORT
P3 8EGKMOR
4 lettres
P1 24ACDEFGHOPST
P2 8CDHOPRTZ
P3 8ACDHO
P4 28AEGKMNOR
5 lettres
P1 48DEGHOPST
P2 28CDHOT
P3 8CDHOTZ
P4 8CDOTZ
P5 28EGKMNR
6 lettres
P1 48AEGOS
P2 DEHPRT
P3 8CDHT
P4 ACTZ
P5 8COT
P6 8GO

—page 216
3 lettres
P1 28CDEGPRST
P2 8ACO
P3 28EGKMORY
4 lettres
P1 48ACDEGHOPST
P2 8CDEHOPR
P3 8ACDO
P4 28EGKMOR
5 lettres
P1 4DEGHOT
P2 8CDHPST
P3 8CDFOT
P4 28CHSZ
P5 2EGKLMOR
6 lettres
P1 EGO
P2 CDEHT
P3 8CDHP
P4 CO
P5 8C
P6 8G

—page 217

3 lettres
P1 28DEHPRST
P2 AINO
P3 EGMNOR
4 lettres
P1 8ADEGHOST
P2 8DEHPRT
P3 8ACOT
P4 28CEGIKMOR
5 lettres
P1 48AEFGOPT
P2 CDHOPRSTZ
P3 8CDHPST
P4 8CO
P5 28EGMNOR
6 lettres
P1 4GOT
P2 DH
P3 CDPTZ
P4 COT
P5
P6 EGMO

—page 218

3 lettres
P1 28DEFORST
P2 8ACDHO
P3 8EGIKMOR
4 lettres
P1 48ADEFGHOPRST
P2 8CDEHOPRST
P3 8ACDHO
P4 28EGKMNOR
5 lettres
P1 48DEGHOPST
P2 ACDEOST
P3 8CDHOPST
P4 8ACDEO
P5 2EGKMNR
6 lettres
P1 DEGHOST
P2 DEHPT
P3 CDHST
P4 CEORZ
P5 8C
P6 8EGO
7 lettres
P1 AO
P2
P3 DH
P4 CT
P5
P6 8T
P7 GO

—page 219

3 lettres
P1 248DEHOPRST
P2 28ACDHINO
P3 28AEGKMOR
4 lettres
P1 248ADEGHOPRST
P2 28ACDEHOPRT
P3 8ACDHOTZ
P4 2AEGKMOR
5 lettres
P1 248ADEFOPST
P2 CDEHOST
P3 8CDEHOPRT
P4 8ACOST
P5 28EGKMOR
6 lettres
P1 DGP
P2 DHST
P3 CDHPS
P4 COSTZ
P5 8C
P6

—page 220

3 lettres
P1 248CDEFGHOPRST
P2 8ACDHO
P3 EGMOR
4 lettres
P1 28ACDEGHOPST
P2 8ACDEHOPR
P3 8ACDO
P4 2EGKMOR
5 lettres
P1 4DEGORST
P2 CDFHOST
P3 8CDHMTZ
P4 8ACOTZ
P5 8EGMOR
6 lettres
P1 24EGHOT
P2 DEFHPT
P3 CDHOST
P4 8CRT
P5 8C
P6 8EGKMOR

—page 221

3 lettres
P1 248ADEHOPRST
P2 ACDHO
P3 EGKMNR
4 lettres
P1 48ADEGHOST
P2 8CDEHOPR
P3 8ACDO
P4 EKMR
5 lettres
P1 48ADEGOPRS
P2 ACDEHOPRT
P3 8CDHT
P4 8ACOST
P5 EGKMNOR
6 lettres
P1 4EOT
P2 DH
P3 DH
P4 CT
P5 8C
P6 GOR

—page 222

3 lettres
P1 248DEHOPRST
P2 8ACDEORT
P3 8EGKMOR
4 lettres
P1 48ADEOST
P2 8ACDEFHIRSZ
P3 8ACO
P4 8EGKMR
5 lettres
P1 48ADEGHOPRST
P2 CDFHPT
P3 CDHOT
P4 8ACDORT
P5 8AEGKMOR
6 lettres
P1 4AEGOST
P2 DHP
P3 CDHOPTZ
P4 8COTZ
P5 8ACOT
P6 8EGKMOR

—page 223

3 lettres
P1 248ADEHPRST
P2 ADOS
P3 28CDEGKLMOR
4 lettres
P1 248ADEGHOST
P2 8CDEHRSTZ
P3 8ACOT
P4 8CEGKMOR
5 lettres
P1 8CDEFGHORST
P2 CDHOST
P3 28CDHO
P4 8ACDOS
P5 EKMR
6 lettres
P1 4DEOST
P2 CDH
P3 CDHST
P4 8CO
P5 8CO
P6 8EGKLMOR
7 lettres
P1
P2 CDH
P3 DHT
P4
P5 8CS
P6 8ACO
P7 28EGMR

—page 224

3 lettres
P1 248ADEHOPRST
P2 8ACOT
P3 8DEGHKMOR
4 lettres
P1 248ADEHOPRST
P2 8CDEHORST
P3 8ACDOTZ
P4 28ADEGHKMOR
5 lettres
P1 28DEGHOPST
P2 ACDHSTZ
P3 8CDHOSTZ
P4 8ACDFOSTZ
P5 8EGKMOR
6 lettres
P1 8AEOPST
P2 DHT
P3 CDHPST
P4 COTZ
P5 8ACOST
P6 28AEGMOR

—page 225

3 lettres
P1 248ADEHOPRST
P2 8ADEIO
P3 28EGKLMOR
4 lettres
P1 28DEHOST
P2 8CDEHST
P3 28ACDHOT
P4 2DEGKMNOR
5 lettres
P1 48DEGHOPST
P2 CDEGHPT
P3 8CDEHORSTZ
P4 8C
P5 28EGKLMNOR
6 lettres
P1 4AEGOT
P2 CDFHOT
P3 8DHST
P4 DO
P5 8C
P6

—page 226

3 lettres
P1 248ADEGHORSTY
P2 8ACHOR
P3 2EGKMOR
4 lettres
P1 248ADHOPST
P2 CDEHOPR
P3 8ACDIZ
P4 EKMR
5 lettres
P1 DEGHOPS
P2 CDHTZ
P3 CDOPTZ
P4 8ACOT
P5 EKMR
6 lettres
P1 4AEGOT
P2 DHPST
P3 8CDHPST
P4 COT
P5 8CT
P6 EGMO

—page 227

3 lettres
P1 248ADEHOST
P2 8CT
P3 CDEGKMOR
4 lettres
P1 28ACDEHOST
P2 28CDEFHOPRT
P3 8ACDHO
P4 8AEGKMR
5 lettres
P1 CDEFGHOST
P2 8CDEHRTZ
P3 CDHOT
P4 8CIOT
P5 ACEGKMOR
6 lettres
P1 4DEGHOT
P2 8CDEHO
P3 8CDHPT
P4 8COT
P5 8AC
P6

—page 228

3 lettres
P1 28ACDEGHOPRST
P2 28ACDEHOP
P3 28ACEGMNOR
4 lettres
P1 48DEGHOPRST
P2 ACDHOR
P3 28ACDHORS
P4 28EGKMOR
5 lettres
P1 248DEGHORST
P2 CDHOST
P3 28CDHOPT
P4 8CDTZ
P5 28EGKMOR
6 lettres
P1 4DEHOPST
P2 ADFHOP
P3 8CDEHPST
P4 COT
P5 8CT
P6 2EGOR

—page 229

3 lettres
P1 248DEHOPRST
P2 8ADO
P3 8ADEGKMRT
4 lettres
P1 8ADEGHOST
P2 28CDEHOPRT
P3 8ACDO

P4 EGKMNOR
5 lettres
P1 4DEFGHOPRST
P2 CDEHPST
P3 ACDEHORT
P4 8ACOT
P5 AEGKMNOR
6 lettres
P1 EO
P2 DEHPST
P3 DHST
P4 COST
P5 8CT
P6
7 lettres
P1 EO
P2
P3 ADPT
P4 CT
P5 CO
P6
P7

—page 230
3 lettres
P1 28ADHORST
P2 8ACEHO
P3 28EGKMNOR
4 lettres
P1 248ACDEGHOPST
P2 8CDHOP
P3 8ACEIO
P4 28EGKMOR
5 lettres
P1 48CDEGHOPST
P2 8CDEHOPRST
P3 8CDHOTZ
P4 8ACHOP
P5 8EGMOR
6 lettres
P1 4EGHOP
P2 DEFHPT
P3 8CDHPST
P4
P5 8C
P6
7 lettres
P1
P2 DFP
P3 CDP
P4 COT
P5
P6
P7 KMR

—page 231
3 lettres
P1 28CDEGHOPRT
P2 8ACO
P3 2EGKMOR
4 lettres
P1 2DGHOST
P2 8CDEHOS
P3 8ACDEHIO
P4 28EGKMOR
5 lettres
P1 248ADFGHOST
P2 CDEHOSTZ
P3 8CDHOPT
P4 8ACOT
P5 8EGKMNOR
6 lettres
P1 GO
P2 DHOT
P3 CDHOP
P4 COT
P5 8C
P6 28GMOR

—page 232
3 lettres
P1 248DEORST
P2 8ACINOST
P3 2EGHKMOPR
4 lettres
P1 78DEGHOPRST
P2 8CDEHORSTZ
P3 8CDHOS
P4 28EFGKMOPR
5 lettres
P1 48DEFGHPRST
P2 CDEHORST
P3 8CDEHOPRT
P4 8ACOT
P5 8CEGKMOR
6 lettres
P1 4DEOST
P2 CDP
P3 CDHT
P4 CDHT
P5 8CO
P6 8EGO
7 lettres
P1 4T
P2
P3 DFHP
P4 CST
P5 CT
P6 8C
P7

—page 233
3 lettres
P1 248ADEHORSTY
P2 8ACDHOT
P3 28CEGHKMOR
4 lettres
P1 48CDEGHOPST
P2 8CDEFHOPRST
P3 8ACDHO
P4 28EGHKMOR
5 lettres
P1 48DEGHORST
P2 CDEHPRST
P3 8CDHOPT
P4 8ACOT
P5 28EGKMOR
6 lettres
P1 48DEFGOT
P2 DEHP
P3 CDHST
P4 8COT
P5 8CT
P6 28GO

—page 234
3 lettres
P1 248ACEHORST
P2 8ACDEFHORZ
P3 28ADEGKMOR
4 lettres
P1 28ADEORST
P2 28CDEHKPRSTZ
P3 8ACDHORSZ
P4 28EGKLMNOR
5 lettres
P1 24DEGHOPRST
P2 ADHOST
P3 CDEGHR
P4 8CDTZ
P5 2EKMR
6 lettres
P1 GO
P2 DH
P3 DH
P4 ACT
P5 8C
P6

Dictionnaires (page 226)

Le dictionnaire indique le numéro de page du manuscrit et l'alphabet de substitution rencontré. Si plusieurs numéros de pages identiques se suivent alors plusieurs alphabets de substitutions ont été utilisés pour cette page du manuscrit.

001 NMLRES2TCZAD8HGOPF
002 GOA
002 MR
002 S8DTH
003 DECTHP
003 8O
004 NMRE
004 DTP
005 GOA
005 CTS4
005 DPH
005 KRE
005 82
006 EKRI
006 OAHDTC
007 EM
007 CTD
008 SCT4OAD8
008 MR
009 LN
009 TDSZ
009 MR
009 GO8
010 REH8
011 KMRDH8E
011 OAGP
011 SZT
012 KRG2EOA8CDH
013 RE
013 OG82HDT4CS
014 2LDPH
014 4T
015 SZTERMK
015 P8HD2FGOC
016 8ERMLNDH
016 GOCA
016 TS
017 8ERMH
017 GO
018 FTGP8REMKHD
018 OA
019 ER
019 HD
020 HD
020 RM
021 ST8DHFP42
021 MN
021 EG
022 DH
023 RE
023 CTS8DHPOAG
024 E8R
024 ST
024 OAG
024 DH4
025 DHER8STOC2G4
026 HD
026 ST4
026 GO
027 DH
028 OG
028 EMR
028 H8D
028 T4
029 ZTS4
029 DHP8
030 OGT4Z
030 HD8
031 RKGO
031 PDE
031 84
032 GCTZDERKHO
033 ER
033 TS48
033 ZC
033 GO
034 KGREOTASDH
034 48
035 PDH8ST
035 RE
035 OGA
036 R8MEKG2DHTOA
037 CT4
037 HDP
038 DHP
038 COTSGM
038 ER2
039 TC
040 FEHDT48Z
041 OG8HPAD2
041 TZ
041 REM
042 HD8TGOF
042 KM
043 DFHETSOG
043 RMN
044 ERHD
044 28L
044 TSC
044 4G
045 MREKN
045 DHC8T4OAP
045 2G
046 2EMKRP8CDHTZ
046 OG
047 FO
047 T4S
048 TS8D
048 REM
049 COG
049 8T
050 COTDHPG8
050 E2
051 RMNKEL8H2DGOASPTZC
052 8H
052 TS
053 PHD
053 ER
053 OG
053 T4C
054 TS
055 HDCEST4
055 R8
055 OG
056 GO
056 H8D
056 SZC
057 COTZ
057 GR
058 R8
059 OC8G2
059 ER
059 DH
060 OCZDH8FTSE2RA
061 OGTS
061 HD
061 28
062 OG
062 REL
062 HDP
062 TS
063 DH
063 OG
064 STZ
064 DCH84OAGEKRMN
065 8CTZO
065 HD
065 RE
066 TC8
066 PDHE
066 KRM
066 2G
067 OE82HDMT
068 T2Z4GO
068 HEDC8
069 RELNM
069 HDPS8TZ
069 OG
070 PH
070 AO
071 RKE
071 HDF
071 OAG
071 TS
072 RME
072 OAG
072 ST
073 RGMN
073 HDE8
073 ZA
074 RMEN
074 8THOASD
075 CZ
075 S8P
075 HEFMRK
075 TG
076 RNMEOCGKADH8TS
076 FP
077 DS
077 RE4
077 OGA
077 T8
078 8CTO
078 MNR
078 DFP2H
079 ZCO8G
080 OCGE
081 R8
082 DH
082 4T
082 LM
083 ZCOG
083 HD8
084 COSGDHZT
084 82E
085 TZS4
085 PDHF8
085 OG
086 HE8SZCTRGOADP4M
087 D8HFR
087 E4
087 GO
088 ZCT
088 HD
088 GO
089 DPS
089 48
089 GO
089 RKM
089 CT
090 GOTCDH8E
091 OKME8GRNCZTSDH
092 EA
092 CTR8G2
092 HDO
093 TC8

093 HDS
094 OAZCTG8SFE
094 RN
094 DH
095 TS8ERGOHPD
096 8D
097 CTZ
097 RN
097 OG
098 S4
098 TOC8Z
098 DHRE
099 TZC
099 4P
099 GHD
100 EMK
100 OA
100 CZ
100 H8DP4T
101 OA
101 HDF
102 PHD4
102 REK
102 OZTCS
103 OT8
103 E2
103 HR
104 ZSTH
105 2E
105 OG
105 CHD
105 ST
106 EKMRDH8TZC
106 S4
107 DH
107 EMRK
108 CO
109 TC42DHE
109 GO
110 G2T4C
110 HD
111 OCZ
113 GOA
113 HDER82
117 OGCT284SZ
117 PHDE
118 CTSODH
119 DT
119 KMR
119 O8
121 2GO
125 CP
126 ER
126 AO
128 SH
129 DC
129 GOS
131 ME
131 AOTHDPS
131 CZ8R
134 HDCZTSOG4
134 KERM
147 EHDSC82T4
147 AO
148 HDST8G2CPEO
149 82OGCFTZDHSEP
150 C8SZHDE
150 T4
151 OC
151 HD8
151 ST
152 CO8TSHDR
153 CT8S42EGO
153 DHP
154 FEP
154 DHTS
154 C8
154 OG
155 28CST4PHDFE
156 8CSTDHFP
156 G2O
157 PDH
158 DHTCG8SAO
158 24
159 C82TDHSPE
159 GO
160 DSTZC8PREHMNGOA
161 SDHO8CT
162 DHEP
162 8CST
162 GO
163 REHPD
163 CTS8Z
163 42
164 SC8G
164 HD
164 OEA
165 C8SDEHT2
165 OGA
166 HCD8T4GROS2EF
167 HPFDS8CTOGZE4
168 C8
169 OCT8SHDR
169 PF
169 GE
172 C2OG
172 DH
173 HG8DC
173 MK
173 TS
175 COA
175 D2H
180 PG
180 8DHKE
181 4G
181 ER
181 CZ
182 DH
182 KRE
183 T4SCD8
183 OG
183 MR
184 TCS8DHF
184 EP
185 DH
185 TGKR24
185 CO
186 FHPDCZ8OA4TS
186 ERM
186 2K
187 G8RE2
187 HD
187 4S
188 EMR
188 AO
188 28
188 ST
189 DHTS4
189 GO
189 KE
190 ER
190 GSOT
191 R8E2G
191 DH
191 KM
191 TS
192 MR
192 ZTCO
192 HD
193 CO
194 SC8OGHDLT
194 MR
195 DHF
195 CE
195 MR
195 ST
196 D8H4P
196 OA
196 ER
197 2DH8
197 AOC
197 EMR
198 8CDHOTG
198 ERNM
199 ERM
199 PHTDS
199 ZC
200 AO
200 DH
200 8P
201 OG82ATCDHFP
201 ER
202 4TOCZGA
202 DH
202 REM
203 CZ
203 G2
203 DH
204 2E
204 OC
205 ZCOT4
205 RE
206 8ER
206 OCDHG4TS
207 8E
207 T2CZ
208 TCZDH4
208 GO
209 GO4A
209 E8
209 CZDHTS
210 2E8RGOADCZT4HS
211 DCHZT
211 RE2
211 GO
212 CO8TEGHDPS4A2
213 DHC8GSTEOA
214 DPT8CHS
215 TC8OZGAHDREP
215 S4
216 TC8DHGOESAP
217 8COGTDHZP4
217 EM
218 DH
218 GOA
218 T8C
219 TCS8OZHDFPG
220 C8ZTOGREKMDHSPF
220 42
221 OC8TDLZHGRE4
222 RMKEG8HOTC4AZPDS
223 DHCS8GT2EMROA
224 E8TCOAZG4M2RSDHFP
225 KR
225 ACT8SODHFGE4
226 8CTDH4OAEPSGM
227 O8CDHATEG4P
227 RM
228 8C2OTERGSPFDHA4
229 OCTAE
229 DP
230 8COTDHPF
230 KRM
231 CTO8GDHPA42FREM
232 CT8S4
232 HDPF
233 OCSTR4G82EPDHF
234 DH

234 C8AT
234 OG

Période d'encryptage et langues naturelles (page 173)

La formule de l'indice de coïncidence en fonction de la période d'encryptage et de la *Measure of roughness* permet de déterminer la longueur de la clé d'encryptage en fonction de l'indice de coïncidence attendu ; c'est un retournement d'équation dans lequel nous faisons varier la valeur de l'indice de coïncidence en fonction des langues probablement utilisées.

Détails du retournement

- $$ic = \frac{\frac{1}{d} \times (N - d)}{N - 1} \times h + \frac{(d - 1) \times N}{d \times (N - 1)} \times l$$

$$\Leftrightarrow ic \times d \times (N-1) = (N-d) \times h + (d-1) \times N \times l$$

$$\Leftrightarrow ic \times d \times N - d \times ic = N \times h - d \times h + N \times d \times l - N \times l,$$

$$\Leftrightarrow d \times (ic \times N - ic + h - N \times l) = N \times h - N \times l,$$

$$\Leftrightarrow d = \frac{N(h - l)}{ic \times N - ic + h - N \times l},$$

- $$d = \frac{N(h - l)}{N(ic - l) + h - ic}$$

Périodes probables d'encryptage

danglais=(143476(0.0661−0.0384615)/(143476(0.0842423−0.0384615)+0.0661−0.0842423))=0.603716;

dfrancais=(143476(0.0778−0.0384615)/(143476(0.0842423−0.0384615)+0.0778−0.0842423))=0.859281;

dallemand=(143476(0.0762−0.0384615)/(143476(0.0842423−0.0384615)+0.0762−0.0842423))=0.824332;

ditalien=(143476(0.0738−0.047619)/(143476(0.0842423−0.047619)+0.0738−0.0842423))=0.714875;

dromaji=(143476(0.0819−0.0454545)/(143476(0.0842423−0.0454545)+0.0819−0.0842423))=0.939614;

dportugais=(143476(0.0791−0.0416667)/(143476(0.0842423−0.0416667)+0.0791−0.0842423))=0.879221;

drusse=(143476(0.0529−0.04)/(143476(0.0842423−0.04)+0.0529−0.0842423))=0.291578;

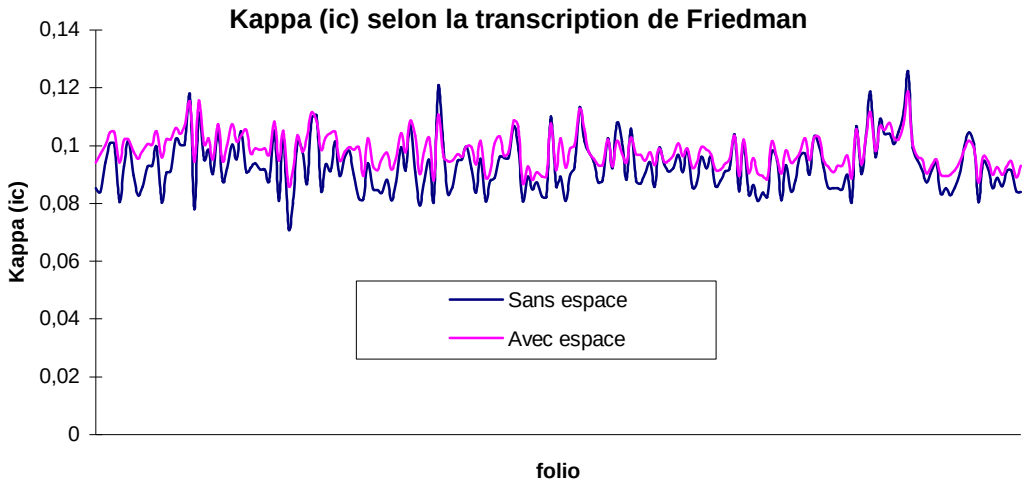
despagnol=(143476(0.0775−0.0357143)/(143476(0.0842423−0.0357143)+0.0775−0.0842423))=0.861065;

Kappa et indice de coïncidences dans le manuscrit

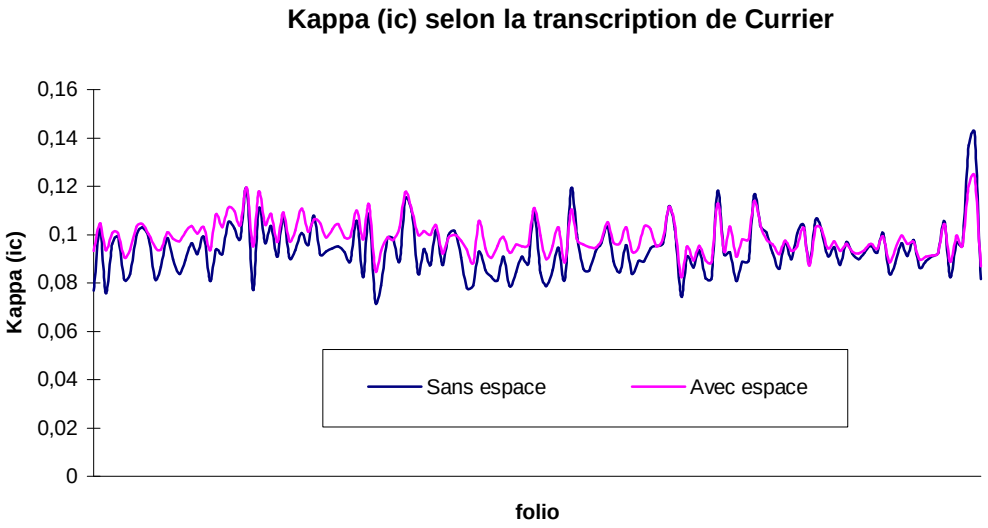
FRIEDMAN

Page	sans espace	avec espace
001	0,076326	0,0905065
002	0,105358	0,110125
003	0,0759241	0,0922555
004	0,101245	0,107757
005	0,101685	0,102718
006	0,0851954	0,0942279
007	0,0839985	0,097034
008	0,094101	0,100039
009	0,100818	0,104578
010	0,100462	0,104576
011	0,0806763	0,0941863
012	0,0929156	0,101974
013	0,101638	0,102102
014	0,089719	0,0979297
015	0,0829194	0,0955308
016	0,0858045	0,0981527
017	0,0927704	0,100465
018	0,0929401	0,100452
019	0,0994644	0,105076
020	0,0804878	0,0959024
021	0,0906014	0,102014
022	0,0911659	0,102104
023	0,102328	0,106059
024	0,100442	0,104015
025	0,100395	0,106962
026	0,117642	0,115263
027	0,0779129	0,0944177
028	0,111179	0,115708
029	0,0952565	0,100266
030	0,0985915	0,102469
031	0,0902177	0,095256
032	0,105453	0,107364
033	0,0877383	0,0946298
034	0,0921309	0,100156
035	0,100345	0,107499
036	0,0951672	0,101513
037	0,104984	0,103552
038	0,0907724	0,105394
039	0,0924548	0,0973377
040	0,094023	0,0989714
041	0,0916209	0,0985917
042	0,091813	0,0991097
043	0,0876523	0,0969087
044	0,10527	0,108262
045	0,0807499	0,0948483
046	0,103643	0,105034
047	0,0716078	0,086065
048	0,0800747	0,0914097
049	0,101271	0,103532
050	0,0981445	0,0979093
051	0,0868903	0,103311
052	0,109313	0,11145
053	0,110415	0,108308
054	0,084431	0,0985696
055	0,0934798	0,102696
056	0,0912739	0,104386
057	0,101541	0,104716
058	0,0895655	0,0948385
059	0,0962368	0,0979434
060	0,0980349	0,0994881
061	0,0900131	0,0985549
062	0,0818505	0,0995541
063	0,081427	0,089415
064	0,0939797	0,102579
065	0,0850496	0,0929764
066	0,084698	0,0914679
067	0,0837695	0,0954418
068	0,0881425	0,097413
069	0,0810159	0,0918106
070	0,0872169	0,0956132
071	0,0993658	0,104305
072	0,091391	0,097645
073	0,10718	0,108625
074	0,0908692	0,103543
075	0,0793661	0,0901573
076	0,0878226	0,0981212
077	0,0951166	0,102561
078	0,0808567	0,0880189
079	0,120764	0,110715
080	0,0993409	0,0960709
081	0,0832683	0,0945539
082	0,0856044	0,0947567
083	0,0945217	0,0970719
084	0,095164	0,0962242
085	0,0997061	0,0997573
086	0,0920142	0,0993828
087	0,0837043	0,0935372
088	0,0955797	0,101735
089	0,0808683	0,0889336
090	0,0878143	0,0909641
091	0,0888274	0,100703
092	0,0962289	0,103313
093	0,0956555	0,0963819
094	0,0958682	0,0979811
095	0,106801	0,108779
096	0,0995409	0,106618
097	0,08096	0,0871413
098	0,0892208	0,092927
099	0,0848796	0,0881084

100	0,0872416	0,0908614
101	0,0823899	0,0892184
102	0,0822819	0,0895154
103	0,110057	0,107737
104	0,0859914	0,0915772
105	0,0893534	0,102578
106	0,0807814	0,0924242
107	0,0898935	0,0990282
108	0,0926377	0,100079
109	0,113258	0,112749
110	0,101626	0,105963
111	0,0978678	0,0978218
113	0,0942794	0,0954872
117	0,0871912	0,0931741
118	0,088166	0,0935366
119	0,102516	0,102041
121	0,0921901	0,0927785
125	0,107903	0,101648
126	0,101483	0,0971891
128	0,0882556	0,0941258
129	0,105926	0,102789
131	0,087697	0,0969371
134	0,0869403	0,0967594
147	0,0904561	0,094795
148	0,0942231	0,0977832
149	0,0858054	0,0933423
150	0,0991553	0,0990701
151	0,0933997	0,0944028
152	0,0909394	0,0948633
153	0,0922425	0,0965579
154	0,0968399	0,100808
155	0,090876	0,0964008
156	0,0987922	0,0990424
157	0,0855014	0,092331
158	0,087341	0,0942345
159	0,0962412	0,0995344
160	0,0920818	0,0986372
161	0,0960453	0,0971184
162	0,0860204	0,0916934
163	0,0879293	0,0917512
164	0,0909452	0,0937735
165	0,0920226	0,0952434
166	0,103957	0,103399
167	0,084231	0,0894341
168	0,101603	0,102065
169	0,0831616	0,0906614
172	0,0864472	0,0956848
173	0,0808105	0,0904138
175	0,0836333	0,0895507
180	0,0821578	0,0883672
181	0,0981812	0,101399
182	0,0954974	0,095727
183	0,080987	0,090355
184	0,0932848	0,0982699
185	0,0841792	0,0941942
186	0,087893	0,0952194
187	0,0963143	0,0977924
188	0,0971597	0,102487
189	0,0900183	0,0950143
190	0,102956	0,10272
191	0,099576	0,102825
192	0,0923438	0,0947792
193	0,0855235	0,0927335
194	0,0851988	0,0907893
195	0,0853434	0,0931128
196	0,0848891	0,0931339
197	0,0900056	0,0964721
198	0,0805958	0,0887905
199	0,10682	0,105664
200	0,0900778	0,0934613
201	0,10282	0,102687
202	0,118808	0,111575
203	0,0960386	0,0981512
204	0,109146	0,1067
205	0,104155	0,105421
206	0,104197	0,107814
207	0,100521	0,102634
208	0,104669	0,10209
209	0,11133	0,107736
210	0,125521	0,118628
211	0,0992553	0,100584
212	0,0949024	0,0961845
213	0,0914501	0,0952864
214	0,0872923	0,0903036
215	0,0914928	0,093368
216	0,0939373	0,0953067
217	0,0832183	0,089896
218	0,0852632	0,0895642
219	0,0829574	0,0900199
220	0,0855031	0,0915659
221	0,090499	0,0944994
222	0,0998741	0,098721
223	0,104562	0,101713
224	0,100607	0,0990377
225	0,0803699	0,0872529
226	0,0943427	0,0961911
227	0,0918762	0,094591
228	0,0852037	0,0899458
229	0,0887664	0,0925152
230	0,0859942	0,0899716
231	0,0911301	0,092922
232	0,0914248	0,0945819
233	0,0842161	0,0891015
234	0,0839992	0,0929814
moyenne	**0,09291978**	**0,09807306**
écart-type	**0,0091**	**0,0062**



CURRIER



Page	sans espace	avec espace
001	0,0767578	0,0932546
002	0,102541	0,104547
003	0,0758654	0,0935321
004	0,0960714	0,100686
005	0,0991251	0,100605
006	0,0812405	0,090689
007	0,083733	0,0938956
008	0,0997401	0,103398
009	0,103132	0,104502
010	0,0984761	0,100198
011	0,0815262	0,0948951
012	0,0867321	0,0938933
013	0,0985457	0,10089
014	0,089893	0,0983542
015	0,0835906	0,0971366
016	0,0893979	0,100884
017	0,0964571	0,103593
018	0,091842	0,100288
019	0,0990322	0,103085
020	0,0809182	0,0934722
021	0,0936823	0,1084
022	0,091954	0,103139
023	0,104881	0,110938
024	0,10251	0,109663
025	0,0982555	0,103896
026	0,119174	0,119596
027	0,0771327	0,0951163
028	0,111071	0,117754
029	0,0964401	0,104144
030	0,103557	0,108571
031	0,0909449	0,0968524
032	0,10755	0,109117
033	0,0904441	0,0973355
034	0,0935455	0,101686

035	0,10067	0,110749
036	0,0955709	0,101229
037	0,10789	0,106146
038	0,0915254	0,104517
039	0,0930326	0,098792
040	0,0943708	0,102209
041	0,0951541	0,104295
042	0,0926477	0,0988208
043	0,0889017	0,0991058
044	0,105779	0,110043
045	0,082454	0,097899
046	0,108614	0,11251
047	0,0723292	0,0853228
048	0,0789406	0,0932061
049	0,0985383	0,098905
050	0,0983206	0,0977956
051	0,0889081	0,102933
052	0,114854	0,117643
053	0,109516	0,110229
054	0,0836278	0,0998133
055	0,0941669	0,101359
056	0,0875401	0,0999201
057	0,102032	0,103774
058	0,0875018	0,0921934
059	0,0996079	0,0985468
060	0,101384	0,0997579
061	0,0905558	0,0976145
062	0,0778138	0,0937322
063	0,0788388	0,0883092
064	0,0930377	0,105823
065	0,0854108	0,0944247
066	0,0826237	0,0904219
067	0,0810978	0,0952483
068	0,0907882	0,0989599
069	0,0786406	0,0924517
070	0,0844451	0,0958821
071	0,0907803	0,0952164
072	0,0878339	0,0955326
073	0,109446	0,111038
074	0,0843445	0,099488
075	0,0786859	0,0899322
076	0,0853583	0,0954022
077	0,0946265	0,103155
078	0,0813346	0,0885372
079	0,119207	0,110177
080	0,100045	0,0981419
081	0,0857315	0,0959515
082	0,0849391	0,0948345
083	0,0930027	0,0945197
084	0,0964995	0,0974505
085	0,103267	0,105277
086	0,0889778	0,0965703
087	0,0846103	0,0963405
088	0,0955215	0,103033
089	0,0837438	0,0929607
090	0,0889466	0,0944372
091	0,0889356	0,103325
092	0,0944222	0,10232
093	0,0952495	0,0951147
094	0,0961969	0,0979169
095	0,111731	0,111506
096	0,102119	0,103776
097	0,0745163	0,082406
098	0,0907816	0,0950127
099	0,0864622	0,0892
100	0,0935898	0,0954168
101	0,0817496	0,0891716
102	0,0816548	0,0884925
103	0,118034	0,112925
104	0,0917835	0,0930723
105	0,0926752	0,103415
106	0,0807608	0,0907499
107	0,0888016	0,098047
108	0,089006	0,0979831
109	0,116441	0,113987
110	0,103218	0,10348
111	0,100846	0,0979475
116	0,0922175	0,0957979
117	0,0859596	0,0918927
119	0,0968883	0,097466
122	0,0897922	0,0931461
125	0,10052	0,0951069
128	0,103809	0,102755
129	0,0879246	0,0872206
135	0,106328	0,103021
138	0,101802	0,102393
147	0,0910677	0,0943499
148	0,0948166	0,0971258
149	0,0873042	0,0932146
150	0,0970116	0,0961478
151	0,0922798	0,0929119
152	0,0898697	0,0920558
153	0,0925625	0,0934207
154	0,0952583	0,0961656
155	0,0925291	0,093984
156	0,100615	0,0994154
157	0,0840867	0,0884394
158	0,0878926	0,0938928
159	0,0965554	0,0996283
160	0,091181	0,0961456
161	0,0976234	0,0969317
162	0,0864621	0,0899155
163	0,0889573	0,0909665
164	0,0912286	0,0913017
165	0,0921279	0,0922862
166	0,105483	0,104252
173	0,0824057	0,0887198
191	0,096988	0,0996005
203	0,0953394	0,0953442
204	0,136905	0,120397
207	0,142235	0,124504
219	0,0816857	0,0868708

moyenne	0,0937293	0,09903175
écart-type	0,0109	0,0074

Symétries et redondances (page 258)

Le tableau que nous présentons résume les statistiques de présences des motifs symétrique et redondants en fonction des textes références et des deux textes MS408 des versions CURRIER et FRIEDMAN. La dernière colonne est consacrée à l'énumération des diversités rencontrées dans chacun des textes.

Le premier tableau est dédié aux textes avec voyelles et espaces ; le deuxième tableau est consacré aux textes sans voyelles et avec espaces.

Symétries et redondances avec voyelles et avec espaces (page 258)

Texte	symétrie	redondance	$\frac{Qs}{Qr}$	$\frac{Qs}{Nlettre}$	$\frac{Qr}{Nlettre}$	$\frac{(Qs+Qr)}{Nlettre}$	Nlettre	diversité
MISERAB	298651	21966	13.596058	0.113679	0.008361	0.122041	2627133	1425
W92	237422	8298	28.611955	0.126410	0.004418	0.130828	1878194	1638
W90	196374	7940	24.732242	0.123018	0.004974	0.127992	1596297	1608
BEAGLE	90499	3106	29.136832	0.115100	0.003950	0.119050	786267	740
DRACU10	74462	5923	12.571670	0.111612	0.008878	0.120490	667152	785
HISTOI	55443	3337	16.614624	0.095228	0.005732	0.100959	582214	556
LORDJIM	66386	6837	9.709814	0.114587	0.011801	0.126388	579350	825
TWOCITY	55057	5028	10.950080	0.106874	0.009760	0.116634	515159	685
DARWIN	52610	2234	23.549687	0.113740	0.004830	0.118570	462546	477
ADVENTUR	53953	2993	18.026395	0.118542	0.006576	0.125118	455140	590
TARZAN	39794	2225	17.884944	0.101812	0.005693	0.107505	390857	547
PARLOST	34720	1574	22.058450	0.091719	0.004158	0.095877	378546	451
GODSMARS	42107	2286	18.419510	0.115139	0.006251	0.121390	365707	503
CASEBOOK	42393	3016	14.056034	0.116945	0.008320	0.125265	362504	537
DGRAY10	37415	3036	12.323781	0.107353	0.008711	0.116064	348524	527
FRANK10	41715	1508	27.662467	0.121597	0.004396	0.125993	343059	480
LOSTWO	38715	1752	22.097603	0.112881	0.005108	0.117990	342971	533
JUNGLE	34598	1836	18.844227	0.102169	0.005422	0.107591	338634	476
RHETO	33693	2208	15.259511	0.107971	0.007076	0.115047	312055	468
OPAR	31837	1228	25.925896	0.104698	0.004038	0.108737	304083	455
EIGHTY	31154	1761	17.691085	0.103488	0.005850	0.109338	301040	496
WARWORLD	32460	1650	19.672727	0.117419	0.005969	0.123388	276446	474
LASTBOW	29674	2052	14.461014	0.112550	0.007783	0.120333	263651	475
HOUND	29371	1718	17.096042	0.114167	0.006678	0.120845	257264	451
ROUND	26557	1221	21.750205	0.105724	0.004861	0.110585	251192	463
SUNZU10	29044	1490	19.492617	0.115840	0.005943	0.121782	250726	491
LIBERTY	27691	1146	24.163176	0.118292	0.004896	0.123188	234090	359
INVISM	24447	1717	14.238206	0.110049	0.007729	0.117778	222147	459
WOMEN	24200	1198	20.200334	0.112783	0.005583	0.118366	214571	382
MOON	22013	730	30.154795	0.110308	0.003658	0.113966	199560	444
STUDY	22753	1344	16.929315	0.116918	0.006906	0.123824	194607	455
OZLAND	19655	1053	18.665717	0.101184	0.005421	0.106605	194250	403
SIGNFOUR	22591	1198	18.857262	0.120506	0.006390	0.126896	187468	441
FABLES	19321	1148	16.830139	0.107920	0.006412	0.114332	179031	418
DARKNESS	20607	2142	9.620448	0.119239	0.012394	0.131633	172821	461
WIZOZ	18520	826	22.421308	0.111242	0.004961	0.116203	166484	325
TIMEMACH	18947	692	27.380058	0.129517	0.004730	0.134247	146290	380
VMS408F	11116	9995	1.112156	0.077475	0.069662	0.147137	143479	709
CRICKET	14877	1560	9.536538	0.103932	0.010898	0.114830	143142	407
CALLWILD	14293	758	18.856201	0.099936	0.005300	0.105236	143022	353
CHIMES	13590	2865	4.743455	0.099212	0.020915	0.120127	136980	464
LOOKING	14006	1370	10.223358	0.108282	0.010592	0.118874	129347	372
CAROL	13726	1057	12.985809	0.107761	0.008298	0.116060	127374	361
ATHENE	13263	644	20.594720	0.113778	0.005525	0.119303	116569	288
ALICE	12071	1496	8.068850	0.104063	0.012897	0.116960	115997	339
HYDEA10	12984	676	19.207101	0.115265	0.006001	0.121266	112645	326
CANDIDE	15636	874	17.890160	0.145732	0.008146	0.153878	107293	290
GUERILLA	9518	276	34.485507	0.117702	0.003413	0.121115	80865	245
VMS408C	6676	5517	1.210078	0.086785	0.071718	0.158503	76926	497
PARGAIN	6973	354	19.697740	0.094452	0.004795	0.099247	73826	268
SHARER	8889	462	19.240260	0.123388	0.006413	0.129801	72041	296
ATLANTIS	6572	216	30.425926	0.095862	0.003151	0.099013	68557	218
OEDIPU2	6953	556	12.505396	0.109360	0.008745	0.118105	63579	277
OEDIPU1	6263	420	14.911905	0.110049	0.007380	0.117429	56911	262
ANTIGONE	5047	420	12.016667	0.109143	0.009083	0.118226	46242	251
MANUEL	4335	202	21.460396	0.134331	0.006259	0.140591	32271	168

MICROMEG	4140	308	13.441558	0.130250	0.009690	0.139940	31785	178
PIT	3459	120	28.825000	0.123044	0.004269	0.127312	28112	189
ILIAD01	2642	100	26.420000	0.106696	0.004038	0.110734	24762	130
SNARK	2431	220	11.050000	0.107329	0.009713	0.117042	22650	153
ODYS1	1815	110	16.500000	0.105450	0.006391	0.111841	17212	124
PD_2	2266	98	23.122449	0.131805	0.005700	0.137506	17192	145
CRITON3	1651	106	15.575472	0.142956	0.009178	0.152134	11549	115
CRITON2	1295	94	13.776596	0.140853	0.010224	0.151077	9194	101
CRITON1	752	82	9.170732	0.115302	0.012573	0.127875	6522	93
JABBER	82	48	1.708333	0.104459	0.061146	0.165605	785	16

Tableau 13 Statistique des symétries et redondances, diversité.

Symétries et redondances sans voyelles avec espaces (page 258)

Nom Texte	Qsymétrie	Qredondance	Qs/Qr	Qs/size(txt)	Qr/size(txt)	(Qs+Qr)/size(txt)	size(txt)	diversité
vms408c	6676	5517	1,210078	0,086785	0,071718	0,158503	76926	497
vms408f	11116	9995	1,112156	0,077475	0,069662	0,147137	143479	709
ADVENTUR	95577	2924	32,687073	0,209995	0,006424	0,216419	455140	1014
ALICE	23431	1407	16,653163	0,201997	0,01213	0,214126	115997	514
ANTIGONE	8524	444	19,198198	0,184335	0,009602	0,193936	46242	346
ATHENE	22756	1028	22,136187	0,195215	0,008819	0,204034	116569	436
ATLANTIS	14808	436	33,963303	0,215995	0,00636	0,222355	68557	364
BEAGLE	148230	4501	32,932682	0,188524	0,005725	0,194248	786267	1201
CALLWILD	25611	1260	20,32619	0,17907	0,00881	0,18788	143022	540
CANDIDE	24188	526	45,984791	0,225439	0,004902	0,230341	107293	444
CAROL	23897	1109	21,548242	0,187613	0,008707	0,19632	127374	594
CASEBOOK	74384	2542	29,261998	0,205195	0,007012	0,212207	362504	945
CHIMES	26179	2399	10,912464	0,191115	0,017514	0,208629	136980	666
CRICKET	26667	1379	19,337926	0,186298	0,009634	0,195931	143142	612
CRITON1	1419	58	24,465517	0,217571	0,008893	0,226464	6522	111
CRITON2	1906	76	25,078947	0,207309	0,008266	0,215575	9194	137
CRITON3	2656	129	20,589147	0,229977	0,01117	0,241146	11549	155
DARKNESS	32883	1799	18,278488	0,190272	0,01041	0,200682	172821	702
DARWIN	91299	2502	36,490408	0,197384	0,005409	0,202793	462546	816
DGRAY10	68011	2416	28,150248	0,19514	0,006932	0,202072	348524	884
DRACU10	141401	5827	24,266518	0,211947	0,008734	0,220681	667152	1313
EIGHTY	54564	1969	27,711529	0,181252	0,006541	0,187792	301040	781
FABLES	34576	1310	26,393893	0,193129	0,007317	0,200446	179031	638
FRANK10	67227	2021	33,264226	0,195963	0,005891	0,201854	343059	784
GODSMARS	69506	3147	22,086432	0,190059	0,008605	0,198665	365707	857
GUERILLA	16041	554	28,954874	0,198368	0,006851	0,205219	80865	350
HISTOI	119300	5618	21,235315	0,204907	0,009649	0,214557	582214	983
HOUND	53621	1690	31,728402	0,208428	0,006569	0,214997	257264	787
HYDEA10	22387	780	28,701282	0,198739	0,006924	0,205664	112645	501
ILIAD01	4698	218	21,550459	0,189726	0,008804	0,19853	24762	207
INVISM	38894	2280	17,058772	0,175082	0,010263	0,185346	222147	724
JABBER	188	36	5,222222	0,23949	0,04586	0,28535	785	27
JUNGLE	60514	2828	21,398161	0,1787	0,008351	0,187052	338634	756
LASTBOW	53748	1945	27,633933	0,20386	0,007377	0,211238	263651	776
LIBERTY	51471	928	55,46444	0,219877	0,003964	0,223841	234090	614
LOOKING	26142	1143	22,871391	0,202108	0,008837	0,210944	129347	556
LORDJIM	113787	5593	20,344538	0,196405	0,009654	0,206059	579350	1288
LOSTWO	66938	2032	32,941929	0,195171	0,005925	0,201096	342971	845
MANUEL	8685	132	65,795455	0,269127	0,00409	0,273217	32271	247
MICROMEG	7315	212	34,504717	0,23014	0,00667	0,23681	31785	239
MISERAB	509358	21857	23,304113	0,193884	0,00832	0,202203	2627133	2507
MOON	37037	840	44,091667	0,185593	0,004209	0,189803	199560	656
ODYS1	3495	82	42,621951	0,203056	0,004764	0,20782	17212	178

OEDIPU1	10128	485	20,882474	0,177962	0,008522	0,186484	56911	389
OEDIPU2	11773	659	17,864947	0,185171	0,010365	0,195536	63579	414
OPAR	54062	2223	24,319388	0,177787	0,007311	0,185097	304083	739
OZLAND	35117	1377	25,502542	0,180782	0,007089	0,187871	194250	619
PARGAIN	12678	638	19,871473	0,171728	0,008642	0,18037	73826	396

Texte	symétrie	redondance	$\frac{Qs}{Qr}$	$\frac{Qs}{Nlettre}$	$\frac{Qr}{Nlettre}$	$\frac{(Qs+Qr)}{Nlettre}$	Nlettre	diversité
ANONEV	6068	240	25.283333	0.165539	0.006547	0.172086	36656	232
APOLOG	22466	562	39.975089	0.170334	0.004261	0.174595	131894	381
AROATH	1051	26	40.423077	0.156819	0.003879	0.160698	6702	115
DANTE1	390	20	19.500000	0.130174	0.006676	0.136849	2996	61
DANTE13	3512	236	14.881356	0.163562	0.010991	0.174553	21472	182
DANTE2	5107	204	25.034314	0.150179	0.005999	0.156178	34006	219
DANTER	4977	264	18.852273	0.137482	0.007293	0.144775	36201	232
EIN	7813	174	44.902299	0.164401	0.003661	0.168062	47524	268
GAUD	104	162	0.641975	0.152717	0.237885	0.390602	681	24
SEPTSAP	7115	158	45.031646	0.171091	0.003799	0.174891	41586	222
STONE	1428	48	29.750000	0.131226	0.004411	0.135637	10882	133

Motifs les plus longs de MS408

Version FRIEDMAN		Version CURRIER	
Motifs	Taille	Motifs	Taille
#2#(#2#(C8G_4OD))	28	#2#(_8AM_O8AIK_4ODAM_GHCAE_ODAE_OK)	60
#2#(G_8AIRG_SCO2_P)	28	#2#(#2#(C8G_4OD))	28
#3#(CO8G_4OD)	24	#2#(ODC8AE_SC8G_)	24
#3#(C8G_4ODC)	24	#2#(ODAE_ODC8G_4)	24
#3#(C8G_4ODC)	24	#3#(CO8G_4OD)	24
#3#(_4OD#2#C8G)	24	#3#(C8G_4ODC)	24
#2#(C8G_4ODAM_S)	22	#3#(G_4ODC8)	21
#2#(E_SC8G_4ODA)	22	#2#(TODZG_8AM_)	20
#3#(G_4ODC8)	21	#2#(_TCOR_TCG)	18
#3#(C8G_4OD)	21	#2#(OE_TC8G_4)	18
#3#(OD#2#C8G_)	21	#3#(DAN_OE)	18
#2#(G_4ODAM_SC)	20	#2#(C8G_4ODC)	16
#2#(CG_SCG_4OD)	20	#2#(D#2#C8G_TC)	16
#2#(_TCOR_TCG)	18	#2#(#2#CO8_4OH)	16
#2#(OE_TC8G_4)	18	#2#(D#2#C8G_4O)	16
#2#(TC8G_4OE_)	18	#2#(C8G_4ODC)	16
#3#(DAM_OE)	18	#2#(#2#C8G_4OD)	16

Transitions d'états digrammiques avec espace de MS408

	_	2	3	4	6	7	8	9	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	V	W	X	Y	Z
_		338	0,208	1535	1,192	0,208	974,9	0,208	457,9	29,81	432	378,9	43,52	456,7	445,4	4,174		11,03	1,49	8,944	0,894	2004	201,5	146,3	900,3	1623				2,087	
2	4045	9,496			4,748		75,97		2706	180,4	66,47	28,49	9,496	474,8	18,99			9,496		4,748	4,748	1571	18,99	137,7	151,9	384,6					4,748
3					3333					3333				3333																	
4	9,62	3,848					1,924		11,54	75,04	76,96	3,848		15,39	34,63				1,924			9742	11,54	1,924		9,62					
6								2000				5000			3000																
7	3333													3333											3333						
8	491,6	12,96				0,864	19,87		3126	85,53	23,32	63,93		5401	7,776	2,592		9,504		2,592	0,864	340,4	6,048	10,36	133	260					
9	5000						1666		1666					1666																	
A	133,1	30,37		2,336			62,31	0,778	7,009	10,9	52,96	2064	6,231	20,25	26,48	594,2		534,3	67,76	3764	363,7	45,17	10,9	2219	4,673	5,452	1,557	0,778		0,778	
C	54,38	170		0,578	1,157	0,578	2707	0,578	2609	2498	291	5,206	19,09	2091	130,1	4,049	0,578	9,256	8,678	5,785	0,578	1567	42,23	14,46	26,03	88,51					1,735
D	65,01	4,127					10,31		2874	350	1,031	34,05	2,063	681,1	31,99	6,191				4,127		589,2		3,095	208,4	1021					962,8
E	5887	134,7		3,285			411,7		353,7	50,37	988,9	40,52	31,75	400,8	99,66	2,19		10,95		1,095		530	42,71	35,04	266,1	706,2				3,285	
F	559,6	24,33	24,33				145,9		1386	72,99	48,66	24,33		608,2				24,33			24,33	1094			340,6	379,5					1824
G	879,5	20,49		7,044			105		14,73	6,404	365,6	30,74	9,006	1,921	311,2			4,483		0,64	0,64	36,5	45,47	10,88	68,52	164,5					
H	85,49	5,029	1,676	1,676	3,352		28,49		2425	2328	18,44	18,44	1,676	709,1	1,676	1,676				1,676		940,4	3,352	1,676	276,6	1538			1,676		1604
I	78,43	166,6					98,03		9,803	49,01	88,23	274,5		39,21	39,21	1568		568,6	88,23	627,4	137,2	29,41	19,6	6019	39,21	49,01				9,803	
J																								10000							
K	9641						89,55		69,65	9,95				19,9				29,85		9,95		69,65	9,95	19,9	9,95	19,9					
L	9083								76,33		76,33	76,33		152,6		76,33				76,33	76,33			76,33		229					
M	9446	5,844					21,43		15,58	1,948	1,948	7,792		37,01		9,74		9,74	1,948		413	15,58		7,792		3,896					
N	8673	83,79					167,5		13,96	13,96	83,79	83,79		55,86	27,93			41,89	13,96	377		97,76		237,4		27,93					
O	481,2	149,7		12,2			860,6	0,469	155,4	135,6	259,3	229,8	65,26	56,81	153,9	19,71		73,71	5,164	66,66	3,286	31,45	244,6	1108	27,23	69,01				1,878	0,469
P	236,9	13,54					189,5		1056	33,85	6,77		60,93	406,2	6,77	6,77						1387			460,3	4637					1496
R	7536	27,75					61,67		1117	24,66	10,79	24,66	3,083	379,2	3,083	16,95		6,167	1,541	16,95	10,79	494,9	3,083	4,625	67,83	183,4				4,625	
S	76,31	40,54					410,2		355,3	57,14	352,9	23,84	7,154	646,3	164,5					2,384		2134	14,3	7,154	7,154	40,54				2,384	
T	269,9	66,25		1,013			738,8		468,7	457,2	404,5	54,2	20,07	925,5	209,7	3,011		5,019		2,007		2394	53,2	20,07	20,07	11,04				2,007	2,007
V												10000																			
W	10000																														
X														10000																	
Y	3636								1818			454,5		1363								2727									
Z	91,19	41,03					360,2		652	2585	9,119	18,23	4,559	4313	13,67	4,559						1814		4,559	27,35	59,27					

Tableau 14 Transitions digrammiques Markoviennes avec espace de MS408.

Transitions digrammiques sans espace de MS408

	2	3	4	6	7	8	9	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	V	W	X
2	128,2		251,6	4,748		275,4		3566	199,4	170,9	104,4	23,74	759,7	132,9			14,24	4,748	4,748	9,496	2492	104,4	156,6	546	1044			
3				3333					3333				3333															
4	3,848		1,924	3,848		3,848		11,54	75,04	76,96	3,848		15,39	34,63				1,924			9744	11,54	1,924		9,62			
6							2000				5000			3000														
7								3333					3333											3333				
8	28,51		102,8		0,864	58,75		3163	87,26	35,42	94,17	3,456	5440	17,28	4,32		12,96	0,864	3,456	0,864	431,1	10,36	14,68	171,9	316,2			
9	1666			1666		1666		3333					1666															
A	35,04		10,12			75,55	0,778	9,346	10,9	61,53	2046	6,231	25,7	29,59	597,3		542	67,76	3784	365,2	60,75	12,46	2233	8,567	13,24	1,557	0,778	
C	171,8		4,628	1,157	0,578	2715	0,578	264,9	2498	300,2	6,363	20,82	2094	133,6	4,628	0,578	10,41	8,678	5,785	0,578	1577	42,81	15,04	28,34	90,25			
D	5,159		4,127			12,38		2879	3502	1,031	35,08	2,063	683,1	33,02	6,191		1,031		4,127		602,6		4,127	218,7	1042			
E	350,4	1,095	504,8	1,095		1157	1,095	508,1	72,28	1470	252,9	59,13	590,2	338,4	2,19		14,23	1,095	1,095		1540	123,7	108,4	983,4	1912			
F	24,33	24,33	72,99			218,9		1411	72,99	97,32	24,33	24,33	656,9	24,33			24,33			24,33	1119	24,33		437,9	3892			
G	345,8		2295			1019		96,71	22,41	757,7	530,9	41,63	346,5	767,3	0,64		5,764	0,64	1,28	0,64	1576	260	181,2	561,7	1185			
H	8,382	1,676	8,382	3,352		33,52		2432	2328	20,11	18,44	1,676	714,1	1,676	1,676				1,676		955,5	3,352	1,676	298,4	1559			1,676
I	166,6		9,803			98,03		19,6	49,01	117,6	274,5		49,01	39,21	1568		568,6	88,23	627,4	137,2	39,21	19,6	6019	39,21	58,82			
J																							10000					
K	1014		885,5			1442		228,8	29,85	169,1	129,3	59,7	1363	766,1			29,85		9,95		1771	368,1	69,65	646,7	1004			
L	839,6		992,3			992,3		458		381,6	76,33		1068	305,3	76,33				76,33	76,33	1908	152,6	152,6	687	1755			
M	220,1		783,1			769,5		389,6	27,27	169,4	83,77	31,17	535,7	364,3	11,68		15,58	1,948	1,948	413	2637	187	31,17	1211	2111			
N	237,4		628,4			879,8		544,6	13,96	195,5	195,5	27,93	446,9	418,9			41,89	13,96	377		2053	237,4	293,2	935,7	2458			
O	167,6		49,29		0,469	941,8	0,469	171,3	136,1	2648	2350	69,95	69,01	1579	20,65		76,05	5,634	67,13	3,286	72,77	253	1146	49,76	118,3			
P	20,31					209,8		1076	33,85	6,77		67,7	412,9	27,08	6,77						1435			473,9	4732			
R	171,1		434,7			473,3		2269	69,38	154,1	109,4	40,08	732,3	205	21,58		12,33	1,541	16,95	10,79	2394	111	40,08	1014	1709			
S	45,31		11,92			417,3		355,3	5716	355,3	23,84	7,154	646,3	166,9					2,384		2163	16,69	7,154	9,539	52,46			
T	67,25		2,007			742,8		468,7	4572	406,5	55,2	20,07	928,5	210,8	3,011		7,026		2,007		2401	53,2	20,07	22,08	13,04			
V											10000																	
W																					10000							
X													10000															
Y	454,5		454,5					3636			454,5		1818								2727			454,5				
Z	54,71		4,559			360,2		652	2585	9,119	18,23	9,119	4331	13,67	4,559						1842		9,119	31,91	72,95			

Tableau 15 Transition markovienne des lettres du manuscrit de Voynich sans espace.

Indépendances digrammiques de MS408

	2	3	4	6	7	8	9	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	V	Y
2	1,045		1,951			1,672		25,02	1,603	0,975	0,766	0,069	5,436	1,184			0,139		0,069	0,069	19,3	0,418	0,696	4,181	7,597		
3									0,069																		
4	0,139			0,139		0,069		0,278	1,324	1,324	0,069		0,209	0,487							178,7	0,278	0,069		0,209		
6							0,069				0,278			0,069													
7													0,069											0,069			
8	1,115		4,251		0,069	2,369		129,6	3,694	1,184	3,275	0,278	218,2	0,418	0,278		0,557	0,069	0,139	0,069	17,56	0,418	0,627	7,388	13,03		
9	0,069							0,069																			
A	1,742		0,348			3,275		0,278	0,418	2,369	89,28	0,348	1,045	1,463	27,53		23,83	2,997	172	17,21	2,369	0,627	100,3	0,418	0,418	0,069	0,069
C	10,31		0,418	0,069		164,2	0,069	16,72	147,6	19,58	0,418	0,836	126,7	8,781	0,348	0,069	0,627	0,487	0,278		93,81	2,787	1,115	1,672	5,366		
D	0,069		0,139			0,627		96,74	118,7	0,069	1,254	0,069	23,27	1,393	0,348				0,069		20,21		0,139	6,969	36,87		
E	11,01		16,93			37,42	0,069	15,54	2,09	47,32	8,363	1,672	19,44	10,45	0,069		0,418		0,069		50,11	3,624	4,042	30,73	59,52		0,209
F		0,069	0,069			0,278		2,021		0,209			1,254				0,069				1,603	0,069		0,766	4,809		
G	19,23		122,9			54,64		5,227	1,324	40,63	28,43	2,857	19,23	42,3			0,209		0,069	0,069	85,93	13,8	9,827	31,08	66,14		0,069
H	0,139	0,069	0,209	0,069		0,766		49,62	47,81	0,348	0,278		13,1						0,069		19,58	0,069		6,551	32,61		
I	0,487		0,069			0,278		0,069	0,209	0,418	0,766		0,139	0,139	5,575		1,881	0,348	2,3	0,487	0,139		20,97	0,139	0,348		0,069
K	3,903		2,927			5,227		0,696	0,139	0,487	0,487	0,348	4,46	3,136					0,069		6,272	1,184	0,348	2,021	3,206		0,069
L	0,348		0,487			0,487		0,139		0,278	0,069		0,627	0,209	0,069						0,766	0,139	0,069	0,418	0,696		
M	3,624		13,59			13,93		6,969	0,557	3,275	1,672	0,766	9,548	7,666	0,139		0,278	0,069		7,388	45,09	3,275	0,487	21,95	36,73		
N	0,487		1,324			1,951		1,324		0,557	0,627	0,069	1,184	1,045			0,069		0,766		5,227	0,696	0,557	2,369	5,924		
O	12,96		4,112			69,21	0,069	11,63	10,24	193,9	176,3	5,087	5,506	119,8	1,324		6,551	0,348	4,39	0,209	5,297	18,6	83,08	3,763	9,548		0,069
P	0,069					1,045		6,063	0,278	0,069		0,278	2,23	0,209							7,248			2,23	25,23		
R	3,833		8,851			10,87		51,71	1,533	3,554	2,369	0,836	17,49	4,809	0,418		0,139		0,209	0,209	55,47	2,369	0,975	20,83	41,05		0,139
S	0,906		0,139			5,924		5,366	86,21	3,833	0,278		9,688	2,648					0,069		31,01	0,348	0,069	0,139	0,696		0,069
T	2,578		0,069			25,3		15,12	157,5	13,8	1,951	0,906	32,2	7,178	0,069		0,278		0,069		82,24	2,021	0,766	0,766	0,348		0,069
V											0,069																
W																					0,069						
X													0,069														
Y			0,069					0,278			0,069		0,069								0,139			0,069			
Z	0,418					2,369		5,715	20,7		0,139	0,139	32,82	0,139	0,069						14,07		0,139	0,278	0,557		

Tableau 16 Probabilités indépendantes digrammiques du manuscrit de Voynich.

Alphabet par folio (page 181)

A chaque ligne correspond une page du manuscrit. La deuxième colonne contient le caractère le plus représenté dans la page concernée ; le caractère '_' correspond au caractère « espace ». La troisième colonne contient la deuxième lettre la plus rencontrée dans cette page ; puis la dernière colonne de droite contient la lettre la moins fréquente. A coté de chacune des lettres suit la fréquence —séparée par deux points « : ». Si les points ne sont pas présents à droite du premier symbole alors cela signifie que la fréquence est inférieure à 1%.

1	**«_»:22**	**O:11**	A:8	G:8	8:6	C:5	R:4	D:4	T:4	S:4	Z:3	H:3	E:3	M:2	2:1	N:1	P:1	I:1	F	L	K	
2	**«_»:22**	**O:17**	G:8	E:8	T:7	8:7	A:5	D:4	R:3	H:3	C:3	Z:2	S:2	P	M	I	2	K	F	4		
3	**«_»:23**	**G:10**	O:9	A:8	8:6	T:5	E:5	D:4	M:3	S:3	C:3	R:2	H:2	2:2	Z:2	L:1	I:1	N:1	4	P	F	
4	**«_»:22**	**O:16**	T:12	C:5	G:5	8:5	R:4	A:4	E:4	M:3	H:3	S:2	D:2	2:1	I:1	4:1	Z	N	P	L		
5	**«_»:21**	**O:19**	T:7	C:5	E:5	A:5	K:4	R:4	G:4	H:3	8:3	4:3	D:2	S:2	2:2	M:1	Z:1	P:1	I	F		
6	**«_»:22**	**O:14**	A:7	T:7	C:7	D:5	R:5	G:5	E:4	H:3	8:3	K:2	Z:2	S:2	I:1	2:1	M:1	4:1	P	N	L	F
7	**«_»:24**	**O:12**	G:8	T:8	H:6	A:6	M:6	E:4	8:4	S:3	Z:2	R:2	C:2	4:2	P:1	D:1	K	2	N			
8	**«_»:22**	**O:16**	G:8	T:7	C:5	S:5	8:5	H:4	A:4	D:3	R:3	M:3	E:2	Z:2	4:1	P	2	N	K	I	L	
9	**«_»:21**	**O:16**	G:11	C:8	T:6	H:5	S:4	8:4	A:3	D:3	4:3	M:2	Z:1	R:1	E:1	L:1	2:1	P	N			
10	**«_»:22**	**O:18**	T:8	8:7	H:6	A:5	R:5	M:5	E:4	G:3	C:2	S:2	D:1	4:1	2:1	Z	P	I	F	N	K	
11	**«_»:23**	**O:13**	A:8	T:6	R:6	G:4	H:4	Z:3	M:3	D:3	8:3	E:3	C:3	S:2	K:1	2:1	I:1	P	4	F		
12	**«_»:23**	**O:14**	T:9	G:8	R:5	A:5	8:4	H:4	D:4	Z:3	C:3	E:3	2:3	K:1	4:1	M:1	S	N	P	I		
13	**«_»:20**	**O:14**	T:12	C:9	G:9	8:5	D:4	E:3	A:3	H:3	S:2	M:2	4:2	2:2	R:1	Z:1	N:1	P	F			
14	**«_»:21**	**O:13**	C:8	8:8	G:8	T:7	S:4	H:3	A:3	E:3	D:3	R:2	M:2	4:1	Z:1	P	I	2	L	N		
15	**«_»:22**	**O:12**	T:9	G:7	C:6	A:6	8:6	E:4	D:3	S:3	R:3	H:3	M:2	Z:1	2:1	P:1	K	I	F	N	L	4
16	**«_»:23**	**O:11**	T:9	A:9	R:6	E:5	G:5	C:4	H:4	8:3	M:3	D:3	S:2	Z:2	2:1	N:1	P	L	K	4		
17	**«_»:21**	**O:15**	G:9	T:6	H:6	A:6	R:5	8:5	M:3	E:3	D:3	Z:3	S:2	C:1	2:1	4	P	N	I	K	F	
18	**«_»:22**	**O:15**	G:10	T:6	8:5	H:5	A:5	M:4	R:4	E:4	D:3	Z:2	C:2	P:1	4:1	S	F	I	2	K		
19	**«_»:22**	**O:15**	T:8	G:8	H:8	R:6	A:5	8:4	Z:3	M:3	E:2	4:2	D:1	I:1	S	P	C	2	N	K	F	
20	**«_»:23**	**O:12**	G:8	H:6	T:6	A:5	M:5	8:5	4:4	D:3	C:3	Z:2	S:2	R:2	E:2	N:1	P	L	2			
21	**«_»:23**	**G:13**	O:10	8:9	T:7	H:5	A:5	M:3	E:3	Z:3	S:3	D:3	R:2	2:1	4:1	P	F	C	N	I		
22	**«_»:23**	**G:12**	O:12	8:9	T:7	R:4	H:4	D:3	Z:3	S:3	E:3	A:3	4:2	C:2	P:1	L	K	2	N	M		
23	**«_»:22**	**O:14**	G:12	T:9	8:7	D:5	E:4	R:4	S:3	H:2	A:2	C:2	4:2	M:1	P:1	2:1	Z	K	F			
24	**«_»:22**	**O:16**	G:9	T:6	H:6	D:6	8:6	E:5	A:5	4:2	Z:2	M:2	R:1	S:1	2	P	N	I	C	L	F	
25	**«_»:23**	**O:15**	G:10	T:8	8:7	D:5	A:4	E:3	C:3	R:3	M:2	H:2	S:1	2:1	4:1	Z	P	N	I	L	K	
26	**«_»:21**	**G:18**	8:11	O:10	T:7	D:6	H:5	A:4	S:3	R:2	M:2	Z:2	E:1	P	N	K	4	L	I	F	2	
27	**«_»:24**	**O:11**	G:8	A:6	T:6	H:6	M:4	D:4	8:4	R:3	E:3	S:3	Z:3	2:3	C:2	4:1	N	L	K	I		
28	**«_»:25**	**O:18**	T:8	R:7	H:6	G:5	M:4	A:4	E:3	8:3	Z:2	D:2	4:1	2:1	S:1	C	P	L	N			
29	**«_»:21**	**G:13**	O:13	T:7	8:6	D:5	A:4	H:3	C:3	R:2	E:2	S:2	M:2	2:1	4:1	P:1	Z	N	F	K	I	
30	**«_»:22**	**O:12**	T:12	G:12	H:6	R:5	A:4	D:4	8:3	Z:2	E:2	M:2	P:1	4:1	2:1	S:1	C	L	I	N	F	
31	**«_»:20**	**O:15**	G:9	T:8	8:7	R:5	A:5	D:4	P:2	K:2	E:2	H:2	Z:2	S:2	C:2	4:2	2:1	M	I	F	N	
32	**«_»:22**	**O:18**	C:8	E:7	T:7	R:5	D:5	G:4	A:4	8:3	H:2	Z:2	M:2	I:1	4:1	2:1	S	P	K	N	F	
33	**«_»:21**	**O:13**	T:8	A:7	G:7	E:6	R:6	8:6	D:5	Z:3	H:3	M:2	S:1	4:1	K	C	I	N	P	F	2	
34	**«_»:22**	**O:13**	G:11	D:6	T:6	8:6	4:5	R:4	A:4	H:3	E:3	S:2	C:2	K:1	2:1	I	M	Z	P	F		
35	**«_»:24**	**O:12**	G:11	T:9	8:8	R:7	H:5	A:4	D:3	M:3	4:2	S:2	E:2	Z:1	2	P	L	C				
36	**«_»:22**	**O:15**	T:8	G:8	H:7	A:5	R:4	8:4	M:3	D:3	E:3	4:2	C:2	Z:1	2:1	P:1	K	S	L	I		
37	**«_»:20**	**O:16**	T:11	G:8	C:8	8:6	H:5	A:4	M:3	E:3	4:2	R:1	S:1	P:1	D:1	Z:1	2:1	I	N	L	F	
38	**«_»:24**	**O:14**	G:10	T:8	S:4	H:4	E:4	A:4	8:3	M:3	Z:3	D:2	C:2	R:2	2:2	P:1	F:1	4:1	I	N		
39	**«_»:20**	**O:15**	G:9	C:7	T:6	H:6	E:4	A:4	D:3	S:3	M:3	Z:2	8:2	R:2	4:2	P:1	2	F	N	L		
40	**«_»:21**	**O:15**	T:10	G:7	H:6	E:5	A:5	8:5	M:4	C:4	S:3	D:2	4:2	Z:1	F:1	2:1	R	I				
41	**«_»:21**	**O:15**	G:8	8:8	T:6	A:6	E:5	M:4	D:4	H:3	R:3	Z:3	P:1	S:1	4:1	N	C	2	K	F	L	
42	**«_»:22**	**O:13**	G:11	T:6	H:6	A:6	8:5	M:4	D:4	R:3	E:3	S:2	4:2	2:1	Z:1	C	K	F	P	N		
43	**«_»:21**	**O:12**	A:9	G:7	E:7	8:7	T:5	D:5	R:4	M:2	4:2	H:1	N:1	K:1	C:1	I:1	S:1	F:1	2	P	Z	
44	**«_»:22**	**O:19**	E:8	A:6	8:5	R:5	T:4	C:3	G:3	H:3	D:3	S:2	M:2	4:1	2:1	K	I	P	F	Z	N	L
45	**«_»:24**	**O:13**	A:8	C:6	R:5	E:5	T:5	G:4	H:4	Z:3	D:3	8:3	4:3	2:3	K:2	M:1	S	P	I	N		
46	**«_»:22**	**O:19**	T:7	A:6	8:6	R:4	E:4	D:4	G:3	C:3	H:2	Z:2	S:2	K:2	I:1	2:1	M:1	P	F	4	N	
47	**«_»:21**	**O:9**	A:9	T:8	G:7	H:6	8:5	M:3	R:3	N:3	C:3	Z:2	S:2	2:2	D:2	4:2	I:1	E:1	P	L	F	
48	**«_»:22**	**O:13**	A:8	T:7	8:7	C:5	R:5	M:5	D:5	G:4	4:3	S:2	E:2	Z:2	H:1	2:1	N:1	P	I	F		
49	**«_»:21**	**C:13**	G:13	8:11	O:7	T:4	A:4	D:4	2:3	H:2	4:2	S:2	M:1	Z:1	E:1	P:1	R:1	F	I	N	K	
50	**«_»:19**	**C:13**	G:12	8:9	O:8	T:6	A:4	R:4	D:4	2:3	H:2	P:2	4:2	S:1	M:1	I:1	E	Z	F	N	K	

51	**«_»:24**	**T:10**	G:10	O:8	C:7	8:6	A:5	E:4	H:4	S:3	2:2	R:2	D:2	Z:1	M:1	N	K	P	I	4	L	F
52	**«_»:22**	**O:14**	T:13	G:9	8:8	D:6	S:5	R:4	C:3	H:2	E:2	F:1	A:1	2:1	Z	I	P	K	4			
53	**«_»:20**	**O:19**	T:7	H:7	G:6	E:6	8:6	A:4	R:3	S:3	D:3	Z:2	M:2	C:1	4:1	P	K	2				
54	**«_»:23**	**O:14**	T:9	G:6	A:5	H:4	R:4	S:4	M:4	E:4	8:3	4:2	D:2	C:2	I:1	P	N	Z	L	K	2	
55	**«_»:23**	**O:14**	G:10	T:9	C:5	H:5	S:5	D:5	R:3	4:3	A:3	M:2	8:2	Z:1	E:1	2:1	P	K	I			
56	**«_»:24**	**O:13**	G:9	T:8	H:7	A:5	S:4	8:4	M:3	R:3	D:3	E:2	Z:2	C:2	2:1	4:1	N	L				
57	**«_»:21**	**T:12**	O:12	C:11	G:8	R:6	8:4	A:4	D:4	M:2	4:1	H:1	2:1	S:1	E:1	Z:1	N	P	L	K	I	F
58	**«_»:21**	**O:15**	T:9	G:6	C:6	H:5	8:5	A:4	R:3	D:3	S:3	M:3	E:3	Z:2	2:2	4:1	P	I	N	L	F	
59	**«_»:20**	**C:15**	G:9	O:9	8:7	D:6	A:5	T:4	R:3	4:3	S:2	E:2	M:1	I:1	H:1	2:1	Z:1	F	P	N		
60	**«_»:19**	**C:14**	O:12	A:7	G:7	D:6	T:5	8:5	R:4	H:3	E:3	2:2	Z:1	M:1	S	P	K	I	4	F	N	
61	**«_»:24**	**O:15**	8:9	T:7	G:5	A:5	H:4	E:4	R:4	S:2	M:2	D:2	C:2	4:2	Z:1	N:1	2:1	I	F	P	L	K
62	**«_»:24**	**O:12**	A:8	T:8	8:8	G:5	M:5	R:4	H:3	S:3	D:3	E:2	Z:2	C:2	N:1	4:1	2	P	L	K	F	
63	**«_»:20**	**A:11**	O:9	G:7	8:7	C:7	D:6	T:5	R:5	M:4	E:3	H:3	4:1	S:1	F:1	P	K	2	Z	I	N	
64	**«_»:22**	**G:11**	8:10	A:10	O:8	R:6	D:6	T:4	C:4	E:3	H:2	M:2	S:2	Z:1	K:1	N	2	P	I	F	4	
65	**«_»:21**	**G:11**	O:9	8:8	C:7	A:7	T:6	D:5	E:4	H:4	R:3	4:1	Z:1	M:1	K:1	S:1	2:1	I	F	P	N	
66	**«_»:20**	**G:10**	8:10	T:8	A:8	C:7	O:7	D:6	R:4	E:3	M:2	S:1	H:1	4:1	2:1	Z:1	I	P	K	N	F	
67	**«_»:23**	**A:10**	T:9	O:9	M:7	G:6	H:5	E:4	C:4	8:3	R:3	D:2	4:2	Z:1	S:1	2:1	N	L	P	I		
68	**«_»:24**	**T:11**	O:11	G:7	A:7	8:5	C:5	H:4	M:4	R:4	D:4	E:3	S:1	Z:1	4:1	2	N	L	P			
69	**«_»:22**	**O:12**	G:8	A:8	8:6	T:5	R:5	H:5	E:4	M:4	Z:2	4:2	2:2	P:1	D:1	N:1	L:1	I:1	F:1	S	K	
70	**«_»:22**	**O:12**	G:10	H:7	T:6	A:6	R:5	8:5	M:4	D:3	Z:2	E:2	4:1	2:1	C:1	S:1	P:1	K	N	L	F	
71	**«_»:22**	**O:17**	G:7	T:6	8:6	R:5	A:5	D:5	M:4	H:4	4:3	E:3	S:2	Z:1	C	P	I	F	N	K	2	
72	**«_»:22**	**O:16**	8:7	M:6	G:6	H:5	A:5	T:4	R:4	E:2	4:2	D:2	C:2	2:2	Z:1	S:1	I:1	L	P	N	K	
73	**«_»:22**	**O:18**	D:9	G:7	T:7	A:6	M:5	R:4	H:3	8:3	Z:2	E:2	S:2	C:1	2:1	N:1	4:1					
74	**«_»:24**	**O:13**	C:8	8:8	A:7	G:7	M:5	D:5	T:4	E:3	H:2	S:1	R:1	N:1	4:1	2:1	I	P	K			
75	**«_»:21**	**8:9**	G:9	A:8	C:7	O:7	T:6	D:5	E:4	R:4	M:3	S:3	4:1	Z:1	H:1	F:1	I:1	2:1	K	P	N	
76	**«_»:22**	**O:11**	A:10	G:9	D:7	8:7	R:6	C:4	T:3	E:3	M:3	S:2	N:1	H:1	4:1	Z	K	F	P	I	2	
77	**«_»:22**	**O:12**	A:11	D:9	R:7	G:7	8:6	C:4	T:3	E:3	M:3	K:1	4:1	S:1	I:1	H	Z	P	N	F	2	
78	**«_»:21**	**O:11**	A:9	G:8	D:7	C:7	8:6	T:5	R:4	M:3	E:3	4:2	H:2	2:1	I:1	F:1	Z	P	N	K	S	
79	**«_»:17**	**C:15**	G:15	8:11	D:8	T:7	O:6	4:3	A:2	S:1	H:1	E:1	P:1	2	Z	R	K	N	M	I		
80	**«_»:18**	**O:13**	C:13	G:9	8:8	E:6	D:6	A:5	T:4	H:3	4:2	R:2	M:1	S:1	P:1	F:1	2:1	Z	N	K		
81	**«_»:22**	**O:13**	T:8	A:7	S:5	H:5	G:5	E:5	8:4	R:4	D:3	C:3	M:3	Z:2	2:1	N:1	P	I	4	L	K	F
82	**«_»:21**	**O:11**	C:9	T:9	G:7	A:5	H:5	D:4	E:3	8:3	R:3	S:2	M:2	2:2	Z:1	4:1	P	N	L	K	I	
83	**«_»:19**	**G:13**	8:10	O:9	C:8	A:6	H:5	T:4	D:4	R:3	S:2	E:2	4:2	M:1	P:1	Z	K	N	I	2	F	
84	**«_»:19**	**G:12**	C:11	O:9	8:9	A:6	T:4	D:4	H:4	R:3	E:3	S:1	Z:1	M:1	4:1	2	P	K	F	N	I	
85	**«_»:19**	**O:14**	G:14	T:7	D:5	C:5	H:5	8:3	S:3	4:3	A:3	R:2	E:2	P:1	Z	M	2	K	I	F		
86	**«_»:21**	**O:15**	H:8	E:8	G:7	A:5	T:5	Z:3	S:3	C:3	8:3	D:3	M:2	R:2	4:1	P	N	I	2			
87	**«_»:21**	**O:11**	A:10	G:8	E:6	8:6	T:5	D:5	R:4	H:4	M:3	4:2	Z:1	C:1	S:1	P:1	K	N	L	I	F	
88	**«_»:22**	**O:16**	G:9	T:7	8:5	H:5	E:5	R:4	D:4	A:4	S:2	M:1	K:1	4:1	Z:1	C:1	P	2	I	N	F	
89	**«_»:20**	**G:11**	C:9	8:8	A:7	O:6	D:5	T:5	S:5	E:4	R:3	H:2	Z:1	M:1	4:1	P:1	2:1	K	F	Y	I	N
90	**«_»:19**	**G:12**	8:10	C:9	O:7	A:6	T:5	D:4	H:4	R:2	E:2	S:2	Z:1	M:1	K:1	I:1	4:1	2:1	P	F	N	
91	**«_»:23**	**O:13**	T:11	E:6	A:6	G:5	8:4	D:4	M:4	C:3	S:2	R:2	H:2	Z:1	N:1	K:1	2:1	P	I	4	F	
92	**«_»:23**	**T:12**	G:11	O:10	8:7	C:6	A:5	H:4	E:4	R:2	M:2	S:2	2:1	D:1	Z	P	4	N	I			
93	**«_»:19**	**C:12**	O:11	G:10	8:7	H:7	A:6	E:5	D:5	T:2	S:2	M:1	4:1	Z:1	R:1	P	N	K	7	2		
94	**«_»:19**	**G:13**	C:9	O:9	8:9	H:6	A:6	T:5	E:4	D:4	R:3	S:1	Z:1	K:1	P	N	M	F	4	2	I	
95	**«_»:22**	**O:17**	T:11	G:6	C:6	8:5	R:5	S:4	H:3	E:3	A:3	4:2	M:2	D:1	P	2	Z	N	L	I		
96	**«_»:24**	**O:15**	T:12	C:5	G:5	8:5	D:4	A:4	E:3	H:3	R:3	M:2	S:2	2:1	4:1	Z:1	P	N	K	F	L	I
97	**«_»:19**	**O:10**	A:10	D:8	G:7	8:6	R:5	T:5	C:4	E:4	M:3	H:2	4:2	S:1	P:1	N:1	2:1	Z	I	K	F	
98	**«_»:19**	**O:11**	G:10	D:8	A:8	8:8	C:7	T:5	R:4	M:3	E:2	H:2	4:2	S:1	N:1	Z	I	P	K	F		
99	**«_»:19**	**O:12**	G:8	A:8	C:7	8:7	D:6	T:5	E:5	Z:3	H:3	M:2	4:2	R:1	P:1	K	2	S	I	N		
100	**«_»:20**	**O:14**	G:8	8:7	A:7	C:5	D:5	E:5	T:4	H:4	M:3	4:3	Z:2	S:1	R:1	2:1	P	N	K	F		
101	**«_»:20**	**O:13**	G:10	A:7	8:7	H:6	T:5	D:4	E:3	C:3	R:3	K:2	S:2	4:2	M:1	2:1	Z:1	I:1	P	F		
102	**«_»:21**	**O:14**	C:8	G:6	R:6	T:5	A:5	D:4	E:4	Z:4	H:4	8:3	M:2	2:1	P:1	4:1	S	K	I			
103	**«_»:21**	**O:20**	G:8	8:7	H:6	T:5	A:5	D:4	C:3	E:2	4:2	R:2	2:2	Z:1	S:1	M	N	P	L	K	F	
104	**«_»:21**	**O:12**	8:9	G:9	A:7	C:6	S:4	H:4	T:3	D:3	Z:3	M:3	E:3	4:2	R:1	K:1	P	I	2			
105	**«_»:23**	**O:15**	A:7	E:6	8:5	T:5	D:5	R:4	G:4	C:4	S:2	H:2	Z:2	2:2	K:2	M:1	P	4	I	F		
106	**«_»:22**	**O:10**	A:10	G:7	E:6	8:5	T:5	D:4	M:3	H:3	C:3	Z:3	4:3	R:2	K:2	P:1	2:1	I	S			
107	**«_»:22**	**A:11**	O:11	D:8	8:7	G:6	R:6	T:5	E:4	C:4	M:3	4:1	H:1	Z:1	S	I	P	N	2	K	F	
108	**«_»:22**	**A:12**	O:9	G:9	D:7	C:6	8:5	M:5	R:4	T:4	E:3	H:2	4:1	2	Z	K	N	L	I	S	P	F
109	**«_»:23**	**T:14**	O:13	G:10	D:7	C:6	H:3	E:3	A:3	R:3	8:2	M:1	2:1	S:1	4:1	Z	P	L	K			

110	**«_»:22**	**O:15**	T:11	C:8	G:6	E:5	D:5	H:5	A:3	M:2	8:2	S:2	R:2	4:1	2:1	Z	N								
111	**«_»:19**	**C:13**	O:10	G:10	8:10	T:6	D:5	A:4	H:3	Z:3	S:2	M:1	4:1	K:1	2:1	R:1	P:1	E	I	F					
113	**«_»:19**	**A:13**	O:11	E:10	G:7	R:5	C:5	T:5	8:4	H:3	D:3	S:2	K:1	4:1	M:1	2:1	P	I	Z	F	N				
117	**«_»:20**	**O:10**	G:10	C:10	8:8	A:5	D:5	E:5	T:4	R:3	S:3	4:2	H:2	M:1	Z	2	I	P	F	Y	K				
118	**«_»:20**	**8:10**	O:9	C:9	G:8	A:7	D:7	T:5	E:4	S:3	H:2	R:2	2:1	M:1	4:1	P:1	Z	F	K	->J<-					
119	**«_»:19**	**C:17**	A:10	O:9	G:6	8:4	2:4	R:3	D:3	M:3	I:2	H:2	T:1	S:1	K:1	P	E	Z	4						
121	**«_»:18**	**O:13**	G:12	C:9	A:9	D:6	M:4	8:4	4:3	2:3	T:3	R:3	E:3	S:1	I:1	Z	P	K	H	F					
125	**«_»:17**	**O:15**	C:14	T:10	G:8	R:5	D:5	H:4	A:3	E:2	8:2	Z:1	P:1	S:1	4:1	M	K	2							
126	**«_»:17**	**O:16**	T:10	C:9	G:9	D:6	E:4	A:4	8:4	R:4	H:2	S:1	4:1	Z:1	2:1	P	M	K							
128	**«_»:20**	**C:11**	O:11	G:9	T:8	H:5	S:4	A:4	8:4	E:4	R:3	D:2	M:1	4:1	2:1	I	Z	P	N	K					
129	**«_»:19**	**C:15**	G:13	O:9	8:7	S:5	D:5	T:4	H:4	E:3	A:3	Z:2	2:2	4:1	K	R	P	M							
131	**«_»:21**	**G:11**	C:10	O:9	A:7	T:7	H:6	S:4	D:3	M:3	E:3	R:2	2:1	Z:1	K:1	8:1	P	4							
134	**«_»:22**	**A:12**	E:10	O:8	G:7	C:6	H:4	T:4	8:4	D:3	S:3	R:2	Z:1	4:1	K:1	M:1	2:1	I	P	N					
147	**«_»:20**	**G:10**	O:10	C:10	8:8	D:7	A:5	4:5	E:4	R:3	S:3	T:3	H:1	M:1	2:1	Z	N	P	K	I	L				
148	**«_»:20**	**O:12**	G:10	C:10	8:7	E:7	D:6	4:5	A:4	T:3	S:2	H:2	R:2	M:1	2:1	N	Z	P	K	L	I				
149	**«_»:20**	**C:10**	G:10	O:9	8:7	A:6	E:6	D:5	T:4	4:3	S:3	R:2	M:2	H:1	2:1	Z:1	N	P	I	K	F	L			
150	**«_»:19**	**C:15**	G:10	8:8	O:8	E:4	D:4	A:4	T:4	S:3	4:3	H:3	R:2	M:1	2:1	Z:1	P	I	N	K	L	F			
151	**«_»:19**	**C:14**	O:9	G:9	8:7	4:6	A:5	E:5	T:4	D:4	H:2	M:2	S:2	R:1	2:1	N	P	Z	I	K					
152	**«_»:20**	**C:10**	G:9	8:9	O:9	E:7	A:6	4:5	D:5	T:4	S:2	R:2	M:1	H:1	2	N	Z	I	P	K	F				
153	**«_»:20**	**G:10**	C:10	8:10	O:9	D:7	A:6	E:4	4:3	T:3	H:2	R:2	M:1	S:1	N:1	2:1	Z:1	P	F	K	L				
154	**«_»:21**	**O:11**	C:11	G:10	8:8	E:7	D:5	A:4	4:3	T:3	S:3	R:2	H:2	M:1	Z	2	P	N	F	K					
155	**«_»:20**	**O:12**	C:10	G:10	E:6	A:5	8:4	T:4	D:4	S:4	4:3	H:3	R:2	M:2	2:1	P	Z	K	N	L	F	I			
156	**«_»:19**	**C:13**	O:12	G:11	D:6	8:5	A:5	E:4	4:4	H:3	M:2	R:2	S:2	T:2	2	P	K	Z	N	I	F	L			
157	**«_»:20**	**O:12**	G:8	C:8	E:7	D:7	A:6	4:4	H:4	T:3	M:3	8:2	S:2	R:2	Z:1	2:1	P	K	I	N	F				
158	**«_»:20**	**O:12**	G:8	E:8	C:7	A:6	D:6	8:4	4:4	H:3	T:3	M:3	S:3	R:2	Z:1	P	2	N	K	F	L	I			
159	**«_»:21**	**O:12**	C:11	G:10	E:7	8:7	T:4	A:3	D:3	4:3	H:3	S:2	R:2	M:1	2:1	P:1	Z	K	I						
160	**«_»:21**	**G:11**	C:9	8:9	O:8	D:7	E:6	A:6	T:3	4:3	S:2	M:2	R:1	H:1	Z:1	P	2	N	I	K	F				
161	**«_»:19**	**C:14**	G:10	O:9	8:7	D:5	E:5	4:5	T:5	A:4	R:2	S:2	M:2	H:2	Z:1	2	P	N	K	I					
162	**«_»:20**	**O:10**	C:9	G:9	E:7	A:6	D:6	8:6	4:5	T:4	H:2	S:2	R:2	M:2	Z	2	P	N	I	K	F				
163	**«_»:19**	**C:11**	G:10	8:9	O:8	E:5	T:5	D:5	A:5	4:4	S:3	H:2	2:2	M:2	R:1	Z:1	P	I	K	L	F				
164	**«_»:19**	**O:11**	C:10	E:8	G:7	8:7	A:6	4:5	D:5	T:4	S:3	H:2	M:1	R:1	Z	2	P	I	N	K					
165	**«_»:19**	**G:11**	O:10	C:10	8:9	D:5	A:5	E:4	R:3	4:3	H:3	T:3	S:2	M:1	Z:1	2	P	K	F	I					
166	**«_»:20**	**O:12**	C:11	G:11	8:9	D:7	E:5	A:3	4:3	T:2	S:2	R:1	M:1	H:1	2	Z	K	F	P	I	N				
167	**«_»:19**	**O:10**	8:9	C:9	G:8	A:7	T:5	R:5	D:3	H:3	E:3	S:2	M:2	4:2	P:1	2:1	Z	I	K	F					
168	**«_»:20**	**O:16**	C:11	E:8	A:6	G:6	8:5	D:4	R:4	4:3	S:2	M:2	T:1	H:1	Z:1	2:1	N	K	I						
169	**«_»:20**	**O:11**	A:10	G:7	R:6	C:5	E:5	D:5	8:5	T:3	M:3	H:3	4:3	S:1	P:1	Z	K	I	2	F	L	N	Y	X	
172	**«_»:21**	**A:11**	O:10	G:10	C:6	H:5	R:4	D:4	8:4	M:4	E:4	T:3	S:2	4:1	P:1	K:1	2	Z	I	F	N				
173	**«_»:21**	**G:10**	A:10	O:7	8:7	C:5	M:5	H:5	T:4	R:4	E:3	D:3	S:2	4:2	K:1	P:1	2:1	I	Z	F					
175	**«_»:20**	**O:12**	C:11	G:6	A:5	8:5	2:5	H:4	T:4	Z:3	E:3	D:3	S:3	R:2	M:2	P:1	4	K	I	N					
180	**«_»:20**	**O:12**	C:11	G:7	A:5	T:5	H:4	E:4	8:4	2:4	Z:3	D:3	R:3	4:1	S:1	P:1	M:1	K:1	I	L	F				
181	**«_»:20**	**O:16**	C:9	E:8	T:6	A:5	G:5	R:4	D:4	8:3	2:2	4:2	S:1	K:1	H:1	Z:1	M:1	P	F						
182	**«_»:19**	**O:15**	C:11	G:8	8:7	A:5	D:5	T:5	E:3	R:3	M:2	4:2	S:2	H:2	Z:1	2:1	K	I	P	F					
183	**«_»:21**	**O:10**	A:9	8:8	C:7	G:7	T:5	E:5	M:3	4:3	D:3	K:2	H:2	Z:2	R:2	S:1	2:1	P	I	N					
184	**«_»:20**	**O:13**	C:11	G:7	E:6	T:6	A:5	8:5	D:5	M:3	4:2	R:2	2:1	H:1	Z:1	6	I	S	P	K	3	F	9	L	
185	**«_»:21**	**O:13**	A:9	8:7	C:6	G:6	R:5	D:4	T:4	M:3	E:3	2:2	H:2	4:1	Z:1	S:1	I:1	K:1	P	N	F				
186	**«_»:20**	**O:14**	A:8	G:6	E:6	C:6	8:6	D:5	T:4	R:3	M:2	H:2	4:2	Z:2	S:1	2:1	I	F	K	P					
187	**«_»:20**	**O:17**	D:7	G:7	A:5	T:5	R:5	E:5	C:5	8:4	4:4	S:2	H:2	2:2	Z:1	K	F	P	M	I					
188	**«_»:21**	**O:16**	C:10	A:7	D:6	2:5	R:4	E:4	M:3	G:3	8:3	4:3	T:2	Z:2	S:1	H:1	K								
189	**«_»:20**	**C:14**	O:12	G:7	A:5	2:5	T:4	E:4	8:4	S:4	D:3	H:2	4:2	Z:1	R:1	M:1	P:1	K:1	F	L					
190	**«_»:20**	**O:15**	C:14	G:8	D:5	T:4	E:4	8:3	R:3	S:3	H:3	2:3	A:2	Z:2	4:2	M:1	P	K	I	F					
191	**«_»:22**	**O:18**	T:6	E:6	8:6	A:5	G:4	C:4	H:4	S:3	2:3	D:3	Z:2	R:2	M:1	K:1	4:1	F	P	N	L	I			
192	**«_»:19**	**O:16**	G:7	8:7	C:6	T:6	H:4	E:4	A:4	D:4	Z:3	4:2	S:2	R:2	2:1	M:1	K:1	P	I						
193	**«_»:20**	**O:11**	A:10	G:7	8:7	D:7	T:5	R:4	C:4	E:4	M:3	H:2	4:2	I:1	P	2	S	K	Z	Y	N	F			
194	**«_»:20**	**O:10**	G:10	C:8	A:8	8:7	H:6	T:5	D:4	R:4	M:2	4:2	E:2	S:1	Z:1	P:1	K	I	2	L					
195	**«_»:20**	**G:9**	O:9	A:8	8:7	D:7	T:7	C:6	M:5	E:4	R:3	H:2	4:2	S:1	Z	P	F	2	L	K					
196	**«_»:21**	**O:12**	A:9	8:8	G:7	D:6	T:5	E:5	R:4	C:3	H:3	M:2	4:2	S:2	Z:1	F	K	P	N	2					
197	**«_»:21**	**A:12**	O:12	M:7	G:6	D:6	8:6	E:5	R:3	C:3	H:3	T:2	S:2	2:2	4:1	F:1	Z	P	L						
198	**«_»:20**	**O:9**	A:8	G:8	8:8	C:6	D:6	H:5	S:5	T:4	M:4	R:3	E:2	4:2	2	F	Z	P	N	K					
199	**«_»:20**	**O:19**	C:9	T:6	G:5	8:5	H:5	E:4	R:4	D:4	Z:3	S:2	A:2	2:1	4:1	P:1	M:1	F							

200	**«_»:21**	**C:12**	O:11	G:7	A:6	R:6	2:5	H:4	Z:4	T:4	8:4	D:2	E:2	S:1	P:1	M:1	4	K						
201	**«_»:19**	**O:15**	C:13	D:7	G:7	E:7	A:4	T:3	R:3	8:3	Z:3	4:2	S:1	H:1	M:1	2:1	P	I	K	F				
202	**O:20**	**« _ »:18**	E:10	D:8	C:8	A:6	G:5	8:3	4:3	M:2	R:1	T:1	H:1	Z:1	S:1	2	I	K	P	N	W			
203	**«_»:20**	**O:16**	C:11	E:7	T:6	G:5	D:4	8:4	A:4	R:3	S:3	Z:2	4:2	M:2	H:2	2:1	P	F	K	I				
204	**«_»:20**	**O:17**	C:12	T:7	G:6	E:6	D:6	R:4	A:4	2:2	8:2	Z:2	H:1	4:1	S:1	M	I	P	K					
205	**«_»:20**	**O:16**	C:13	E:7	G:6	D:5	T:5	A:4	R:3	S:3	8:3	M:2	H:2	Z:1	4:1	2:1	P	I	K	F	9			
206	**«_»:22**	**O:16**	C:11	E:7	T:5	G:5	D:5	A:4	8:4	R:4	M:2	Z:2	4:2	H:2	S:1	2	P	N	I	F				
207	**«_»:20**	**O:15**	C:12	G:7	8:6	A:5	R:5	T:4	E:4	D:4	M:3	4:2	Z:2	H:2	S:1	2	P	K						
208	**«_»:19**	**O:18**	C:10	E:7	8:7	G:7	A:5	D:4	R:3	S:2	T:2	M:2	4:2	H:1	2:1	Z:1	P	F	K	N				
209	**«_»:19**	**O:17**	C:13	G:9	D:7	E:5	8:5	T:3	A:2	4:2	R:2	Z:2	M:1	H:1	2:1	S:1	P	K	F	I				
210	**«_»:20**	**C:17**	O:16	G:8	D:7	R:5	T:4	A:3	E:2	8:2	S:2	2:2	4:1	M:1	Z:1	H	P	I	N					
211	**«_»:20**	**O:16**	C:11	G:8	D:6	T:5	8:5	A:4	E:4	4:3	R:3	M:2	Z:2	S:1	2:1	H:1	I	P	K	F				
212	**«_»:19**	**C:13**	G:10	O:10	D:6	A:6	8:5	E:5	4:4	T:4	S:4	H:3	M:2	R:1	Z	P	2	N	K	I	F			
213	**«_»:19**	**C:12**	G:10	O:10	A:7	E:5	D:5	8:4	T:3	S:3	H:3	R:3	4:3	M:3	P	Z	2	K	L	F	I			
214	**«_»:18**	**O:13**	C:9	A:8	G:6	8:6	T:5	D:5	E:4	R:4	4:3	H:3	M:3	S:1	Z:1	P	I	2	K	F	Y	L		
215	**«_»:18**	**C:12**	O:11	T:8	G:7	A:6	8:6	4:4	D:4	R:3	E:3	H:3	M:3	S:1	2:1	I	Z	P	K	N	F	9		
216	**«_»:18**	**C:13**	O:10	G:9	8:8	A:7	D:4	E:4	R:3	T:3	H:3	M:2	4:2	I:1	P:1	2:1	S:1	K	Z	F	N	Y	L	9
217	**«_»:19**	**O:11**	A:11	C:8	8:7	G:5	R:5	E:4	D:4	T:4	M:4	I:3	H:2	P:2	4:1	2:1	S	K	Z	N	F	Y		
218	**«_»:19**	**O:11**	C:10	A:8	G:7	T:6	8:5	D:5	E:4	R:4	M:3	4:2	S:2	H:2	P:1	I	2	K	Z	N	F			
219	**«_»:19**	**O:11**	A:10	G:8	C:7	8:6	T:5	D:4	R:4	E:4	M:3	H:3	S:3	4:2	2:1	P:1	I	K	Z	F	N	Y		
220	**«_»:19**	**A:11**	O:10	C:8	E:7	G:6	D:6	T:5	M:4	R:4	H:3	8:3	4:2	I:1	S:1	P	2	Z	K	F	N	L	Y	
221	**«_»:19**	**O:11**	A:10	C:8	D:8	G:7	E:6	M:4	T:3	8:3	4:3	R:3	H:2	I:1	P	S	Z	K	2	N	L	F		
222	**«_»:18**	**C:13**	O:11	G:9	8:8	D:7	A:6	T:4	E:4	4:3	H:2	R:2	M:2	S	P	K	Z	I	F	2	N			
223	**«_»:18**	**C:17**	O:9	G:8	A:7	8:6	D:6	E:5	T:3	4:3	M:2	R:2	H:2	S:2	K	Z	2	P	I	F	N	L	Y	
224	**«_»:18**	**C:17**	G:8	O:8	D:6	8:6	A:6	E:5	T:4	4:2	H:2	M:2	R:2	S:2	I:1	Z	K	2	P	F				
225	**«_»:19**	**C:11**	A:9	O:8	G:6	D:6	E:5	T:5	M:4	N:3	8:3	4:3	R:2	H:2	S:2	Z	2	P	K	I	L	F	V	
226	**«_»:19**	**C:13**	O:11	G:9	A:7	D:5	8:5	R:3	T:3	E:3	H:3	4:2	M:2	2:1	K:1	P	S	N	I	Z	F	Y	V	L
227	**«_»:19**	**C:14**	O:10	A:9	G:7	8:5	D:5	T:5	M:4	E:3	R:3	4:2	H:2	N:1	S	P	2	K	I	Z	F	L		
228	**«_»:19**	**O:11**	C:11	A:8	T:7	G:6	D:6	E:4	8:4	R:4	M:3	H:2	S:2	4:2	2:1	P:1	Z	N	I	K	F	9		
229	**«_»:19**	**O:12**	C:10	A:10	E:6	G:5	D:5	R:5	T:4	H:4	M:3	8:3	4:2	S:1	P:1	I	N	Z	K	2	F	Y	7	
230	**«_»:19**	**O:10**	8:9	C:9	A:9	G:6	T:6	M:4	R:3	D:3	E:3	H:2	4:2	I:2	P:1	N:1	2:1	S	Z	K	F			
231	**«_»:18**	**O:12**	C:11	8:8	A:7	G:6	T:6	H:5	M:4	4:4	E:3	D:3	R:2	S:1	P:1	Z	2	K	I	F	N	Y		
232	**«_»:19**	**O:12**	C:11	T:8	8:7	G:7	A:6	R:5	4:4	D:4	E:3	H:2	M:2	S:1	2	P	Z	I	K	F	N	7		
233	**«_»:19**	**C:11**	O:10	G:8	T:7	8:7	A:6	E:5	D:5	R:4	H:3	4:3	M:2	S:1	2:1	P:1	K	Z	I	Y	F			
234	**«_»:20**	**C:10**	G:9	A:8	O:8	E:5	D:5	8:4	R:4	T:4	M:4	S:3	4:3	H:2	Z:1	K	2	P	L	I	F	N		

Ecart entre mots de FRIEDMAN (page 164)

La colonne de gauche indique le numéro de la page du manuscrit, à droite, le résultat du calcul de l'Equation 9 Ratio des écarts entre mots. (page 161).

Page	Ecart
1	0,00690335
2	0,0162037
3	0,00421053
5	0,00985222
6	0,00473934
7	0,00632911
8	0,0023753
9	0,0108303
10	0,00847458
11	0,00735294
12	0,0107914
13	0,00584795
14	0,00531915
15	0,00145138
16	0,00695652
18	0,00487805
19	0,00674157
20	0,011194
23	0,00808625
24	0,00961538
25	0,00534759
26	0,00581395
27	0,00455581
28	0,00632911
29	0,00995025
30	0,0190217
31	0,00252525
32	0,0158046
33	0,0164319
34	0,0176991
35	0,0110497
36	0,0130548
37	0,0105932
38	0,00251256
39	0,0118812
40	0,0108696
41	0,0117188
42	0,0154639
43	0,00982318
45	0,00385356
47	0,00404858
48	0,00704225
49	0,0253165
50	0,02
51	0,00729927
52	0,00338983
53	0,0169492
54	0,00980392
55	0,0127389
56	0,00700935
57	0,01222
58	0,00294985
59	0,0230496
60	0,00515464
61	0,00260417
62	0,00268097
63	0,015873
64	0,0100604
65	0,0149254
66	0,0213465
67	0,00936768
68	0,00705882
69	0,00338983
70	0,00842697
71	0,0104987
72	0,00647948
73	0,0101523
74	0,00704225
75	0,0113208
76	0,0162963
77	0,02079
78	0,0257827
79	0,0280992
80	0,00864553
81	0,00285714
83	0,0166468
84	0,0149626
85	0,0074813
86	0,0144928
87	0,00696056
88	0,004914
89	0,0165877
90	0,0190311
91	0,00828729
92	0,00970874
93	0,00380228
94	0,015083
95	0,0103448
96	0,00947867
97	0,0117878
98	0,0183824
99	0,00792079
100	0,00444444
101	0,00797872
102	0,00244499
103	0,00970874
104	0,00737101
105	0,00792079
106	0,00875274
107	0,0183946
108	0,0159681
109	0,0175781
110	0,00662252
111	0,0121457
113	0,0150778
117	0,02581
118	0,0189274
121	0,0102041
128	0,00884956
134	0,012685
147	0,0603533
148	0,0527497
149	0,0564808
150	0,0531168
151	0,0654926
152	0,0641026
153	0,0521684
154	0,0508143
155	0,0462777
156	0,054664
157	0,070191
158	0,0550275
159	0,038078
160	0,038432
161	0,05864
162	0,0603908
163	0,0554415
164	0,0577485
165	0,0613718
166	0,0653951
167	0,0283843
169	0,0451157
172	0,0421719
173	0,0194553
175	0,00536673
180	0,00595238
181	0,0186782
182	0,0247396
183	0,0100334
184	0,0275229
185	0,0174129
186	0,0219355
187	0,00251256
188	0,00425532
189	0,00560224
190	0,0133843
191	0,0199253
192	0,0159363
193	0,00702576
194	0,0115385
195	0,0179641
196	0,0289855
197	0,0136054
198	0,0206349
199	0,00627615
200	0,00286533
201	0,0300481
202	0,0171184
203	0,0114504
204	0,00915332

205	0,0201005
206	0,00223714
207	0,0192308
208	0,00838926
209	0,0147929
210	0,0251799
211	0,0232558
212	0,0621139
213	0,0572762
214	0,0305873
215	0,0411697
216	0,0296404
217	0,0250929
218	0,0336441
219	0,0376214
220	0,0410276
221	0,0580697
222	0,0585125
223	0,0605319
224	0,0501567
225	0,0546533
226	0,0399649
227	0,0393443
228	0,030754
229	0,0425532
230	0,0306886
231	0,0365169
232	0,0361727
233	0,0284139
234	0,0527293
moyenne	0,020380466
écart-type	0,017746287

Les trigrammes internes et leurs contextes (page 129)

Nous avons trouvé des trigrammes qui ne finissent ni ne commencent un mot. Nous les listons en indiquant en premier le trigramme suivi du folio dans lequel il a été trouvé suivi à sa droite par le texte dans lequel se trouve ce trigramme (attention aux chiffres qui sont aussi des caractères de l'alphabet de VOYNICH). Le premier tableau considère les symboles  ,  ,  et  comme les digrammes DZ, FZ, HZ et PZ : il est donc possible de trouver des trigrammes comme ZAA mais ils n'ont pas de représentation graphique. Le deuxième tableau corrige cet effet en associant un code propre à chacun de ces digrammes : ceci marque l'opposition entre la discrétisation de FRIEDMAN et de CURRIER.

PREMIER TABLEAU.

AF8	<f23v.2;F>	4OHCO HOR TG ODTAF8G 4ODTCG 8OE OHTOE TAE OHT
AF8	<f36r.1;C>	TAF8AL 4ORAN TFZAE 2OM PZOR SAM HZG 8AIR
AF8	<f36r.1;F>	PTAF8AL 4ORAN TFZAE 2OM PZOR SAM HZG 8AIR
AFE	<f49v.25;F>	D TOE TOR TCR TDAFETG TODCCODG
AGF	<f46r.11;F>	PT8AIR S8S8 SCP 8AM S8G OFZC8G 4OPT8G E8G SCAR OP8AR S8G 2AGFTC8G
ATT	<f42r.1;C>	SO OFAM DZATTG OHTCCG PTCAR
ATT	<f42r.1;F>	HZSO OFAM HZATTG OHTCCG PTCAR
C9A	<f104v.37;F>	PO2AIRG GHC9AR TC8G SOCFTCCG DCTG 2AR O8 AIR SCG 4OPTCCG 2OE AM ARO8AK
CG4	<f108v.43;T>	GSCG 4OE ETCG SCG 4ODCAR SCG 4ODCCG ESCCG OHCCG SCCG4OE TCCDCCG ETK
CG4	<f111r.31;T>	SCOHTC8G TC8AIL SDCG4ODCAIIL SHCO8G 4ODCCG 4ODCC8G TDAE TCHZG
CG4	<f80v.20;C>	GSCCG4O RAR OE TCCG 8AM SCG 4ODAM OE ODAM
CG4	<f80v.26;C>	4OHG TCG4GHAM TCG ETC8G SC8G OETCG
CG4	<f80v.26;F>	4OHG TCG4G HAM TCG ETC8G SC8G ETCG
CG4	<f84r.5;C>	PTOE PZOE 2OEHCOE HC8G 4OHC8G 4ODCC8G 4ODCCG OEDCC8G HCG4ODC8G 4OPOR OEG
CGS	<f79r.38;F>	POE OEDCCGSCOE 4ODCCG
CGT	<f116r.44;F>	O8AM S 4ODA2 AECCGTG
CGT	<f32r.6;F>	FTO HTCGTC8G
CIC	<f111v.18;F>	HOLI2 SC8G 4OCIC8AM GODAMN SCG DAM SCG OHAMN AE DAMN O E R OE 8AMN
CII	<f108v.17;F>	4ODCCG EDCIIIR8 TC8G 4ODCCO2 SCOE HC8G 4OPT8G 4ODCS8G DC8AR OHAE RARAK
CII	<f108v.3;T>	2SCC8AE OE EDC8G EDCC8G TC8AEDC8G EDCC8G 4ODCTC8G OHC8CIIL OHCCG EOE
CII	<f111r.25;F>	2O SCOR ODCC8G OHCCCG 4ODCCIIIR 4ODCCA 2 TC8AR AEAE ODZG OyAR AM O8AM TO8G
CII	<f111v.28;T>	4OR TCIIL ODAIL TCAR EDAIL
CII	<f68r2.S14.1;R>	OHCCCIIR
CII	<f75r.21;C>	O4ODAN TCG 4HZ2G OR GSCIIR OE EOR AK
CII	<f81v.2;C>	4ODC8G ODAM DAIR ODAE 2AR OE DCIIE OEDAN AE OE ROE 8E
CII	<f81v.5;C>	ODAM 8CIIIL OHAN TDZG ODCC8G 4ODG
CII	<f83r.13;C>	2AETCOE HAR SC8G 2AEHC8G 2CIIR 4ODC8G 4PTC8G ETPZC8G E8AR
CII	<f84v.7;C>	SCOE 4OETCG OHCC8G 2CIIIL ODA8G TDC8G
CII	<f88v.14;L>	HOEDCCIIIR8AM 4ODG TCOE 8AM TCC2 AM TODAR 8AIK8
CII	<f88v.4;L>	TOCCG DCCIIIR8G 2 AM TO8G ODCARTCIIIR8 ARTCCG RAIIRAE
CII	<f88v.4;L>	TOCCG DCCIIIR8G 2 AM TO8G ODCARTCIIIR8 ARTCCG RAIIRAE
CII	<f88v.8;L>	4ODCCG 4IIIRDCO8G TOR OHCIIIR8G 4ODZOE ODOE TCC8G 4OHO8G
CII	<f88v.9;L>	GDCCOR TODZG OHOE TCCOE TCIIIR8G 4OHO8G 2OHOE TCHO7
CII	<f89r1.3;L>	4ODCOE TAE 4IIIR8AM TOE TCIIIR8G 4ODCTG 8AM HZCO8G 8A7
CII	<f89r1.9;L>	8AE2AE 8AE TCIIIR8G 8ANAE8G A 8AE8AE
CIO	<f2v.7;C>	8AM TOHTCG 4OHCCCIG TODCIO2 TCC2 TR TCAM
CKC	<f112r.43;F>	GHCCO R AM ODAR OPOR AM GTCC8G 4CCO8AR GHCTCCG SCOR OHCCKCE
CMA	<f111v.22;F>	2AM GTCAR OESCCG TCHZAMN TC8G 4ODCMAN ODAMN AE TAL ODAE TCG EDCCCG
CZ8	<f41r.9;F>	4ODCC8G ODC8G TCDCZ8G TC8G
CZ8	<f48v.5;F>	EDCCG 4OHZC8G HAM SC8 4ODAR OHCZ8G 8G
DFZ	<f43v.9;F>	GHCC8G OEO2 AM ODFZG
EII	<f107r.8;F>	HARSOR CCG OHCCOE 4ODCCG 4ODC8G EDAM 4ODAM 4ODAR AE ADIROEIIIRG
EII	<f111r.21;F>	8AM ODAR AM HCCG OHCCG OyOR SCG TCG TCG DG8CC8G TCO 8AM SCCH AR AEIIIR TCOHG8G
EII	<f68v2.R.1;C>	OHCG 8AEIIR
EII	<f89v2.12;L>	ODZO8G 8AM ODAK 2 CC CC 8AIRGIR TOOE EIIIRG 8AIR
ELI	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
H36	<f89r2.4;F>	PORATOE 4O8G 4OHCOE OE8A4 6H6E 2C69 269 6EHA4 6H36E 3C6E 6H6EF3G HAR TO EDCOPOE OCCOR AR
IKH	<f50r.7;C>	HO8AEAN 4IIKHAE DAM OHAM OHAE SC DAR AIIIL ODTC8G 8ARM
ILC	<f42v.5;C>	TODCCOR IIIILCG TCHAL
ILD	<f106v.9;T>	HSO8AIIL SOEDAIR ORAILDARAIIL SHTG 4OPT8G 4OPTG EOEDAIR SCARAK
ILD	<f43v.5;C>	4IIILDTC8G ORAEO8G OHC8OE THZ8G THCG
ILD	<f46r.3;C>	8AM SOR GDAE TDZG 8AM SC 8AE SC8G 4IIIILDOE 2 AM SCC GDAR 8AM

ILD	<f47r.9;C>	IIILDO DOR TAM ODAE TOE 8AM ODTO DTOR 2G
ILD	<f50r.3;C>	HSOE DAR SCC8G ODCO8G 4IIILDC8G TO8G DT8G PT8G TDAM O8AK
ILD	<f50r.4;C>	HT8G 4IIILDAR TC8G 4ODT8G 4ODAM OR AR AE OE DCO8AM OE2
ILD	<f55v.5;C>	4IIILDAM TAM GDAN GDAL O8G
ILO	<f106v.46;T>	GHAR ODAIL TCODAIIL TC8G ODCCCG TDAIILOE ODG RAIIL TCOAR TO2
ILO	<f108v.20;T>	POEDCC8AE SCODTCG EOHC8AIIL OHC8G OPTC8AIIL OHSC8G 4OHCG RAIILOE
ILO	<f112r.5;T>	OHAIR ODO8G OHO8G OHAE ODCCCG OHAR AK OAILOG
ILO	<f112v.19;T>	2ARAIL AILAE 4OCCCG 4OIICO ARAIIILOE TAEOR
ILO	<f29v.12;C>	4ODCO IIILOR OHTCG 2G
ILT	<f106r.17;T>	GOTOR ESC8G 4ODZCG 4ODC8AIL OR AIILTO8AR
ILT	<f8r.15;C>	8TCG DZOE TOE TCG DT2 TG 8AM 8OE 8AIIILTG DZG
IOA	<f32v.1;C>	DTCO8AM TOEDCTG 4OHAM 8AIIOAK
LTF	<f107v.11;F>	HSC8G OHAE SC8G 4ODTCG TDG 4ODCCG 4OHAM OHOE 4OHCC8G 4OLTFZG
PHH	<f96r.3;F>	HOHP HZCPHHE TO2 DZCO8G DCO8G TO8OE OHG
R2I	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
R5S	<f18v.3;C>	OR5SG 4ODG 4ODG TDTG 4ODSG 4ODAK
RCI	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
RPC	<f79r.1;C>	HORAN SC8G PTOR OR SCD OHARPCC8G OPTOEOR OHAE SC8G
RYO	<f105v.27;F>	SCOC ARYOR CC2G 4OPTCOAM OR DT8G 8AM OHCC8G DOE DAIR OHANEO8G
RYO	<f105v.27;T>	SCOC ARYOR CC2G 4OPTCOAIL ORDT8G 8AIIL OHCC8O DOEDAIR OHAIIEO8G
Z2H	<f30v.1;F>	HZ2HZAN SO2AM TOHZCG SO TCPTG SOR SCAM
Z8T	<f39r.4;C>	HTC8G T8G OEAM TC8G SDZ8TG TOE OR OR8G TCC2 AEG ODAE TC6
Z8T	<f39r.4;F>	HTC8G T8G OEAM TC8G SDZ8TG TOE OR OR8G TCC2 AEG ODAETC
ZAA	<f1r.4;F>	OM OHCCG OHCAR ROEOHG HZAAR 8AM ODAM OR ODAL
ZAT	<f42r.1;C>	SO OFAM DZATTG OHTCCG PTCAR
ZAT	<f42r.1;F>	HZSO OFAM HZATTG OHTCCG PTCAR
ZCI	<f51r.4;F>	8AM CHZCI2R ODOE TCO8G DZG TCCCG
ZCI	<f83r.44;C>	2OE RHAN HZCIE 2DAR SC8G
ZCS	<f105r.30;F>	DO8CCG ETE SOY AR AM8G PZCSG ODAE EDC8G EDAR TC8G 4ODAM OR FTODG
ZFZ	<f39v.6;C>	EDC8G ODTCG SOR 4OGDAK TODZFZCG OR AEG SIIIR8G
ZFZ	<f3v.7;C>	HTOR OHTAK TOR PZFZAK T
ZFZ	<f46v.4;F>	G8AM TDZG T8AE OEAR TDZ8G T8O8G HAR TAK DTC8G 8AM GDAM SDZFZG
ZG4	<f36r.4;F>	PO8AIIR PZG4OGPTOE R
ZGS	<f29v.1;F>	DOOM SOR TCHTG OEAE2 SG HTG HZGSG
ZGT	<f45v.9;C>	GTOR HZGTOE 4ODOK 2G
ZOA	<f101r2.7;F>	PZOAR OAM GPTOEG 8AM OHAM OHAM GFOEAM FTCOEAM GPTCG GPCO8G SOHCG O8ARM SCOAR SCOR DZCCG DZCG 4ODTCG TOEP TCOE 9G
ZOA	<f106v.37;F>	PGOAEG TCO ANR AE DSCO8AR 4O8AM SPZOAR SC8G OHC8AR OPAE FTC8G O8R
ZOA	<f113r.32;F>	SO8AM SDAM STHZAE ODSC8G OHAE ODAM PZOAE OHAMN ODAM TC8G 4OHAE
ZOA	<f113r.32;T>	SO8AIIL SDAIIL THZAE ODSC8G OHAE ODAIIL PZOAE OHAIL ODAIIL TC8G 4OHAE
ZOA	<f1r.3;C>	2GAIIR SCDG OR GDAM SO8 HZOARG HZR 8ARAM 2G
ZOA	<f1r.3;F>	2GAIIR SCDG OR GDAM SO8 HZOARG HZC2 8ARAM 2G
ZOA	<f1r.7;C>	O8AR G SOE PZOG OG8AR S 2 FZOAM SO8A2G
ZOA	<f1r.7;F>	O8AR SG SOE PZOG OG8AR S 2 FZOAM SO8ARG
ZOA	<f1v.5;C>	POHOG SOE 8AIR PZOAE 8AR TCG HO8G OHOAM SOSG
ZOA	<f1v.5;F>	POHOG SOE 8AIR PZOAE 8AR TCG HO8G OHOAM SOSG
ZOA	<f30v.8;C>	OGSG TCOHOE PZOAM PZCG
ZOA	<f30v.8;F>	OGSG TCOHOE PZOAM PZCG
ZOA	<f3v.1;C>	DOAM PZOAR 4OHOGA SA DZOE GDOAM 2 OEG
ZOA	<f53r.8;F>	4OHTOE 8AR 4OHG THOR OEHSO HZOA
ZOA	<f6v.16;C>	OTG HZAR HZOAR HZG
ZOA	<f9r.6;C>	PSOAN HZOAM ODAIIR O8O RAE SAR 2G SG8AE T8G
ZOA	<f9r.6;F>	PSOAN HZOAM ODAIIR FZO8ORAE SAR 2G SG8AE T8G

DEUXIÈME TABLEAU.

AF8	<f23v.2;F>	4OHCO HOR TG ODTAF8G 4ODTCG 8OE OHTOE TAE OHT
AF8	<f36r.1;C>	TAF8AL 4ORAN TYAE 2OM vOR SAM QG 8AIR
AF8	<f36r.1;F>	PTAF8AL 4ORAN TYAE 2OM vOR SAM QG 8AIR
AFE	<f49v.25;F>	D TOE TOR TCR TDAFETG TODCCODG
AGF	<f46r.11;F>	PT8AIR S8S8 SCP 8AM S8G OYC8G 4OPT8G E8G SCAR OP8AR S8G 2AGFTC8G
ATT	<f42r.1;C>	SO OFAM XATTG OHTCCG PTCAR
ATT	<f42r.1;F>	HZSO OFAM QATTG OHTCCG PTCAR
C9A	<f104v.37;F>	PO2AIRG GHC9AR TC8G SOCFTCCG DCTG 2AR O8 AIR SCG 4OPTCCG 2OE AM ARO8AK
CG4	<f108v.43;T>	GSCG 4OE ETCG SCG 4ODCAR SCG 4ODCCG ESCCG OHCCG SCCG4OE TCCDCCG ETK
CG4	<f111r.31;T>	SCOHTC8G TC8AIL SDCG4ODCAIIL SHCO8G 4ODCCG 4ODCC8G TDAE TCQG
CG4	<f80v.20;C>	GSCCG4O RAR OE TCCG 8AM SCG 4ODAM OE ODAM
CG4	<f80v.26;C>	4OHG TCG4GHAM TCG ETC8G SC8G OETCG
CG4	<f80v.26;F>	4OHG TCG4G HAM TCG ETC8G SC8G ETCG
CG4	<f84r.5;C>	PTOE vOE 2OEHCOE HC8G 4OHC8G 4ODCC8G 4ODCCG OEDCC8G HCG4ODC8G 4OPOR OEG
CGS	<f79r.38;F>	POE OEDCCGSCOE 4ODCCG

CGT	<f116r.44;F>	O8AM S 4ODA2 AECCGTG
CGT	<f32r.6;F>	FTO HTCGTC8G
CIC	<f111v.18;F>	HOLI2 SC8G 4OCIC8AM GODAMN SCG DAM SCG OHAMN AE DAMN O E R OE 8AMN
CII	<f108v.17;F>	4ODCCG EDCIIIR8 TC8G 4ODCCO2 SCOE HC8G 4OPT8G 4ODCS8G DC8AR OHAE RARAK
CII	<f108v.3;T>	2SCC8AE OE EDC8G EDCC8G TC8AEDC8G EDCC8G 4ODCTC8G OHC8CIIL OHCCG EOE
CII	<f111r.25;F>	2O SCOR ODCC8G OHCCCG 4ODCCIIIR 4ODCCA 2 TC8AR AEAE OXG OyAR AM O8AM TO8G
CII	<f111v.28;T>	4OR TCIIL ODAIL TCAR EDAIL
CII	<f68r2.S14.1;R>	OHCCCIIR
CII	<f75r.21;C>	O4ODAN TCG 4Q2G OR GSCIIR OE EOR AK
CII	<f81v.2;C>	4ODC8G ODAM DAIR ODAE 2AR OE DCIIE OEDAN AE OE ROE 8E
CII	<f81v.5;C>	ODAM 8CIIIL OHAN TXG ODCC8G 4ODG
CII	<f83r.13;C>	2AETCOE HAR SC8G 2AEHC8G 2CIIR 4ODC8G 4PTC8G ETvC8G E8AR
CII	<f84v.7;C>	SCOE 4OETCG OHCC8G 2CIIIL ODA8G TDC8G
CII	<f88v.14;L>	HOEDCCIIIR8AM 4ODG TCOE 8AM TCC2 AM TODAR 8AIK8
CII	<f88v.4;L>	TOCCG DCCIIIR8G 2 AM TO8G ODCARTCIIIR8 ARTCCG RAIIRAE
CII	<f88v.4;L>	TOCCG DCCIIIR8G 2 AM TO8G ODCARTCIIIR8 ARTCCG RAIIRAE
CII	<f88v.8;L>	4ODCCG 4IIIRDCO8G TOR OHCIIIR8G 4OXOE ODOE TCC8G 4OHO8G
CII	<f88v.9;L>	GDCCOR TOXG OHOE TCCOE TCIIIR8G 4OHO8G 2OHOE TCHO7
CII	<f89r1.3;L>	4ODCOE TAE 4IIIR8AM TOE TCIIIR8G 4ODCTG 8AM QCO8G 8A7
CII	<f89r1.9;L>	8AE2AE 8AE TCIIIR8G 8ANAE8G A 8AE8AE
CIO	<f2v.7;C>	8AM TOHTCG 4OHCCCIG TODCIO2 TCC2 TR TCAM
CKC	<f112r.43;F>	GHCCO R AM ODAR OPOR AM GTCC8G 4CCO8AR GHCTCCG SCOR OHCCKCE
CMA	<f111v.22;F>	2AM GTCAR OESCCG TCHZAMN TC8G 4ODCMAN ODAMN AE TAL ODAE TCG EDCCCG
CXC	<f100r.6;C>	2OM TOE vOE SOE 4OXOG TOR TOE SA DCCG CXCG GDCCAK
CXC	<f101r2.1;F>	PTCOE SCOE OESCG 4OXOE SOR GHCOE SCOXCG 4POE TCAR 2AM OECCCG 4DCCG TOPTCCG TCXCG vCOQG GDTG TCCG TCDCCG 8AE TCG
CXC	<f101r2.6;F>	ODCCOE SO SO8G SO SOE ODCCCOE TCG2 SCODCCG SCCOR TTG TO8AM SCCXCG HCCOE 2TCOE 2AR OCCOR
CXC	<f107v.5;T>	HOE SCCXC8G 4OHOE T8OR OHCT8G HCOE HC8AIIL OPTC8G 4OPT8G GHAR AIIIE
CXC	<f108v.30;F>	OETCOE SC8 4ODC8G 4ODC8AM TCXC8 4OHCC8G OHC8G 4ODC8G ODCCAR EDAK
CXC	<f108v.30;T>	OE TCOE SC8 4ODC8G 4ODC8AIL TCXC8 4OHCC8G OHC8G 4ODC8G ODCCOR EDAK
CXC	<f108v.36;F>	2AM SCOR SCCG SCXCG 4ODCG ODCG SCG EDAM SC8G 4ODAM 8AEAK
CXC	<f108v.36;T>	2AIL SCOR SCCG SCXCG 4ODCG ODCG SCG EDAIL SC8G 4ODAIL 8AEAK
CXC	<f108v.40;F>	8SC8G HC8G TCXCG SCCDG ESCC8AM SCAR OEDC8G TE DAR HAR OHAM
CXC	<f108v.40;T>	8SC8GHC8G TCXCG SCCDG ESCC8AIL SCAR OEDC8G TG DAR HAR OHAIIL
CXC	<f108v.48;F>	2AM ODAM TCCG EDAM TCAE TCOE DCAR 4ODCC8G 4ODCCG TCXC8G 4ODAE AAK
CXC	<f108v.48;T>	2AIIL ODAIL TCCG EDAIIL TCAE TCOE DCCAR 4ODCC8G 4ODCCG TCXC8G 4ODAE OAK
CXC	<f111r.22;F>	2SCOE DCC8G 8AE HTC8 TCXCG ODCG 4OAM 4OTC8G 4ODCOR ODCCG DCO QC8G 4ODCG
CXC	<f111r.22;T>	2SCOE DCC8G 8AE HTC8 TCXCG ODCCG 4OAIL 4OTC8G 4ODCOR ODCCG DCO QC8G 4ODCG
CXC	<f111r.45;T>	OAIL AIL DCCCGHCC8 TCXC8AR ODCCG EDCCCG ODCCO EDCCG EDCCG EDCC8G 4ODG
CXC	<f111v.38;F>	GTCCG O AM TCXCG OHAMN 4OHE TCAR TC8G 4ODCCAG ODCC8G EDCCG
CXC	<f111v.38;T>	GTCCG OAIIL TCXCG OHAIL 4OHE TCAR TC8G 4ODCCG ODCC8G EDCCG
CXC	<f111v.40;F>	GDCCCG EDAN TXG TODAMN TXAE SCXC8G 4ODCCG 4ODCC8G ET2E
CXC	<f111v.40;T>	GDCCCG EDAIL TXG TODAIL TXAE SCXC8G 4ODCCG 4ODCC8G ET2E
CXC	<f112v.26;F>	GTC8AE TCXCG TCXG TCCOE 4ODCC8G 4OHCA 2 AK TOR2
CXC	<f112v.26;T>	GTC8AE TCXCG TCXG TCCOE 4ODCC8G 4OHCOR AK TO2
CXC	<f112v.41;F>	GDCC8AL TCXCG OAMN TOE
CXC	<f112v.41;T>	GDCC8AL TCXCG OAIL TOE
CXC	<f31r.7;C>	GDCC8AR 2AM TCXCG SCOE 4ODC8G GDCC8G TC8G E8G
CXC	<f31r.7;F>	GDCC8AR 2AM TCXCG SCOE 4ODC8G GDCC8G TC8G E8G
CXC	<f43r.13;C>	HSC8 4OSCXCG O8CC8G 4CODCCG 4OHC8G 8AS SO8O8G SOTOE TXG GDCCG8G
CXC	<f43r.13;F>	M HSC8 4OSCXCG O8CC8G 4CODCCG 4OHC8G 8AM SO8O8G SOTOE TXG GDC8G8G
CXC	<f52v.4;F>	HTOR QCOR QCOE TCCOR TCOE TCXCCG 2A8G
CXC	<f76r.10;C>	4ODCC8G TCQG TCXCG ODOE ODAM SCXCG EDCC8G OHCG 8AE GDAE TC8G 2AR
CXC	<f76r.10;C>	4ODCC8G TCQG TCXCG ODOE ODAM SCXCG EDCC8G OHCG 8AE GDAE TC8G 2AR
CXC	<f76r.10;F>	4ODCC8G TCQG TXCG ODAE ODAM SCXCG ODCC8G OHCG 8AE GDAE TC8G 2AR
CXC	<f76r.46;F>	2AM SCCG OR OR AE 2OESCG ODCC8G E8AM TCXCG ODC8AEOR
CXC	<f76v.19;C>	ORAR SCCG OHAR SC8G OHC8G TCXCG OETC8G TCXG TCXG EDG
CXC	<f76v.19;F>	OR AR SCCG OHAR SC8G OHTC8G TCXCG OETC8G TCXG SCXG EDG
CXC	<f77r.10;C>	8AM TCC8G ESCG 4OE AR TCC2 SCXC8G 4OE TCC8G 4OHAM
CXC	<f77r.10;F>	8AM TCC8G ESCG 4OE AR TCC2 SCXC8G 4OE TCC8G 4OHAM
CXC	<f77r.31;C>	OEAM TCCG SCXCG ESCCG 4GDAM SCC8G EAM
CXC	<f77r.31;F>	OEAM TCCG SCXCG ESCCG 4GDAM SCC8G EAM
CXC	<f78v.25;C>	HCCOE OEDCSCG 4OETCOE OE OR SCXC8G OR OE SAK
CXC	<f78v.25;F>	HCCOE OEDCSCG 4OETCOE OE OR SCXC8G OR OE SAK
CXC	<f78v.4;C>	OETG ES8G ETCXG OE DCC8G ETCXCG EOEDC8GDANOE
CXC	<f78v.4;F>	K OETG ES8G ETCXG OEDCC8G ETCXCG EOEDC8G DAM OE
CXC	<f79v.10;C>	PTC8G ESCXC8G 4ODCCG 4ODAM OEDG OPTC8G PTC8G
CXC	<f79v.10;F>	PTC8G ESCXC8G 4ODCCG 4ODAM OEDG OPTC8G PTC8G
CXC	<f79v.6;C>	GTCXCG R AN TC8G 4ODAN TC8G OESC8G 8AR GHAK
CXC	<f79v.6;F>	GTCXCG 2AM TC8G 4ODAM TC8G OESC8G 8ARG HAK

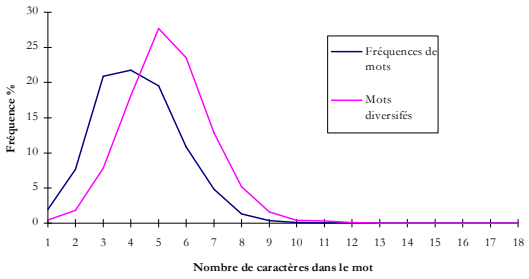
CXC	<f81r.11;C>	OESCOE OEDC8G SCXC8G OEHC8G
CXC	<f81r.11;F>	OESCOE OEDC8G SCXC8G OEHC8G
CXC	<f82r.3;C>	4ODCCG ETCXC8G 4ODAEG 2OEDAM TXG 4ODAM
CXC	<f82r.3;F>	4ODCCG ETCXC8G 4ODAEG 2OE DAM TXG 4ODAM
CXC	<f83v.14;C>	8AM 4ODAE SCXCG 4ODCCG TAE 4ODCCG 4ODAM TC8G 2AR AE
CXC	<f96v.11;F>	2AR O2 TCXCG 2OQ
CXC	<f99r.11;F>	8AM TCCODCCG TCXCG 8AR OE8G SCCG DCO8G ODCCCG 2AM OE2
CXT	<f112r.33;F>	2AROE ODTCCG vC8G S2CXTG ODCCOR TC8G S8AE
CZ8	<f41r.9;F>	4ODCC8G ODC8G TCDCZ8G TC8G
CZ8	<f48v.5;F>	EDCCG 4OQC8G HAM SC8 4ODAR OHCZ8G 8G
DFZ	<f43v.9;F>	GHCC8G OEO2 AM ODFZG
EII	<f107r.8;F>	HARSOR CCG OHCCOE 4ODCCG 4ODC8G EDAM 4ODAM 4ODAR AE ADIROEIIIRG
EII	<f111r.21;F>	8AM ODAR AM HCCG OHCCG OyOR SCG TCG TCG DG8CC8G TCO 8AM SCCH AR AEIIIR TCOHG8G
EII	<f68v2.R.1;C>	OHCG 8AEIIR
EII	<f89v2.12;L>	OXO8G 8AM ODAK 2 CC CC 8AIRGIR TOOE EIIIRG 8AIR
ELI	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
H36	<f89r2.4;F>	PORATOE 4O8G 4OHCOE OE8A4 6H6E 2C69 269 6EHA4 6H36E 3C6E 6H6EF3G HAR TO EDCOPOE OCCOR AR
IKH	<f50r.7;C>	HO8AEAN 4IIKHAE DAM OHAM OHAE SC DAR AIIIL ODTC8G 8ARM
ILC	<f42v.5;C>	TODCCOR IIILCG TCHAL
ILD	<f106v.9;T>	HSO8AIIL SOEDAIR ORAILDARAIIL SHTG 4OPT8G 4OPTG EOEDAIR SCARAK
ILD	<f43v.5;C>	4IIILDTC8G ORAEO8G OHC8OE TQ8G THCG
ILD	<f46r.3;C>	8AM SOR GDAE TXG 8AM SC 8AE SC8G 4IIILDOE 2 AM SCC GDAR 8AM
ILD	<f47r.9;C>	IIILDO DOR TAM ODAE TOE 8AM ODTO DTOR 2G
ILD	<f50r.3;C>	HSOE DAR SCC8G ODCO8G 4IIILDC8G TO8G DT8G PT8G TDAM O8AK
ILD	<f50r.4;C>	HT8G 4IIILDAR TC8G 4ODT8G 4ODAM OR AR AE OE DCO8AM OE2
ILD	<f55v.5;C>	4IIILDAM TAM GDAN GDAL O8G
ILO	<f106v.46;T>	GHAR ODAIL TCODAIIL TC8G ODCCCG TDAIILOE ODG RAIIL TCOAR TO2
ILO	<f108v.20;T>	POEDCC8AE SCODTCG EOHC8AIIL OHC8G OPTC8AIIL OHSC8G 4OHCG RAIILOE
ILO	<f112r.5;T>	OHAIR ODO8G OHO8G OHAE ODCCCG OHAR AK OAILOG
ILO	<f112v.19;T>	2ARAIL AILAE 4OCCCG 4OIICO ARAIIILOE TAEOR
ILO	<f29v.12;C>	4ODCO IIILOR OHTCG 2G
ILT	<f106r.17;T>	GOTOR ESC8G 4OXCG 4ODC8AIL OR AIILTO8AR
ILT	<f8r.15;C>	8TCG XOE TOE TCG DT2 TG 8AM 8OE 8AIIILTG XG
IOA	<f32v.1;C>	DTCO8AM TOEDCTG 4OHAM 8AIIOAK
NXC	<f107r.30;F>	PAIR ANXC8G SAE DAM DAIRG ODARAE 4ODAM OPAITG OPAE RARG DG
PHH	<f96r.3;F>	HOHP QCPHHE TO2 XCO8G DCO8G TO8OE OHG
R2I	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
R5S	<f18v.3;C>	OR5SG 4ODG 4ODG TDTG 4ODSG 4ODAK
RCI	<f66r.W.1;C>	OIIEIRCO 8AM IRIIEIE IELIR2IRCIK
RPC	<f79r.1;C>	HORAN SC8G PTOR OR SCD OHARPCC8G OPTOEOR OHAE SC8G
RYO	<f105v.27;F>	SCOC ARYOR CC2G 4OPTCOAM OR DT8G 8AM OHCC8G DOE DAIR OHANEO8G
RYO	<f105v.27;T>	SCOC ARYOR CC2G 4OPTCOAIL ORDT8G 8AIIL OHCC8O DOEDAIR OHAIIEO8G
XYC	<f39v.6;C>	EDC8G ODTCG SOR 4OGDAK TOXYCG OR AEG SIIIR8G
ZCI	<f51r.4;F>	8AM CHZCI2R ODOE TCO8G XG TCCCG

Les mots et leurs fréquences (page 151)

CURRIER

Dimension du mot	Pourcentage	Pourcentage diversifié
1	1,929625426	0,452293776
2	7,654345359	1,8522507
3	20,88535755	7,839758777
4	21,73913043	18,11328882
5	19,52326901	27,6976093
6	10,80787643	23,54081413
7	4,851206633	12,79345251
8	1,327542812	5,212147319
9	0,380002961	1,572259315
10	0,098702068	0,430755977
11	0,074026551	0,323066983
12	0,02961062	0,129226793
14	0	0
15	0	0
16	0,004935103	0,021537799
18	0,004935103	0,021537799
Nombre total de mots	20263	4643

Fréquences de mots dans la transcription de Currier

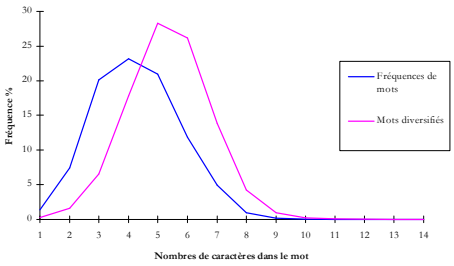


Mot	Taille
DOARG2AROCCCTCCDAR	18
GHC8GIIIR4ODCC8G	16
TCPTCFGS8T8G	12
ODAIIILODCCG	12
EOEDC8GDANOE	12
OEDCC8GESC8G	12
ODAETC8GHORG	12
OEDCCAEDTC8G	12
4IIILHOKO8G	11
RTC8GO4ODOE	11
GDCO8GDCC8G	11
SOIIIRKODTG	11
IELIR2IRCIK	11
HOETCCCHTAE	11
PAE8ARAIRAE	11
ETC8GRPTC8G	11
8OECC2OETCG	11
4OHCC8GDCCG	11
4ODCC8GHT8G	11
2AETHC8GHAR	11
OEDCC8GEARG	11
S8GDAIRGEAK	11
4ODTOEDTC8G	11

FRIEDMAN

Dimension des mots	Pourcentage	Pourcentage diversifié
1	1,384026704	0,288975582
2	7,438465087	1,603814478
3	20,12537654	6,516399364
4	23,1810904	17,80089582
5	20,96393389	28,29070944
6	11,85106787	26,13784135
7	4,89836902	13,85637914
8	0,94710847	4,262389828
9	0,17639556	0,924721861
10	0,03799289	0,202282907
11	0,013568889	0,072243895
12	0,005427556	0,028897558
13	0,002713778	0,014448779
Total de mots	36849	6921

Fréquences de mots dans la transcription de Friedman



Mot	Taille
TDZOCDCDZC2SG	13
PTO8OETOPTAE	12
4ODCC8G4ODAR	12
ODCCO2TCCO2	11
4ODCCGESC8G	11
ADIROEIIIRG	11
OETARIIIRFN	11
AMAIIIRIIIR	11

Autres textes

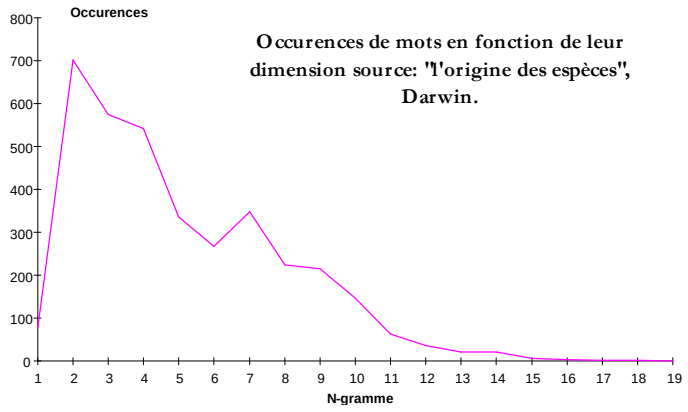


Figure 36 Mots et occurrences, texte de Darwin (3585 mots), anglais.

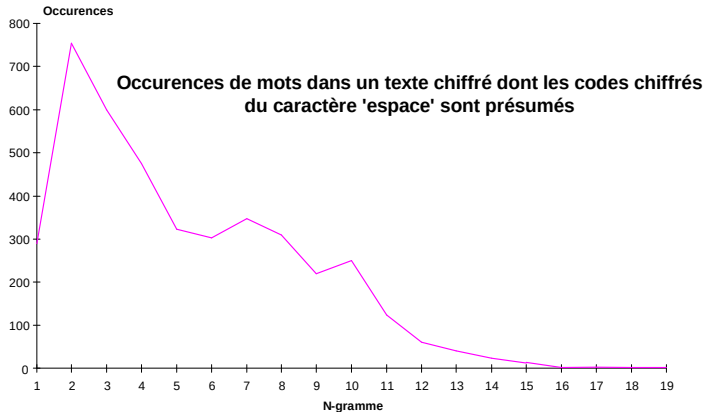


Figure 37 Asymptote en x=6. Source: séquence de codes polysubstitués de la langue Anglaise. Le graphique montre les occurrences des mots polysubstitués en fonction de leur dimension.

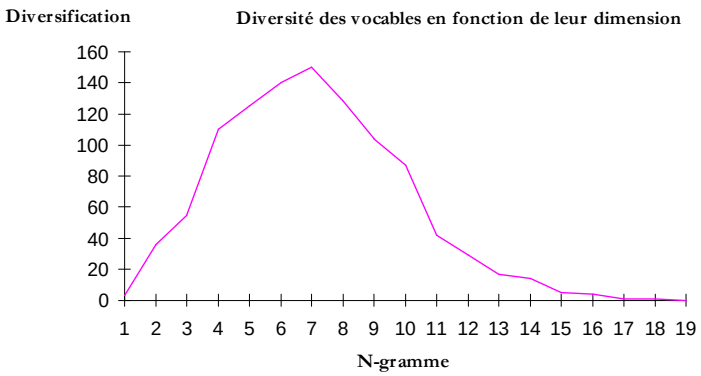


Figure 38 Répartition des n-grammes en fonction de leur diversité (1051 vocables). Source: texte de Darwin, langue anglaise.

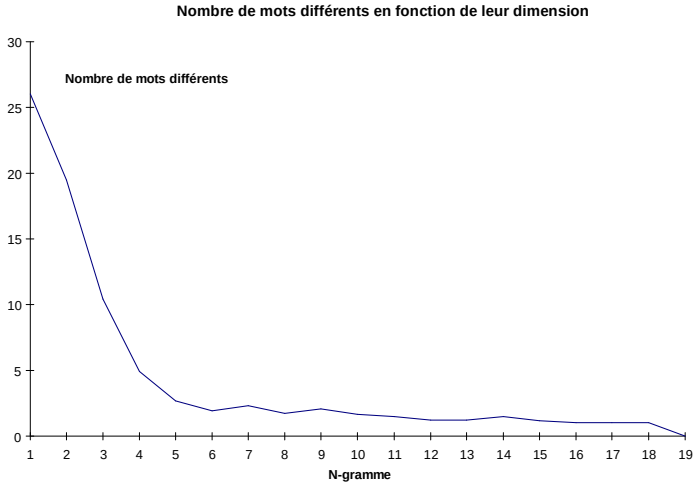


Figure 39 La courbe décrit le rapport (nombre de mots de dimension n-grammique divisé par le nombre de n-gramme différents) en fonction de la dimension n-grammique des mots.

Le graphe des opérations pour Rep. Mul.(page 223)

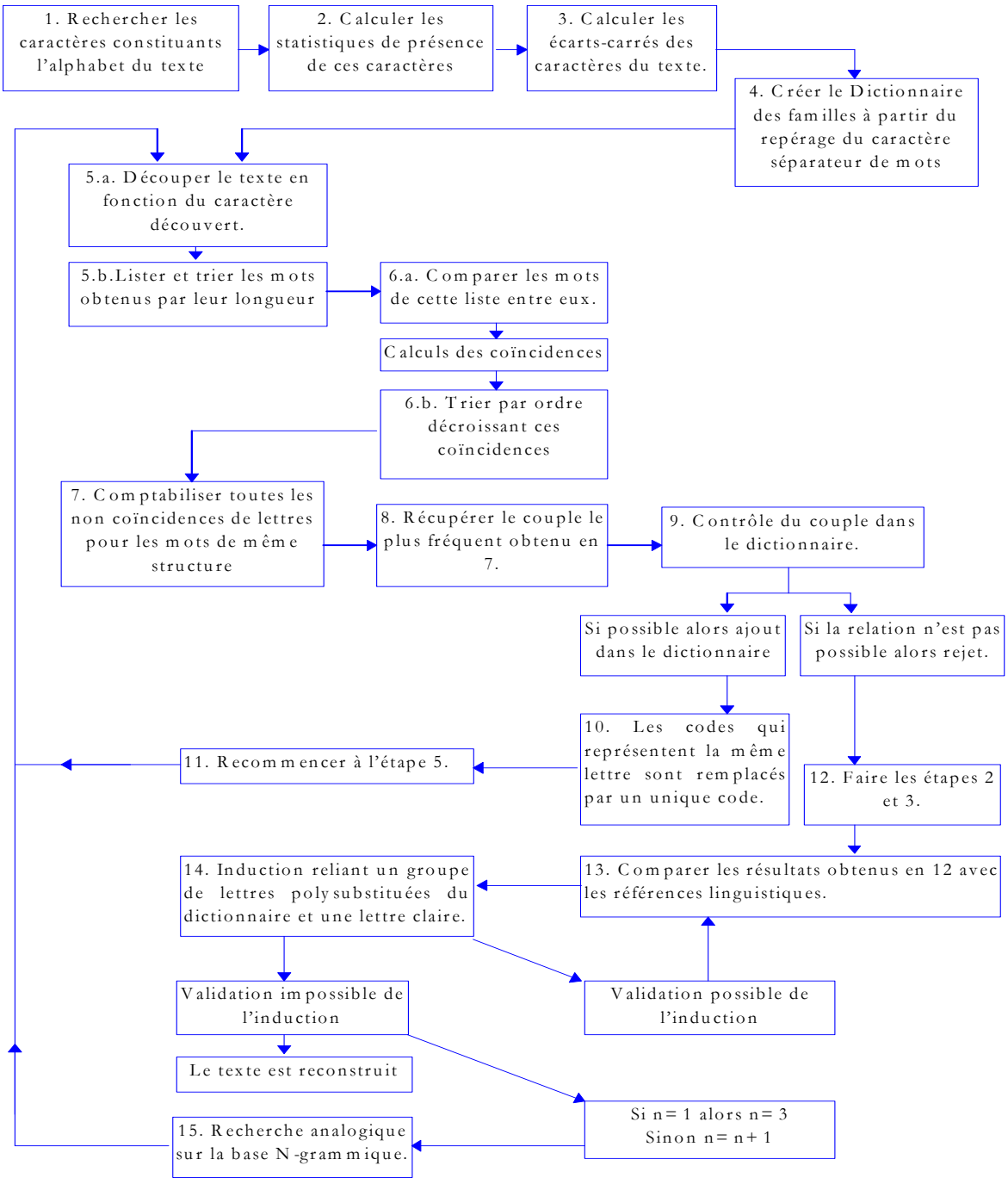


Tableau 17 Décomposition des procédures de reconstruction d'un texte polysubstitué.

Permutations de clés et propositions Lulliennes

712-§ Les arrangements possibles d'entités procèdent de la permutation (page 187 & 237). Au 13ème siècle, Raymond LULLE construisait les bases de ce qui deviendra dans les siècles suivants une description du monde par les langues synthétiques. A travers cette recherche d'un langage universel se dessinait parallèlement les moyens de la représentation multiple propre à la cryptographie desquels découleront les systèmes d'encryptage modernes par disques concentriques. Les réseaux de rosettes du manuscrit de Voynich, les cercles concentriques de Raymond LULLE et les systèmes d'encryptages par rotors ont tous les trois un point commun : l'exploration du possible par la combinatoire. Nous allons observer deux méthodes d'exploration : la première méthode ne s'encombre pas du monde des permutations dans son entier et se limite à énoncer chacune des possibilités tandis que la deuxième méthode est une représentation du monde de toutes les permutations possibles d'un groupe d'entités.

Permutations ordonnées séquentielles (page 187)

713-§ La méthode proposée ici permet de lister automatiquement dans l'ordre l'ensemble des permutations classées par ordre croissant d'une factorielle η. Nous partons du fait que nous connaissons l'état de départ et les permutations suivantes déjà parcourues. Notre méthode se base sur la répétition de chaque élément de {1..η} par la règle (η-p)! tel que p représente le numéro de la position de l'élément considéré de {1..η}. Ainsi le premier élément sera répété (η-1)! fois et ainsi de suite jusqu'au dernier élément répété (η-η)!

	Reste (η-p)-r redondance(s)	Permute	incrémente de 1 jusqu'à ce qu'il soit différent des précédents	état de la permutation en voie de construction	reste les éléments classés par ordre croissant
Elément étudié		**1234**			
1 est possible car il reste	(4-1)!-1= 6-1= 5 redondances	1			
2 est possible car il reste	(4-2)!-1= 2-1= 1 redondance	12			
3 n'est pas possible car il reste	(4-3)!-1= 1-1= 0 redondance	12	3 devient 4	**124**	**3**
		1243	←		
1 est possible car il reste	(4-1)!-2= 6-2= 4 redondance	1			
2 n'est pas possible car il reste	(4-2)!-2= 2-2= 0 redondance	1	2 devient 3	**13**	**24**
		1324	←		
1 est possible car il reste	(4-1)!-3= 6-3= 3 redondances	1			
3 est possible car il reste	(4-2)!-1= 2-1= 1 redondance	13			
2 n'est pas possible car il reste	(4-3)!-1= 1-1= 0 redondance	13	2 devient 3 puis 4	**134**	**2**
		1342	←		
1 est possible car il reste	(4-1)!-4= 6-4= 2 redondances	1			
3 n'est possible car il reste	(4-2)!-2= 2-2= 0 redondance	1	3 devient 4	**14**	**23**
		1423	←		
1 est possible car il reste	(4-1)!-5= 6-5= 1 redondance	1			
4 est possible car il reste	(4-2)!-1= 2-1= 1 redondance	14			
2 n'est possible car il reste	(4-3)!-1= 1-1= 0 redondance	14	2 devient 3	**143**	**2**
		1432	←		

Figure 40 Méthode de génération de clés ordonnées.

Monde des permutations Ordonnées (page 237)

714-§ Nous savons de quelle façon nous obtenons les permutations de {1..η} éléments [ALG] par la théorie des groupes. Nous connaissons par notre faculté de penser quelle permutation succède logiquement par croissance ou décroissance à une autre permutation. Il nous est évident que par ordre croissant, la permutation 1243 succède à la permutation 1234 sans que pour autant nous connaissions les permutations précédentes et successives. Bien que cet exercice nous paraisse

extrêmement simple, nous n'avons pas mis en équation un système permettant de lire les permutations ordonnées précédentes ou suivantes d'une permutation quelconque.

715-§ Nous connaissons la méthode permettant d'obtenir la liste ordonnée des permutations de η éléments quand nous connaissons « l ' état initial »[499] de la permutation.

716-§ Notre méthode se doit de montrer la logique d'accroissement des ensembles de permutations ordonnés donc la caractéristique naturelle s'apparente à la croissance des organismes.

717-§ Nous montrons qu'à partir de cette simple règle d'ordre de permutation des éléments AB en BA, source de la symétrie, nous sommes en mesure de construire tout ensemble de permutations ordonnées en une seule équation conservant le contexte de position de chacune de ces permutations.

718-§ La solution que nous proposons repose sur l'étude des changements de positions de chaque élément de $\{1..\eta\}$.

719-§ Les séquences décrivant ces changements sont agrégées en une seule chaîne dont la caractéristique est d'être symétrique tout comme 123 l'est de 321. Il apparaît que cette chaîne est composée de répétitions de motifs que nous condensons en un programme $\Im_\eta$ de dimension inférieure [BRISS1991] à l'ensemble des permutations de $\{1..\eta\}$.

720-§ Nous montrons que la croissance de $\Im_\eta$ en un programme $\Im_{\eta+i}$ peut être décrite par des règles de réécritures, plus complexes qu'un L-système [LIND1968], appelé IL-système [PRUS1989].

Ordre structurel symétrique des permutations ordonnées

721-§ Un ensemble de permutations d'une factorielle n est déterminé en nombre par son cardinal $Card(\Im_\eta) = \eta!$ En ce sens, ce nombre n'est pas arbitraire et comme nous étudions les ensembles de permutations Ordonnées, nous nous attendons à voir apparaître quelque « notion vague de dessin équilibré » [WEYL1952]. Notre première étape consiste à découvrir cette structure.

722-§ Si nous considérons les permutations de 3! classées par ordre croissant nous obtenons la liste suivante des permutations ordonnées par ordre croissant: 123, 132, 213, 231, 312, 321. Organisons ces permutations dans une colonne du tableau de ci-dessous. La factorielle 3 est constituée de 3 colonnes (Cl, C2, C3) .

[499] La génération de permutations ordonnées peut être effectuée par le calcul de redondance, (h-1)! pour le premier élément (h-2)! pour le deuxième et ainsi de suite jusqu'à (h-i)!=0!, de chaque élément de {1..n}. Dans ce cas il est nécessaire de savoir quel est l'état de décrémentation de chaque (h-x)! , $x \in \{1..\eta\}$.

liste des permutations ordonnées de 3!				
positions				
c1	c2	c3		brins obtenus
1	2	3	Le 1 occupe les positions	1,1,2,3,2,3
1	3	2		
2	1	3	Le 2 occupe les positions	2,3,1,1,3,2
2	3	1		
3	1	2	Le 3 occupe les positions	3,2,3,2,1,1
3	2	1		

Tableau 18 Transformation d'une liste de permutations ordonnées en séquences de positions.

723-§ Chaque chaîne donnant les positions de chaque chiffre est appelée un «brin». La factorielle n est alors composée de η–brins[500]. La juxtaposition des brins {112323}, {231132}, {323211}, par la droite, décrit une « concaténation ». La liste des permutations ordonnées devient: {112323231132323211}. Nous découvrons un axe de symétrie 0 placé au milieu de cette chaîne: {1123232311 0 {132323211}. Nous constatons manuellement qu'il en est de même pour 4! dont la chaîne des positions est fac(4)={ 1 1 1 1 1 1 2 2 3 4 3 4 2 2 3 4 3 4 2 2 3 4 3 4 2 2 3 4 3 4 1 1 1 1 1 1 3 4 2 2 4 3 3 4 2 2 4 3 0 3 4 2 2 4 3 3 4 2 2 4 3 1 1 1 1 1 1 4 3 4 3 2 2 4 3 4 3 2 2 4 3 4 3 2 2 4 3 4 3 2 2 1 1 1 1 1 } et Il nous suffit de connaître l'une des deux parties, soit à droite de l'axe de symétrie $\varnothing$ soit à sa gauche, pour connaître la séquence totale des permutations.

724-§ Nous simplifions la lecture de la chaîne par des mises en facteur des positions {1..η} par les factorielles. Nous associons à chaque élément {1,2,3} de fac(3) un représentant {A,B,C} de valeur à la fois qualitative de position dans la permutation et aussi représentant d'un quantitatif de répétition. La chaîne est réécrite sous sa forme simplifiée[501]: **fac(3)=** {A + **3(B +** C) + A + 3(C + B) + A).

Contraintes régissant la transformation d'un ensemble $\Im_{\eta}$ en $\Im_{\eta+i}$

725-§ Après avoir mis en évidence un ordre structurel dans 3!, nous allons déterminer les « règles » où , « contraintes formelles » qui conditionnent la formation de $\Im_{\eta+1}$ à partir de $\Im_{\eta}$. La fonction de croissance d'une chaîne de position que nous appelons aussi « chaîne factorielle » est dépendante de règles structurelles fixes, de règles de transformations qualitatives et quantitatives. Nous devons commencer par établir la structure de la nouvelle chaîne décrivant $\Im_{\eta+i}$. Puis à partir de cette structure et selon la nature des séquences de motifs à construire dans $\Im_{\eta+1}$, nous appliquons des règles de transformations sur des séquences d'éléments issues de $\Im_{\eta}$.

[500]La factorielle du nombre 3 est formée de 3 brins.

[501] Du même constat, pour n = 4, nous obtenons la chaîne suivante, fac(4)= { A + 4 (B + 2 (C + D)) + A + 2 ((C + D) + B+ (D + C)) + ((C+ D) + B + (D + C)) 2 + A + ((D + C) 2 + B) 4 + A }, et pour n = 5, fac(5)= { A + 5 (B + 3 (C + 2(D + E))) + A + 5 (C + 2(D + E)) + B + 2 ((D + E) + C + (E + D))) + A + (((D + E) + C + (E + D)) 2 + B + ((E + D) 2 + C)) 5 + A + (((E + D) 2 + C) 3 + B) 5 + A }

726-§ Ces règles ne sont pas que qualitatives, certaines d'entre elles sont numériques et leurs valeurs dépendent du contexte dans lequel s'effectue leur calcul.

Structure globale d'une chaîne

727-§ Il existe deux formes de chaîne. La première forme constatée est de structure impaire, elle a pour centre le motif (η-l)! La deuxième forme est paire, elle n'a pas de motif pour centre. La chaîne est impaire pour tous η impair et est paire pour tous η pair. D'une façon générale, nous obtenons la « pyramide » des coefficients de blocs suivante:

η							∅						
1							A						
2					A	η/2	∅	η/2	A				
3					A	η	A	η	A				
4			A	η	A	η/2	∅	η/2	A	η	A		
5			A	η	A	η	A	η	A	η	A		
6	A	η	A	η	A	η/2	∅	η/2	A	η	A	η	A
7	A	η	A	η	A	η	A	η	A	η	A	η	A

Figure 41 Coefficient des blocs l-système de la GAPO.

728-§ Chaque nouveau bloc construit est factorisé par η excepté le bloc central d'une factorielle paire qui sera factorisé par η/2. Chaque chaîne de factorielle η comporte η séquence(s) de (η-1)! Motif(s) ici représentée(s) par 'A'. Ainsi 1! aura une et une seule séquence de (1-1)!=1 motif. Tandis que 4! aura 4 séquences de (4-1)!=3.2.1=6 éléments identiques.

Mutation et Substitution

729-§ Il existe deux règles essentielles gérant l'évolution des chaînes factorielles: la *« substitution »* et la *« mutation ».*

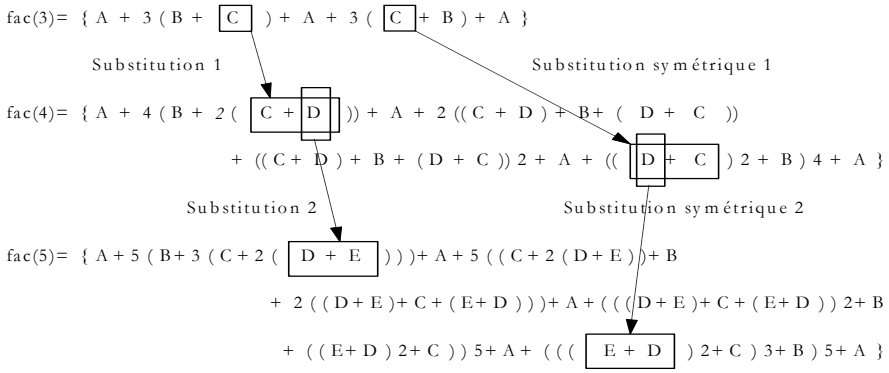
La mutation: nous appelons mutation, l'augmentation d'une unité de l'indice 1 de la factorielle (η-l)!A. Ainsi la mutation du motif 'A' est 'B' et celui de 'B' est 'C'. La conséquence d'une mutation sur un motif est « la conservation de la dimension du motif » A. Dans fac(η = 3), le motif 'B' est représenté (η-l)! = (3-2)! = 1 fois. Si nous incrémentons le motif 'B' dans une factorielle supérieure fac(η=4) alors 'B' augmenté devient 'C' et (η-l)!=(4-3)!= 1 fois. La dimension du motif ne change pas.

730-§ **La substitution:** nous appelons substitution, *le* remplacement du dernier motif d'une factorielle η! par un motif faisant apparaître la nouveauté de la factorielle immédiatement supérieure (η+ 1)!.

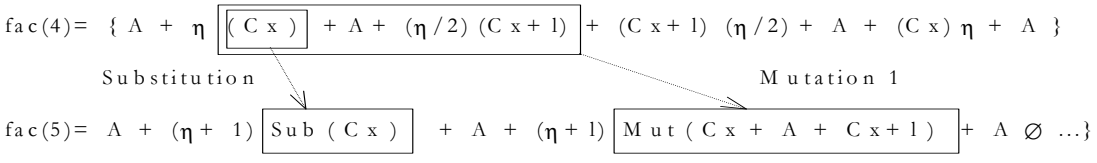
731-§ La substitution n'est effectuée que dans les deux groupes situés aux deux extrémités de la chaîne, entre le premier élément (η-l)!A et le deuxième élément (η-l)!A et symétriquement entre l'avant dernier élément (η-l)!A et le dernier élément (η-l)!A: nous appelons « bloc » l'intervalle entre deux (η-l)!A. Pour exemple, si nous désirons construire le premier bloc de la chaîne fac(η=4) à partir de la chaîne fac(η=3), nous devons substituer le dernier motif 'C' du premier bloc de fac(3) par le motif 'C + D'. Le premier bloc de fac(3) est 'B + C', il devient ' B + C + D ' dans le premier bloc de fac(4).

Règles structurelles de construction d'un bloc

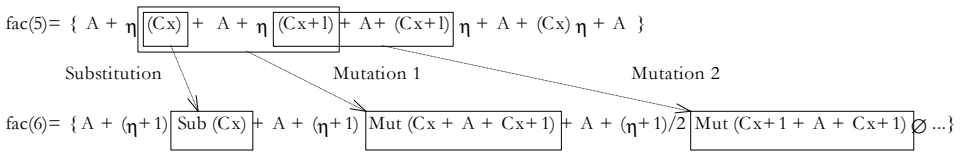
732-§ Le premier bloc et le dernier bloc de $\Im_{\eta+1}$ sont le résultat d'une substitution effectuée dans le premier bloc et le dernier bloc de $\Im_{\eta}$. Si fac(3)= { A + 3 (chaîne 1 + ... + C) + ... ∅ ... (C + ...+ chaîne l)3 + A }, alors fac(4)= { A + 4 (chaîne l + + C + D) + ... ∅ ... (D + C + ... + chaîne l) 4 + A }. La représentation des successions de substitutions entre les chaînes 3, 4, 5 factorielle prend cette forme :



733-§ Le caractère C est remplacé par le motif 2(C+D), puis le caractère D est lui-même remplacé par le motif 2(D+E). Le phénomène se produit symétriquement par rapport à la chaîne factorielle. Le caractère C est remplacé par le motif 2(D+C), puis le caractère D est remplacé par le motif 2(E+D). Tous les autres blocs sont obtenus par la mutation d'une séquence *«η (chaîne x) + A + η (chaîne x+1)»* de la factorielle précédente. La construction d'un bloc 'x' implique la mutation de la séquence (x - 1) + A + (x) de la factorielle précédente. Ainsi fac(3)= { A + η (chaîne 1) + A + (chaîne 2) η + A } se transforme en fac(4) = A + n (substitution (chaîne l)) + A + (η/2) (mutation (chaîne l + A + chaîne 2)) ∅ }. Remarquons que quand nous passons d'une factorielle paire à impaire, le dernier bloc impair, précédant la symétrie ∅, est donné par la mutation de la séquence de la factorielle précédente limitée par son centre de symétrie ∅. . Notons 'Sub' pour substitution et 'Mut' pour mutation;



Ainsi fac(5)= { A + η (Sub (Sub (chaîne l))) + A + η (Mut (Sub (chaîne l) + A + Mut (chaîne l + A + chaîne 2))) + A ∅ } , et



fac(6)={ A + η (Sub (Sub (Sub (chaîne 1)))) + A + η (Mut (Sub (Sub (chaîne 1)) + A + Mut (Sub (chaîne 1) + A + Mut (chaîne 1 + A + chaîne 2)) + η/2 (Mut (Sub (chaîne 1) + A + Mut (chaîne 1 + A + chaîne 2)) + (Mut (chaîne 2 + A + chaîne 1) + A + Sub (chaîne 1))) ∅...}.

734-§ Nous constatons que chaîne 1= { B + C } et chaîne 2= { C + B } sont à la source de la permutation ordonnée BC/CB.

Calculs des facteurs de répétitions de motifs

735-§ Nous l'avons vu, « deux blocs subissent une mutation pour créer un nouveau bloc ». Ces deux blocs ne sont pas développés dans les mêmes proportions: Le deuxième bloc croit en fonction unique de l'accroissement du premier bloc. Trois règles de calculs régissent le processus de pondération de chacun des deux blocs.

736-§ Les coefficients (η-Δ) placés entre le facteur η et le premier motif du premier bloc ne sont pas modifiés. Toutefois η augmentant d'une unité, les coefficients se trouvent être augmentés de cette même unité. Les autres coefficients (η-Δ) inférieur à η sont conservés à leur valeur[502]. Le premier coefficient, différent de η, du premier bloc, constitue l'élément de référence pour le calcul du facteur répétiteur du deuxième bloc. Si le premier coefficient intégré du premier bloc est α et qu'il ne s'agit pas de la construction d'un bloc central alors le facteur répétiteur[503] se calculera comme étant

$$Coefficient = \eta - \alpha - 2$$

Equation 16 Coefficient d'accroissement d'une sous chaîne de la GAPO.

737-§ Pour déterminer le coefficient du deuxième bloc, nous devons lire le premier coefficient[504] du premier bloc qui soit différent et inférieur à η. Si les trois conditions suivantes sont réunies: le bloc construit est le bloc central, η est impair et le coefficient à transformer est celui du deuxième bloc de

502

Bloc(x) dans fac(η-1)		Bloc(x+ 1) dans fac(h-1)	
Etat dans fac(h-1)	Etat dans fac(h)	Etat dans fac(h-1)	Etat dans fac(h)
((...	(2((...	((...	((...
(2((...	(3(2(...	(2((...	(2((...

Tableau 25 Transformation des facteurs de répétitions de motifs l-système.

503 Prenons un extrait de la chaîne 7 factorielle, fac(7)= {... + 7 ((C + 4 (D + 3 (E + 2 (F + G))))+ B + coefficient ((D + 3 (E + ...))))) + A +...}.

504 Le coefficient du premier bloc est '((' qui signifie 1, le deuxième coefficient se calcul donc comme étant h-α-2 = 7-1-2 = 4. L'extrait de 7! sera donc: fac(7)= {...+ 7 ((C + 4 ((D + 3 (E + 2 (F + G)))) + B + 4 ((D + 3 (E + ...))))) + A +...}.

la factorielle précédente fac(η-1) alors le coefficient du deuxième bloc subissant la mutation sera calculé[505] par le rapport (η-3)/2.

$$Coefficient = \frac{(\eta - 3)}{2}$$

Equation 17 Accroissement du coefficient du deuxième bloc subissant la mutation dans une GAPO.

738-§ Dans le cas où le bloc construit est le bloc central, que η est pair et que le coefficient η à transformer est celui du deuxième bloc du factoriel précédant; alors le coefficient se calcule comme étant la moitié[506] de η, soit η/2.

$$Coefficient = \frac{\eta}{2}$$

Equation 18 Coefficient de la chaîne centrale l-système de la GAPO.

Principe de lecture d'une chaîne

739-§ Nous rappelons que la chaîne décrivant n! englobe n sous-chaînes appelées « brins ». Chaque brin décrit la position des éléments de la permutation {1,2,3,4...,n}. Par définition, la première permutation de n! est la suite {1,2,3,4...,n}. Ainsi la première permutation de 4! est {1,2,3,4} et nous constatons que dans la permutation suivante le 4 prend la place du 3 et donne {1,2,**4,3**}. Nous lisons dans le brin n°4, dans la permutation {1,2,3,4}, le 4 occupe la 4ème place. Dans la permutation {1,2,4,3}, nous lisons que le 4 occupe la 3ème place: les deux premiers éléments du brin n°4 sont 4 et 3.

740-§ Le numéro de brin « Nb » dit que nous étudions les changements de positions de l'élément Nb appartenant à n. L'élément lu dans le brin Nb indique deux valeurs: -la première est la position de Nb dans la permutation, -la deuxième est le nombre de fois qu'apparaît successivement Nb à cette même

[505] Soit fac(4)= {...+ 4 (B + 2 (C +D)) + A + 2 ((C + D) + B + (D + C)) ∅ ((C + D) + B + (D + C)) 2 +...}, quel sera le coefficient de la mutation dans fac(5)= {... + Mut ((B + 2 (C + D)) + A + coefficient (2 ((C + D) + B + (D + C)))) ∅ +...}. Nous calculons ce coefficient par l'équation (h - 3) / 2 = (5 - 3) / 2 = 1. Le coefficient n'influence pas la répétition d'un motif puisqu'il est égal à l'unité. Nous ne le faisons pas apparaître dans la chaîne fac(5)= {... + 5 ((C + 2 (D + E)) + B + 2 ((D + E) + C + (E + D))) + A + (((D + E) + C + (E +...}

[506] soit fac(5)= {... + 5 ((C + 2 (D + E)) +...+ A +...+ ((E + D) 2 + C)) 5 + A ...} : la double parenthèse '((' montre un coefficient égal à l'unité, lors de la construction du bloc central de fac(6) ce coefficient est non intégré et sa valeur devient le 2 de la chaîne de ci-dessous. Le coefficient du bloc central est calculé comme étant la moitié de h. Ici comme n=6, alors le coefficient de bloc devient h/2=6/2=3 que nous plaçons comme facteur premier du bloc central de fac(6)= {... + 3 (2 ((D + 2 (E +...) ∅ (... + E) 2 + D)) 2) 3 +...}

position.

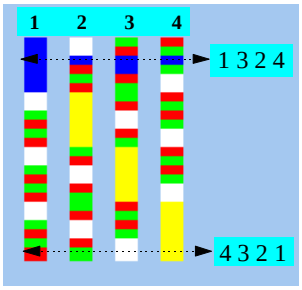
741-§ Ainsi, le premier élément du brin N°1=Nb est 'A'. Cet élément indique que la valeur Nb=1 est en position 'A' qui équivaut à 1, et ce, (n-1)! fois soit 3x2x1=6 fois, pour n=4. De même que le premier élément du brin N°2=Nb est 'B', ce qui signifie que la valeur Nb=2 est en position 'B' qui équivaut à 2, et ce toujours pour n=4, (n-2)! fois soit 2x1=2 fois.

Localisation d'un brin

742-§ La position de départ et de fin d'un brin appartenant à une chaîne sont établies par les constatations suivantes: l'élément 'A' et n(chaîneΔ) sont de dimension (n-1)! La position de départ du premier brin est le premier 'A' de la chaîne. Le point de fin se trouve à la terminaison de la longueur du brin: soit n! plus loin. La conséquence qui en découle est que la séquence du premier brin soit « A + (n-1) (chaine1) ». Implicitement, le deuxième brin commence la ou se termine le premier brin et il finit à la terminaison de la longueur du deuxième brin, soit encore une fois, n! plus loin. La partie n(chaine1) est consommée sur ses (n-1)/n part, il reste[507] donc une seule part de « n (chaine1) ».

La lecture en GAPO

743-§ La lecture en GAPO implique autant de points de lectures sur la chaîne qu'il existe de brins.



744-§ Il existe autant de position de lecture qu'il y a de brins: nous le constatons dans l'image du 4! (ci-contre), chaque élément de chaque brin est lu en termes de positions et de proportions. Ce recoupement de positions et de dimensions donne la permutation {1,2,3,4} pour la première position de chaque brin, {1,3,2,4} pour les motifs de positions {1,2,3,3} et la dernière permutation {4,3,2,1}. Nous ne construisons pas un algorithme de lecture par brin lu. Nous n'utilisons qu'un seul algorithme mais avec des variables dépendantes du brin qui est lu à un instant donné.

[507] Cette part représente une dimension de (n-1)! éléments. La position de fin implique la résolution de l'équation simple du premier degré (n-1)! + A + Δ = n! , Δ est forcément « (n-2)(chaine2) » au lieu de « n (chaine2) ». Le deuxième brin a pour séquence « 1(chaine1) + A + (n-2)(chaine2) ». Par généralisation: SI le brin est celui du centre ET que n est pair alors, l'équation « coef1 (chaîneX) + A + coef2 (chaîneX+1) » a pour solution: coef1 = Numéro de brin - 1 et coef2 = inchangé. Sinon l'équation « coef1 (chaîneX) + A + coef2 (chaîneX+1) » a pour solution coef1 = Numéro de brin - 1 et coef2 = n - numéro de brin.

Algorithme de construction

Etablir la structure de la chaîne selon la factorielle η et la pyramide.

Substitution

Ajouter au dernier motif, du premier et dernier bloc de la chaîne de la factorielle (η-1), le nouveau motif de η.

Mutation:

Soit ζ le numéro de la partie centrale de la factorielle η et ρ la partie à construire.

Tant que ρ est différent de ζ il faut faire:

-si ρ est le bloc central alors appliquons la règle de la pyramide sinon seul le facteur η est à appliquer.
-calculer la position δ de départ et la position de la 'fin' marquant le segment qu'il faut intégrer pour obtenir le nouveau bloc.
-prendre le coefficient du premier bloc de la chaîne de la factorielle précédente (η-1).
-entre δ jusqu'au début du deuxième bloc, intégrer les (η-i)Δ

Fin de lecture du premier bloc de fac(η-1)

-si ρ et ζ et η pair alors appliquer la **règle C**.
autrement
-si ρ est ζ et η impair alors appliquer la **règle B**.
autre si ρ n'est pas ζ et quelque soit la parité alors appliquer la **règle A**.

Fin de lecture du deuxième bloc de fac(η-1)

Fin de la réécriture du bloc ρ de fac(η)

ρ est augmenté d'une unité

Fin si ρ est ζ

Figure 42 Algorithme L-système de la GAPO .

Algorithme de lecture en GAPO

Initialisation des transpositions:
transposition[]={1,2,3,...n}

Faire de Δ=1 à Δ=n Nous lisons n fois le premier factoriel de (n-1).

Initialiser les classes objets et les variables.

Faire de 1 à factoriel de (n-1)

Faire de p=1 à p=n

Si la valeur de l'élément en position p est nulle Alors il faut rechercher le motif suivant ce qui fournit une nouvelle valeur de l'élément.

Décrémenter la valeur de l'élément en position p.

Visualiser la permutation en tenant compte du fait que:
1. l'élément (E) lu dans le brin (B) indique que (B) est en position (E) dans Permutation[], (E-1)! fois.
2. ET que cette position est dépendante de la transposition. Nouvelle_position [Permutation [transposition [p]]] = p.
3. afficher la permutation contenue dans Nouvelle_position[].

fin de faire.

fin de faire.

Intervertir la position Δ et la position Δ+1 de transposition[].

fin de faire.

Figure 43 Algorithme de lecture GAPO.

Diversification des chemins d'inclusions (page 258)

Texte sans voyelle	Nchemin/taille fichier
criton1.txt	0,00909475
criton3.txt	0,00908769
criton2.txt	0,00735846
ODYS1.TXT	0,00620849
VMS408C.TXT	**0,00615411**
PD_2.TXT	0,00593186
MICROMEG.TXT	0,00540062
CHIMES.TXT	0,00516685
VMS408F.TXT	**0,00498179**
ILIAD01.TXT	0,00483311
ANTIGONE.TXT	0,00474515

Texte avec voyelle	Nchemin/taille fichier
VMS408C.TXT	**0,00615411**
VMS408F.TXT	**0,00498179**
criton1.txt	0,00274958
criton2.txt	0,00225259
criton3.txt	0,00177033
CHIMES.TXT	0,00165676
MICROMEG.TXT	0,00160331
PD_2.TXT	0,00160321
ANTIGONE.TXT	0,00151951
PIT.TXT	0,00145647
OEDIPU1.TXT	0,00139306

Tableau 19 Proportion de chemins par texte (Equation 15)

Symétries et redondances dans MS408 (page 254)

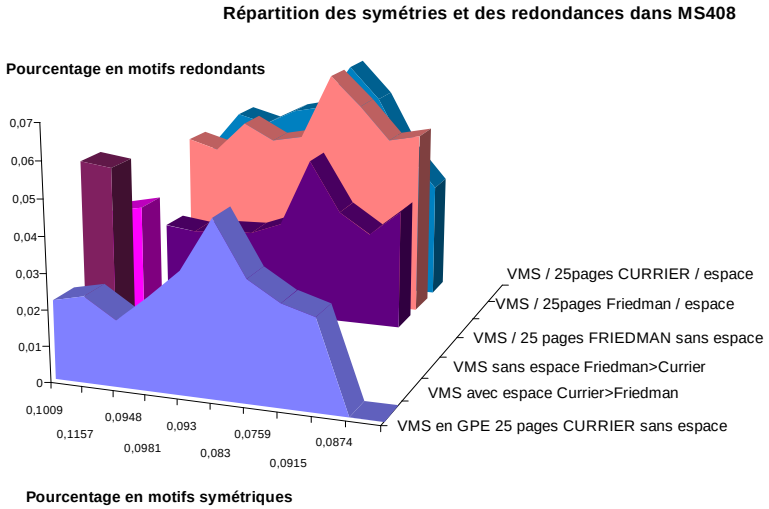


Tableau 20 Symétrie et redondance par groupe de 25 pages de MS408.

Table des transitions trigrammiques sans espace (page 129)

La première colonne contient les deux premières lettres du trigramme, la première ligne du tableau contient la troisième lettre du trigramme. A chaque fois que la première lettre du trigramme change, un nouveau tableau se crée dont la première ligne contient la troisième lettre du trigramme. Chaque nombre est à diviser par 10000 pour retrouver la valeur réelle de la probabilité : (DM=10000).

	2	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
22	0	370	0	0	0	4814	370	0	0	0	740	0	0	0	0	0	370	2592	0	0	740	0	0	0
24	0	0	0	0	0	0	0	377	0	0	0	188	0	0	0	0	0	9433	0	0	0	0	0	0
26	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	344	0	0	0	4137	172	0	344	0	1724	0	0	0	0	0	0	1379	0	0	689	1206	0	0
2A	13	0	0	26	0	13	0	13	1717	0	39	53	825	252	39	4766	159	13	0	2050	13	0	0	0
2C	0	0	238	1190	0	476	2619	476	0	0	2619	476	0	0	0	0	0	952	0	0	238	714	0	0
2D	0	0	0	0	0	2777	833	0	0	0	833	0	0	0	0	0	0	277	0	0	0	1388	0	3888
2E	454	0	0	0	0	2727	0	1818	0	0	0	454	0	0	0	0	0	1818	0	0	454	2272	0	0
2F	0	0	0	0	0	2000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4000	2000	0	2000
2G	1125	500	0	687	0	125	62	2125	250	62	562	1062	0	0	0	0	0	1000	250	0	625	1562	0	0
2H	0	0	0	0	0	714	714	0	0	0	0	0	0	0	0	0	0	1785	0	0	0	2142	0	4642
2K	0	3333	0	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0	0	0
2L	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2M	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2N	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	0
2O	266	0	0	590	0	342	247	1219	3409	57	171	838	76	76	19	400	19	57	95	1809	171	114	19	0
2P	0	0	0	454	0	909	0	454	0	0	454	0	0	0	0	0	0	2272	0	0	454	3181	0	1818
2R	606	0	0	303	0	3636	0	0	0	0	1515	303	0	0	0	0	0	2727	0	0	303	606	0	0
2S	0	0	0	86	0	260	6782	86	0	0	434	173	0	0	0	0	0	2086	0	86	0	0	0	0
2T	45	0	0	181	0	545	5000	227	0	0	590	181	0	0	0	45	0	3000	136	45	0	0	0	0
2Z	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0

	6	E	H
36	0	DM	0
3C	DM	0	0
3G	0	0	DM

	2	4	8	A	C	D	E	F	G	H	I	L	M	N	O	P	R	S	T	Z
42	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
46	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0
48	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0
4A	0	0	0	1666	0	0	1666	0	0	0	1666	0	3333	0	1666	0	0	0	0	0
4C	0	0	256	0	3333	1794	0	256	256	1794	0	0	0	0	1794	512	0	0	0	0
4D	0	0	0	1500	2250	0	0	0	0	0	0	0	0	0	1500	0	0	250	750	3750
4E	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	5000	0	0	0	0	0
4G	0	0	0	0	0	5000	0	0	0	1250	0	0	0	0	1250	0	1250	0	1250	0
4H	0	0	0	3333	1111	0	0	0	0	0	0	0	0	0	555	0	0	0	555	4444
4L	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4O	17	17	242	108	215	6046	493	71	27	2184	11	3	7	1	75	327	71	13	61	0
4P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0	6666
4R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
4T	0	0	0	0	4000	0	0	0	0	0	0	0	0	0	6000	0	0	0	0	0

	2	3	6	F	H
69	5000	0	5000	0	0
6E	2000	2000	2000	2000	2000
6H	0	3333	6666	0	0

	C	E	R
7A	0	0	DM
7G	0	DM	0
7S	DM	0	0

	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
82	606	0	606	2121	0	606	0	0	606	0	0	0	0	0	0	3939	0	0	0	1515	0	0
84	0	0	0	0	168	84	0	0	0	0	0	0	0	0	0	9747	0	0	0	0	0	0
87	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	0	0	0	3823	0	147	1029	147	2205	0	0	0	0	0	0	735	0	0	882	1029	0	0
8A	10	16	32	8	0	19	1788	0	8	8	753	499	65	4347	436	30	5	1952	5	10	0	0
8C	99	99	792	198	6435	99	0	99	1386	99	0	0	0	0	0	594	0	0	0	99	0	0
8D	0	0	0	1951	1951	0	0	0	1219	0	0	0	0	0	0	975	0	0	1219	975	0	1707
8E	642	183	550	1009	183	1192	642	0	642	183	0	0	0	0	0	917	366	458	917	2110	0	0
8F	0	0	2500	5000	0	0	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	0
8G	300	3179	849	95	23	306	505	25	362	427	1	7	1	1	0	1802	247	165	528	1167	1	0
8H	0	0	0	500	1000	500	0	0	500	0	0	0	0	0	0	2500	0	0	500	2000	0	2500
8I	0	0	0	0	0	0	0	0	2000	0	4000	0	0	2000	0	0	0	2000	0	0	0	0
8K	1333	1333	666	0	0	0	0	0	2000	2666	0	0	0	0	0	1333	0	0	0	666	0	0
8L	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0
8M	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	2500	0	0	0	5000	0	0
8N	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0
8O	60	60	480	220	120	721	4028	20	40	761	100	200	0	300	20	40	160	2505	80	80	0	0
8P	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	833	5833	0	833
8R	0	588	0	3529	0	0	588	588	588	588	0	0	0	0	588	1176	0	0	588	1176	0	0
8S	0	0	402	251	6130	50	0	0	653	0	0	0	0	0	0	2261	0	0	0	251	0	0
8T	109	0	464	573	3825	245	27	0	1584	54	27	27	0	0	0	2868	81	54	27	27	0	0

	6	8	E	G	O	R
92	DM	0	0	0	0	0
96	0	0	DM	0	0	0
98	0	0	0	DM	0	0
9A	0	5000	0	0	0	5000
9G	0	0	0	0	DM	0

	2	4	6	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
A2	444	444	0	222	1555	0	444	222	0	1111	222	0	0	0	0	0	2666	222	222	888	1333	0	0
A4	0	0	1538	0	0	769	0	0	0	769	0	0	0	0	0	0	6923	0	0	0	0	0	0
A8	0	103	0	309	3814	206	0	103	0	4329	0	0	0	0	103	0	412	0	0	206	412	0	0
A9	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AA	0	0	0	0	0	0	0	2500	0	0	0	0	1666	833	1666	0	0	0	3333	0	0	0	0
AC	0	0	0	714	0	4285	2142	0	0	714	0	714	0	0	714	0	714	0	0	0	0	0	0
AD	0	0	0	0	3164	1392	0	0	0	2025	126	126	0	0	126	0	886	0	0	0	506	0	1645
AE	468	597	0	1385	590	26	700	296	45	963	251	3	19	0	0	0	1838	106	102	970	1629	3	0
AF	0	0	0	2500	0	0	0	1250	0	0	0	0	0	0	0	0	0	0	0	0	1250	0	5000
AG	606	1212	0	909	606	303	1818	303	303	0	1515	0	0	0	0	0	909	0	0	606	909	0	0
AH	0	0	0	0	1842	1052	0	0	0	789	0	0	0	0	0	0	1578	0	0	263	526	0	3947
AI	130	13	0	78	26	13	117	286	0	26	39	1382	586	104	573	13	13	26	6453	26	78	13	0
AK	1106	732	0	1451	244	28	143	129	57	1479	775	0	28	0	0	0	1810	416	86	502	991	14	0
AL	1149	1149	0	1149	574	0	344	0	0	1379	344	0	0	0	114	0	1724	0	114	574	1379	0	0
AM	211	796	0	747	393	28	172	88	28	524	364	12	14	2	2	436	2646	187	26	1193	2119	2	0
AN	319	490	0	1215	298	21	298	170	42	511	533	0	42	21	575	0	1918	191	277	938	2132	0	0
AO	128	128	0	512	128	128	1282	2820	0	128	641	512	897	0	128	0	0	384	2179	0	0	0	0
AP	0	0	0	0	0	625	0	0	0	1250	0	0	0	0	0	0	625	0	0	625	3125	0	3750
AR	163	509	0	442	2332	48	135	122	34	735	170	20	13	3	24	3	2594	87	48	1000	1495	10	0
AS	0	0	0	909	909	0	909	0	0	1818	0	0	0	0	0	0	5454	0	0	0	0	0	0
AT	0	0	0	1176	588	2352	1176	588	0	1176	0	0	0	0	0	0	1764	0	588	0	588	0	0
AV	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AW	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	
AY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	
	2	4	7	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	V	Z
C2	67	303	0	437	0	2188	538	202	235	67	1313	235	0	67	33	0	0	2626	134	134	505	909	0	0
C4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0
C6	0	0	0	0	5000	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C7	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0
C8	19	123	2	21	0	1033	46	23	51	2	8406	8	0	4	0	0	0	151	4	6	36	59	0	0
C9	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CA	218	21	0	436	0	0	43	196	2882	0	218	87	109	720	65	1135	131	87	0	3602	0	21	21	0
CC	426	6	0	3067	0	222	692	194	4	16	3787	94	4	16	32	6	2	1289	11	27	20	74	0	0
CD	19	19	0	38	0	1714	1348	0	57	0	2658	77	0	0	0	0	0	327	0	0	134	712	0	2890
CE	909	0	0	1818	0	1818	0	0	2727	0	909	0	0	0	0	0	0	909	0	0	909	0	0	0
CF	0	277	0	0	0	1944	0	0	0	0	2777	0	0	0	0	0	0	1111	0	0	277	3055	0	555
CG	317	2582	0	905	0	88	16	720	892	41	256	643	0	2	0	0	0	1640	215	295	430	950	0	0
CH	43	43	0	43	0	1471	1082	43	0	0	2813	0	0	0	0	0	0	173	0	0	216	822	0	3246
CI	1250	0	0	0	0	0	1250	0	1250	0	0	0	2500	1250	0	0	0	0	0	2500	0	0	0	0
CJ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0
CK	1111	1111	0	1111	0	555	555	555	555	0	555	1111	0	0	0	0	0	1111	0	0	1666	0	0	0
CL	0	666	0	666	0	0	0	666	0	0	666	0	0	0	0	0	0	3333	0	0	0	4000	0	0
CM	2000	0	0	0	0	1000	0	0	0	0	0	0	0	0	0	0	0	3000	0	0	3000	1000	0	0
CN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0
CO	561	88	0	2791	3	227	58	524	3367	25	99	264	11	110	0	7	0	124	80	1478	33	143	0	0
CP	135	0	0	270	0	1891	135	0	0	135	1081	135	0	0	0	0	0	810	0	0	270	3918	0	1216
CR	769	384	0	384	0	1538	769	384	384	0	1153	0	0	0	0	0	0	1923	0	0	769	1538	0	0
CS	204	0	0	1632	0	612	2448	0	0	0	3673	0	0	0	0	0	0	1428	0	0	0	0	0	0
CT	0	0	0	1474	0	64	2884	128	0	0	3974	0	0	0	0	0	0	1346	0	0	128	0	0	0
CZ	0	0	0	6666	0	0	0	0	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	4	8	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	Z		
D2	0	0	0	6000	0	0	0	0	2000	0	0	0	0	0	0	0	2000	0	0	0	0	0		
D4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0		
D8	0	0	0	3333	0	0	0	0	5833	0	0	0	0	0	0	0	0	0	0	0	833	0		
DA	35	3	43	7	17	14	1992	10	10	3	458	0	376	60	4494	516	43	0	1892	3	14	0		
DC	23	0	1865	167	5580	5	2	2	745	2	5	2	2	0	2	0	1284	0	2	79	218	2		
DD	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
DE	0	0	1176	1176	0	294	882	0	1176	0	0	0	0	0	0	0	1470	294	0	588	2941	0		
DF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	5000		
DG	453	1283	1752	105	30	332	604	15	422	407	0	0	0	0	0	0	1691	166	211	876	1646	0		
DH	0	0	0	3125	2812	0	0	0	625	0	0	0	0	0	0	0	937	0	0	625	1562	312		
DI	1666	0	0	0	0	0	0	0	0	0	6666	0	0	0	0	0	0	0	1666	0	0	0		
DK	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0		
DM	0	0	0	2500	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	2500	2500	0		
DO	102	68	1164	325	136	342	4589	51	136	119	68	0	119	0	325	17	85	17	2123	68	136	0		
DR	0	0	0	7500	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
DS	47	47	896	377	4716	0	0	0	1981	0	0	0	0	0	0	0	1792	0	0	0	141	0		
DT	49	0	1495	386	3366	9	9	9	2267	0	0	0	0	0	0	0	2336	19	19	19	0	9		
DZ	32	0	353	428	2700	10	10	21	5219	0	0	0	0	0	0	0	1125	0	0	32	64	0		
	2	3	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	W	Y	Z
E2	281	0	312	125	3875	187	156	62	31	781	218	0	0	0	0	0	2218	125	62	562	968	0	0	31
E3	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E4	0	0	0	0	0	43	151	21	0	21	21	0	0	0	0	0	9739	0	0	0	0	0	0	0
E6	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0
E8	56	0	56	66	5260	47	18	113	0	2876	28	18	47	0	9	0	766	18	0	236	378	0	0	0
E9	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EA	21	0	21	64	21	43	64	1831	0	0	0	646	732	43	3857	387	86	0	2112	0	43	21	0	0
EC	151	0	0	0	151	7424	909	0	151	0	454	0	0	151	0	0	606	0	0	0	0	0	0	0
ED	0	0	0	7	3350	4445	0	104	0	528	14	14	0	0	7	0	290	0	7	230	826	0	0	171
EE	259	0	0	432	519	86	3376	86	86	129	259	0	43	0	0	0	1731	173	173	649	1991	0	0	0
EF	0	185	0	185	740	0	185	0	185	370	0	0	0	0	0	0	1296	0	0	370	4629	0	0	1851
EG	760	0	816	1354	204	18	1447	241	74	426	1410	0	0	0	0	0	871	278	111	723	1243	0	18	0
EH	0	0	0	32	1941	2394	0	32	0	194	0	0	0	0	0	0	776	0	0	485	1747	0	0	2394
EI	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0
EK	1538	0	3076	2307	0	0	0	0	769	769	769	0	0	0	0	0	769	0	0	0	0	0	0	0
EL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0
EM	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EO	170	0	63	533	163	163	1997	2771	21	63	1613	49	191	7	71	0	49	248	1698	42	78	0	0	0
EP	0	0	0	88	884	0	0	0	0	442	88	0	0	0	0	0	1238	0	0	353	5132	0	0	1769
ER	101	0	101	202	6060	0	0	0	101	101	202	0	0	0	0	0	2020	0	0	303	808	0	0	0
ES	100	0	0	478	278	6469	167	44	0	467	100	0	0	0	0	0	1848	11	0	11	22	0	0	0
ET	74	0	0	693	452	5727	217	97	11	435	154	5	11	0	5	0	2004	51	17	22	17	0	0	0
EY	0	0	2500	0	2500	0	0	0	0	2500	0	0	0	0	0	0	2500	0	0	0	0	0	0	0
	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	R	S	T	Z					
F2	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
F3	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0					
F4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0					
F8	0	0	0	4444	1111	0	0	0	3333	0	0	0	0	0	0	0	1111	0	0					
FA	0	0	517	0	0	0	1551	0	0	0	1206	862	1896	344	0	3448	0	172	0					
FC	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
FD	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	2500	2500	2500					
FE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0					
FF	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
FG	0	740	1111	370	0	370	0	0	1851	370	0	0	0	0	740	0	2222	2222	0					
FH	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0					
FK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
FN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0					
FO	217	0	869	434	217	217	5434	0	0	0	0	0	217	0	0	1521	0	869	0					
FP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0					
FS	0	0	555	0	5000	0	0	0	1111	0	0	0	0	0	3333	0	0	0	0					
FT	125	0	1312	312	4500	0	0	62	1062	62	0	62	0	0	2437	0	0	62	0					
FZ	133	0	666	933	2400	0	133	0	4000	0	0	0	0	0	1600	0	0	133	0					
	2	4	7	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	X	Y	Z
G2	74	111	0	148	4740	0	74	18	0	518	92	0	18	0	0	0	2759	55	37	425	925	0	0	0
G4	5	2	0	0	11	94	39	2	0	13	25	0	0	0	0	0	9779	16	2	0	5	0	0	0
G8	18	37	0	50	6306	125	75	87	0	1218	18	12	12	6	0	0	822	12	6	395	791	0	0	0
GA	66	0	0	66	0	66	397	1986	0	66	264	662	264	0	2119	198	331	0	3311	66	66	0	66	0
GC	285	285	0	285	0	4000	857	285	285	285	857	0	0	0	0	0	571	1714	0	0	285	0	0	0
GD	16	0	0	16	2256	3355	8	33	0	464	76	0	0	0	0	0	980	0	8	405	1817	0	0	557
GE	120	36	0	506	325	48	3051	108	72	180	289	0	12	0	0	0	1254	108	120	1061	2689	0	12	0
GF	0	0	0	153	1384	307	0	0	0	153	0	0	0	0	0	0	1384	0	0	461	5076	0	0	1076
GG	73	18	0	351	92	18	3419	73	92	0	2865	0	0	0	0	0	277	573	18	794	1330	0	0	0
GH	8	8	0	41	2078	2303	8	0	8	475	0	0	0	0	0	0	1252	0	0	450	1911	8	0	1444
GI	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GK	1111	2222	0	2222	0	0	0	1111	0	1111	0	0	0	0	0	0	1111	0	0	1111	0	0	0	0
GL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0
GM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	5000	0	0	0	0
GN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0
GO	44	32	4	182	117	117	3257	1709	109	40	3131	0	8	0	12	0	24	528	552	36	89	0	0	0
GP	24	0	0	246	738	49	0	0	73	197	24	24	0	0	0	0	1945	0	0	591	4827	0	0	1256
GR	0	70	0	35	4840	70	70	70	35	424	0	0	0	0	0	0	2049	70	0	777	1484	0	0	0
GS	34	22	0	433	273	5256	627	34	34	376	296	0	0	0	0	0	2531	34	11	11	22	0	0	0
GT	43	5	0	464	356	4689	675	32	32	329	388	0	0	0	0	0	2879	54	5	21	16	0	5	0
GY	5000	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z	
H2	0	0	0	0	0	8000	0	0	0	0	2000	0	0	0	0	0	0	0	0	0	0	0	0	

H3	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H4	0	0	0	0	0	0	0	0	0	0	2000	0	0	0	0	0	0	8000	0	0	0	0	0
H6	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H8	0	0	0	500	0	5000	0	0	0	0	2000	500	0	500	0	0	0	1000	0	0	0	500	0
HA	27	6	0	55	0	6	13	27	2329	6	20	0	489	640	41	3563	206	41	13	2494	13	0	0
HC	43	0	0	2793	7	215	4204	0	7	0	849	0	0	7	0	7	0	1670	0	7	14	165	7
HD	0	0	0	0	0	3333	4166	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1666	833
HE	0	0	0	0	0	1818	909	0	909	0	0	0	0	0	0	0	0	1818	0	909	909	2727	0
HF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM
HG	352	1408	0	1830	0	70	23	375	469	23	446	492	0	0	0	0	0	1807	140	187	798	1572	0
HH	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0
HM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0
HO	157	0	0	1491	0	280	140	333	4350	70	157	263	35	70	35	228	0	17	35	2035	122	175	0
HP	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	5000
HR	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HS	112	0	0	1067	0	337	4494	0	56	0	1179	56	0	0	0	0	0	2640	0	0	0	56	0
HT	64	0	0	1161	0	483	3311	10	10	0	2161	32	0	21	0	0	0	2720	0	0	0	21	0
HX	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0
HZ	83	10	0	313	0	794	2246	0	10	0	3991	10	0	0	0	0	0	2445	0	20	31	41	0

	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	P	R	S	T	Y	Z
I2	0	0	0	4117	0	0	588	0	588	0	0	0	0	0	1764	0	1764	588	588	0	0
I4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0
I8	0	0	1000	2000	0	0	0	0	7000	0	0	0	0	0	0	0	0	0	0	0	0
IA	0	0	5000	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IC	4000	0	2000	0	4000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ID	0	0	0	833	1666	0	0	0	1666	0	0	0	0	0	0	0	0	0	833	0	5000
IE	714	714	2500	0	0	357	0	0	714	0	0	357	357	0	2142	0	0	357	1785	0	0
IG	0	0	0	0	0	0	0	0	0	2000	0	0	0	0	6000	2000	0	0	0	0	0
IH	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	5000
II	187	0	125	0	0	0	312	0	0	62	1312	750	62	750	62	0	6312	62	0	0	0
IK	344	862	1034	517	0	517	0	172	1034	517	0	172	172	0	1896	0	172	1034	1551	0	0
IL	0	1111	0	1111	0	0	0	0	0	1111	0	0	0	1111	2222	1111	0	1111	1111	0	0
IM	468	781	1406	468	0	0	0	0	468	156	0	0	0	0	2656	312	0	1250	2031	0	0
IN	0	0	1428	0	0	0	714	0	0	0	0	0	0	0	1428	0	5000	714	714	0	0
IO	0	0	2500	0	0	0	0	2500	0	2500	0	0	0	0	0	0	0	0	2500	0	0
IP	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IR	146	456	325	1644	48	195	195	32	879	146	97	16	65	81	3192	97	48	960	1351	16	0
IS	0	0	5000	0	2500	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0
IT	0	0	0	1666	1666	0	0	0	5000	0	0	0	0	0	1666	0	0	0	0	0	0
IY	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	T																				
JR	DM																				

	2	4	8	A	C	D	E	F	G	H	I	K	L	M	O	P	R	S	T	Z
K2	98	98	0	5196	0	196	0	0	294	0	0	0	0	0	3137	0	98	392	490	0	
K4	0	0	0	0	0	112	0	0	0	0	0	0	0	0	9775	0	0	0	112	0	
K8	0	206	137	4620	68	0	0	0	758	68	0	0	0	68	482	0	68	1310	2206	0	
KA	0	0	0	0	0	0	1739	0	0	0	434	2608	434	0	869	0	3913	0	0	0	
KC	0	0	0	0	3333	0	3333	0	0	3333	0	0	0	0	0	0	0	0	0	0	
KD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5294	0	0	588	4117	0	
KE	0	0	769	1538	0	2307	0	0	0	769	0	0	0	0	769	0	769	2307	769	0	
KF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1666	0	0	1666	6666	0	
KG	72	0	291	218	0	1897	0	0	0	2189	0	0	0	0	437	145	72	1751	2919	0	
KH	0	0	129	1948	779	0	0	0	0	0	0	0	0	0	2207	0	0	649	2987	1298	
KK	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0	0	0	0	0	3333	0	
KM	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	
KO	0	0	617	617	280	2808	1629	0	56	2247	0	168	0	0	56	112	898	280	224	0	
KP	0	0	540	810	0	0	0	0	0	0	0	0	0	0	2972	0	0	810	4594	270	
KR	1428	0	0	2857	0	0	0	0	0	0	0	0	0	0	2857	0	0	1428	1428	0	
KS	0	0	153	1076	4153	0	0	0	153	0	0	0	0	0	4461	0	0	0	0	0	
KT	0	0	792	891	3069	396	99	99	495	396	0	99	0	0	3564	0	0	0	99	0	
KY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	

	2	4	8	A	C	D	E	F	G	H	K	L	O	P	R	S	T	Z
L2	0	0	0	4545	0	0	0	0	0	0	0	0	3636	0	909	0	909	0
L4	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
L8	0	769	0	6923	0	0	769	0	769	0	0	0	769	0	0	0	0	0
LA	1666	0	0	0	0	0	1666	0	0	1666	1666	1666	0	0	1666	0	0	0
LD	0	0	0	0	2000	0	0	0	2000	2000	0	0	0	0	0	2000	2000	0
LE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0
LG	0	0	0	0	714	3571	0	0	714	2142	0	0	0	0	0	2857	0	0
LH	0	0	0	0	2500	0	0	0	0	0	0	0	2500	0	0	2500	0	2500
LI	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LM	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LN	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LO	0	0	1600	0	0	800	3600	0	400	2400	0	0	0	800	0	0	400	0
LP	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	5000	0
LR	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0
LS	0	0	0	1111	1111	1111	0	0	1111	0	0	0	5555	0	0	0	0	0
LT	0	0	434	2173	3043	434	0	434	434	434	0	0	2608	0	0	0	0	0

	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
M2	88	176	265	3539	0	0	88	0	1061	88	0	0	0	0	0	3274	88	88	265	973	0
M4	0	0	0	0	0	223	0	0	0	49	0	0	24	0	0	9676	0	0	0	24	0
M8	50	25	0	6481	177	75	202	0	1063	50	0	25	0	0	0	860	0	25	379	582	0
MA	50	0	100	0	50	300	4050	0	0	100	400	750	50	550	400	150	50	3000	0	0	0
MC	714	0	0	714	2142	714	714	0	0	3571	0	0	0	0	0	714	0	0	0	714	0
MD	114	0	0	1034	344	0	0	0	114	114	0	0	0	0	0	804	0	0	1379	1609	4482
ME	697	0	697	465	0	3488	0	0	697	0	0	0	0	0	0	1860	232	232	697	930	0
MF	0	0	0	625	0	0	0	0	0	0	0	0	0	0	0	1875	0	0	625	4375	2500
MG	109	72	654	72	36	3054	181	109	181	2909	0	0	0	0	36	436	436	36	218	1454	0
MH	0	0	106	374	427	0	0	0	53	0	0	0	0	53	0	1336	0	0	588	802	6256
MI	0	0	0	0	0	0	0	0	1666	0	1666	0	0	0	0	0	0	6666	0	0	0
MK	2500	0	1250	0	0	0	0	0	2500	1250	0	0	0	0	0	1250	1250	0	0	0	0
ML	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0
MM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
MN	94	1037	94	1037	0	0	235	0	377	235	0	0	0	0	0	2405	330	0	943	3207	0
MO	29	51	369	140	103	2968	2319	110	22	2843	0	7	0	7	0	36	332	583	7	59	7
MP	0	0	312	520	0	0	0	208	312	0	0	0	0	0	0	2916	0	0	625	2291	2812
MR	0	0	625	3750	625	0	0	0	2500	0	0	0	0	0	0	1875	0	0	0	625	0
MS	0	32	96	466	5916	819	32	0	321	289	0	0	0	0	0	1977	16	0	0	32	0
MT	36	0	341	507	4907	1116	119	18	212	461	0	0	0	0	0	2103	147	18	9	0	0
MY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0

	2	4	8	A	C	D	E	F	G	H	I	K	L	M	O	P	R	S	T	Z
N2	0	0	0	2941	588	1176	0	0	0	588	0	0	0	0	4117	0	0	0	588	0
N4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
N8	0	0	476	6666	317	0	0	0	1269	0	0	0	0	0	0	0	158	158	952	0
NA	0	0	0	0	0	256	3846	0	0	0	512	256	256	1794	0	0	3076	0	0	0
NC	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ND	0	0	0	2142	2142	0	0	0	714	0	0	0	0	0	0	0	0	0	0	5000
NE	0	0	714	714	0	1428	714	0	1428	0	0	0	0	0	2857	0	0	714	1428	0
NF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0
NG	312	312	312	0	0	3437	0	312	312	1562	0	312	0	312	937	0	0	625	1250	0
NH	0	0	0	1666	1000	0	0	0	666	0	0	0	0	0	1000	0	0	666	1000	4000
NK	0	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0	0	0	0	3333	0
NL	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0
NM	370	740	1111	0	0	0	0	0	2222	740	0	0	0	0	2222	370	0	1111	1111	0	

NO	68	0	408	272	0	2857	1904	68	136	3061	0	0	0	68	68	272	748	0	68	0		
NP	0	0	0	1176	0	0	0	588	588	0	0	0	0	0	1764	0	0	588	2941	2352		
NR	0	0	0	2857	0	0	476	0	1428	0	0	0	0	0	1904	0	0	952	2380	0		
NS	0	0	149	597	6119	895	0	0	149	298	0	0	0	0	1641	0	0	0	149	0		
NT	0	0	340	965	5170	1363	113	170	170	625	0	0	0	0	1079	0	0	0	0	0		
	2	4	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
O2	168	532	364	0	2857	112	280	168	28	532	112	0	0	0	28	0	1848	168	336	812	1652	0	0
O4	0	0	190	0	95	0	95	0	0	0	285	0	0	0	0	0	9333	0	0	0	0	0	0
O7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0
O8	44	149	109	0	3514	169	54	149	9	4870	19	0	4	0	0	0	393	9	34	149	314	0	0
O9	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OA	136	54	191	0	27	0	301	1726	0	136	82	465	164	27	3178	438	136	54	2876	0	0	0	0
OC	137	0	655	0	310	5482	1172	34	172	344	379	34	34	0	68	0	689	310	0	34	137	0	0
OD	1	3	10	0	3216	3948	0	21	3	588	19	5	1	0	3	0	631	0	3	171	1003	0	365
OE	305	583	1216	1	455	99	1525	213	65	483	413	1	9	1	0	0	1428	129	97	1004	1957	3	0
OF	67	134	201	0	1812	0	67	0	0	671	0	0	0	0	0	0	1073	67	0	402	4429	0	1073
OG	612	748	680	0	204	0	2176	136	68	204	1428	0	0	0	0	0	1020	340	272	952	1156	0	0
OH	8	8	29	0	3014	2853	26	20	0	796	0	2	0	0	0	0	868	5	2	208	1614	0	538
OI	227	0	0	0	0	454	227	0	0	0	0	2954	0	0	4090	0	0	0	1818	227	0	0	0
OK	802	1234	1543	0	123	0	185	123	0	987	617	0	0	0	0	0	1790	432	0	1111	1049	0	0
OL	833	833	1666	0	0	0	0	0	0	0	0	833	0	0	0	0	833	833	0	833	3333	0	0
OM	279	419	1048	0	279	0	139	0	0	629	349	0	69	0	0	0	2447	139	209	1748	2237	0	0
ON	0	0	1428	0	0	0	0	0	0	0	0	0	0	0	0	0	1428	0	1428	1428	4285	0	0
OO	193	64	645	0	322	193	1741	2258	64	0	1548	64	0	0	322	0	0	258	2193	0	129	0	0
OP	0	0	204	0	1484	18	0	0	37	500	0	0	0	0	0	0	760	0	0	408	5825	0	760
OR	188	421	622	0	1838	90	184	77	45	708	290	8	12	0	0	0	2039	159	24	1130	2153	4	0
OS	0	0	94	0	283	3867	188	0	0	2075	188	0	0	0	0	0	2924	0	0	0	283	94	0
OT	158	0	158	0	555	3809	396	0	39	1230	277	0	0	0	0	0	3293	39	0	39	0	0	0
OY	0	0	0	0	5000	0	0	0	0	2500	0	0	0	0	0	0	2500	0	0	0	0	0	0
OZ	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	P	R	S	T	Y	Z		
P2	0	0	0	6666	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0		
P8	322	0	0	7419	0	0	0	0	967	0	0	0	0	322	322	0	322	322	0	0	0		
PA	0	0	188	0	0	188	2389	0	0	0	1823	314	2075	125	188	0	2704	0	0	0	0		
PC	0	0	2000	0	2000	0	0	0	2000	0	0	0	0	0	2000	0	0	2000	0	0	0		
PD	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
PF	0	0	0	3000	0	1000	0	0	1000	0	0	0	0	0	2000	0	0	0	3000	0	0		
PG	163	327	2622	163	0	819	491	0	655	163	0	0	0	0	1639	163	163	1147	1475	0	0		
PH	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	2500	0	0	0	2500	0	2500		
PI	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0		
PO	141	0	1037	566	377	235	4669	94	0	188	47	94	141	0	0	0	1886	141	377	0	0		
PS	0	0	1000	571	6000	0	0	0	285	0	0	0	0	0	2142	0	0	0	0	0	0		
PT	85	0	1330	543	5364	28	14	28	929	14	0	0	0	0	1602	0	14	28	0	14	0		
PZ	0	0	407	904	3665	45	0	0	2262	45	45	0	0	0	2352	0	0	45	226	0	0		

	2	4	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	V	Y	Z
R2	0	180	0	0	3963	360	0	180	0	720	0	0	0	0	0	90	2432	90	0	720	1261	0	0	0
R4	0	0	0	0	35	0	177	0	0	0	70	0	0	0	0	0	9680	0	0	0	35	0	0	0
R8	0	32	65	0	6644	65	32	65	0	1368	32	0	32	0	0	0	814	0	0	293	553	0	0	0
RA	27	6	61	6	6	0	74	2099	13	27	88	713	828	27	3648	230	61	33	2017	6	13	6	0	0
RC	666	0	666	0	444	5333	222	0	0	666	666	0	0	0	0	0	888	0	0	0	444	0	0	0
RD	0	0	0	0	2200	1200	0	0	0	300	100	0	0	0	0	0	900	0	0	500	1400	0	0	3400
RE	422	140	281	0	563	0	3098	704	0	281	140	0	0	0	0	0	1830	140	0	1408	985	0	0	0
RF	0	0	0	0	769	0	0	0	0	0	384	0	384	0	0	384	769	0	0	384	2692	0	0	4230
RG	295	569	1139	0	42	21	1729	210	42	654	2194	0	21	0	0	0	780	527	42	569	1160	0	0	0
RH	0	0	0	0	827	300	0	0	0	75	0	0	0	0	0	0	977	0	0	451	1052	0	0	6315
RI	0	0	714	0	0	714	714	0	0	714	0	5000	0	714	0	714	714	0	0	0	0	0	0	0
RK	0	1250	0	0	0	0	0	0	0	2500	0	0	0	0	0	0	1250	0	0	1250	3750	0	0	0
RL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
RM	0	1818	1818	0	0	0	0	0	909	909	909	0	0	0	0	0	2727	0	0	909	0	0	0	0
RN	0	0	0	0	2857	0	0	0	0	0	0	0	1428	0	0	0	2857	1428	0	0	1428	0	0	0
RO	128	32	688	0	160	141	2028	2588	96	45	1873	19	128	6	96	19	51	418	1307	38	122	0	6	0
RP	138	0	138	0	555	0	0	0	0	277	0	0	0	0	0	0	2638	0	0	416	3472	0	0	2361
RR	384	0	0	0	4615	0	0	0	0	1538	0	0	0	0	0	0	2692	0	384	0	384	0	0	0
RS	30	0	212	0	395	6382	243	0	0	577	151	0	0	0	15	0	1884	15	15	30	45	0	0	0
RT	108	9	504	0	513	4697	532	99	0	522	216	9	0	0	0	0	2578	81	63	45	9	0	0	9
RY	0	0	0	0	4000	0	0	0	0	2000	0	0	0	0	0	0	4000	0	0	0	0	0	0	0
	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z		
S2	0	0	1052	1578	1052	0	0	526	1578	0	0	0	0	0	0	3157	0	0	526	526	0	0		
S4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0		
S8	0	171	114	2342	0	0	57	0	6114	57	0	0	0	0	0	514	114	114	228	171	0	0		
SA	0	0	335	0	0	469	2281	0	0	0	268	469	335	1946	268	201	67	3355	0	0	0	0		
SC	83	12	3095	325	1869	609	8	20	1802	200	0	8	0	0	0	1843	62	16	12	25	0	4		
SD	0	0	0	1073	805	0	0	0	805	0	0	0	0	0	0	134	0	0	67	604	0	6510		
SE	0	1000	3000	0	0	0	3000	0	1000	0	0	0	0	0	0	1000	0	0	0	1000	0	0		
SF	0	0	0	0	0	0	0	0	6666	0	0	0	0	0	0	0	0	0	0	0	0	3333		
SG	147	2066	1660	110	73	885	295	110	221	590	0	0	0	0	0	1586	295	36	738	1180	0	0		
SH	0	0	0	714	428	0	0	0	714	0	0	0	0	0	0	285	0	0	428	428	0	7000		
SM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0		
SO	209	242	1598	198	66	1003	2976	99	176	815	0	44	11	88	0	187	132	1576	198	352	22	0		
SP	0	0	0	0	0	0	0	0	1428	0	0	0	0	0	0	0	0	0	0	0	0	8571		
SR	0	0	0	6666	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0		
SS	0	0	5000	0	2500	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0		
ST	454	0	454	0	2727	454	0	0	1818	454	0	0	0	0	0	3636	0	0	0	0	0	0		
SY	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
	2	4	7	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z		
T2	0	0	0	1641	1343	895	447	149	0	1194	0	0	0	0	0	0	1343	298	895	746	1044	0		
T4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0		
T8	40	67	0	81	2081	40	0	67	0	6905	0	13	27	0	13	0	527	27	0	13	94	0		
TA	42	0	0	149	0	21	107	2312	42	21	64	171	813	299	1970	471	171	64	3211	64	0	0		
TC	133	0	2	3209	371	1503	496	2	30	1861	228	2	13	0	2	0	2019	79	15	8	19	0		
TD	0	24	0	24	1629	765	0	24	0	543	49	0	0	0	0	0	246	0	0	49	395	6246		
TE	1636	545	0	181	1454	0	363	1818	0	727	0	0	0	0	0	0	1272	0	181	545	1272	0		
TF	0	0	0	0	1000	500	500	0	0	0	0	0	0	0	0	0	500	0	0	0	0	7500		
TG	454	1729	0	1545	54	10	994	291	64	410	1027	0	0	0	0	0	1362	324	162	378	1189	0		
TH	0	0	0	0	1095	476	0	95	0	666	0	0	0	0	0	0	714	0	0	95	380	6476		
TI	0	0	0	3333	0	0	0	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0		
TK	0	0	0	2857	0	0	0	0	0	1428	1428	0	0	0	0	0	2857	0	0	1428	0	0		
TM	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0		
TO	267	45	0	1446	108	62	1082	3127	87	96	844	16	117	16	71	0	79	137	2182	50	158	0		
TP	0	0	0	0	1320	0	0	0	188	0	0	0	0	0	0	0	377	0	0	377	2264	5471		
TR	500	0	0	500	1000	0	500	0	0	2000	0	0	0	0	0	0	2000	0	500	1000	2000	0		
TS	0	0	0	1363	0	3181	0	0	0	2272	0	0	0	0	0	0	2727	454	0	0	0	0		
TT	769	0	0	769	0	2307	0	0	0	3846	1538	0	0	0	0	0	769	0	0	0	0	0		
TY	0	0	0	0	5000	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0		
TZ	0	0	0	0	0	0	0	0	0	5000	5000	0	0	0	0	0	0	0	0	0	0	0		

	E	O
VE	5000	5000
	D	
WO	DM	
	4	
XG	DM	

	4	C	D	E	F	G	K	M	O	P	R	S
Y2	0	0	0	0	0	0	0	0	0	0	0	DM

Y4	0	0	0	0	0	0	0	0	DM	0	0	0							
YA	0	0	1250	0	0	0	2500	0	0	0	6250	0							
YE	0	0	0	0	0	0	0	0	DM	0	0	0							
YG	2500	0	0	0	2500	2500	0	0	0	2500	0	0							
YO	0	0	1666	1666	0	0	0	1666	0	0	5000	0							
YS	0	DM	0	0	0	0	0	0	0	0	0	0							
	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
Z2	0	833	833	833	833	0	0	0	2500	1666	0	0	0	0	0	1666	0	0	833	0	0
Z4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
Z8	0	253	126	1012	126	0	253	0	7848	0	0	0	0	0	0	253	0	0	0	126	0
ZA	69	0	69	69	0	0	2447	0	0	0	209	1048	209	2447	559	69	0	2657	0	139	0
ZC	88	0	1834	194	1005	52	0	0	5149	17	17	0	0	17	0	1569	17	17	17	0	0
ZD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	5000
ZE	2500	0	5000	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ZF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM
ZG	536	1915	1421	94	10	231	526	42	484	378	0	10	0	0	0	2147	210	178	600	1210	0
ZH	0	0	0	3333	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0
ZI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
ZO	297	24	2079	222	74	173	3712	0	123	173	0	321	0	74	0	198	0	2301	148	74	0
ZR	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0
ZS	1428	0	0	0	4285	0	0	0	1428	0	0	0	0	0	0	2857	0	0	0	0	0
ZT	0	0	0	1250	1875	0	0	0	5000	0	0	0	0	0	0	1875	0	0	0	0	0

Table des transitions trigrammiques avec espace (page 129)

Identique à la Table des transitions trigrammiques sans espace (page 129) (page 394). Chaque nombre est à diviser par 10000 pour retrouver la valeur réelle de la probabilité : (DM=10000).

	_	2	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	V	X	Y	Z
_2	1322	8	0	8	8	0	4426	70	97	17	8	423	26	0	8	0	0	0	2636	26	44	246	617	0	0	0	0
_3	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_4	3	3	0	0	0	0	9	75	77	3	0	11	29	0	0	1	0	0	9759	11	1	0	9	0	0	0	0
_6	0	0	0	0	0	0	0	0	0	2500	0	0	7500	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
_8	91	9	0	0	12	0	6675	103	55	107	0	822	21	6	9	0	3	0	862	9	9	422	779	0	0	0	0
_9	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_A	58	26	0	0	58	6	13	19	175	2480	13	0	123	755	494	26	2708	221	97	32	2656	13	6	6	0	6	0
_C	100	300	0	0	100	0	300	4800	900	100	100	0	1500	0	0	0	0	0	900	500	0	0	400	0	0	0	0
_D	55	13	0	0	6	0	2298	2732	0	20	0	186	103	6	0	0	0	0	959	0	6	559	1683	0	0	0	1366
_E	298	133	7	0	346	0	369	55	3241	133	55	94	267	0	15	0	0	0	1369	133	110	904	2454	0	0	7	0
_F	342	0	0	0	136	0	1027	136	68	0	0	136	0	0	0	0	0	0	1301	0	0	616	3972	0	0	0	2260
_G	417	52	26	0	385	0	84	39	3165	71	84	6	2872	0	6	0	0	0	208	391	32	613	1540	0	0	0	0
_H	20	0	0	0	40	0	1372	1385	13	6	6	147	0	0	0	0	6	0	1265	0	0	542	1713	0	6	0	3473
_I	0	0	0	0	0	0	0	0	714	0	0	0	0	5000	714	714	714	714	0	0	1428	0	0	0	0	0	0
_K	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_L	8000	0	0	0	0	0	0	0	0	2000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_M	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_N	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
_O	46	55	32	0	306	0	136	138	2926	2113	96	35	2733	8	19	4	25	4	13	444	733	34	86	0	0	2	1
_P	88	29	0	0	236	0	606	29	14	0	73	266	0	14	0	0	0	0	2307	0	0	606	3801	0	0	0	1923
_R	1323	20	0	0	0	0	4623	81	61	40	20	244	40	20	0	0	0	0	1914	20	0	407	1181	0	0	0	0
_S	52	26	0	0	271	0	400	5738	480	19	9	377	218	0	0	0	0	0	2341	16	6	9	26	0	0	3	0
_T	9	56	0	0	462	0	490	4641	703	77	27	314	339	1	0	0	1	0	2722	90	18	23	14	0	0	1	1
_Y	4285	0	0	0	0	0	1428	0	0	1428	0	0	0	0	0	0	0	0	2857	0	0	0	0	0	0	0	0

	_	2	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
2_	0	293	622	0	492	0	1901	46	258	187	35	704	281	0	11	11	0	11	2277	211	46	974	1631	0
22	5000	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	3750	0	0	0	0	0	625	0	0	0	0	5625	0	0	0	0	0	0	0	0	0	0	0	0
2A	169	16	0	0	33	0	0	0	16	1663	0	33	33	899	203	50	4634	152	16	0	2071	0	0	0
2C	1052	0	0	263	1315	0	263	2368	526	0	0	2894	0	0	0	0	0	0	789	0	0	0	526	0
2D	0	0	0	0	0	0	4285	1428	0	0	0	2142	0	0	0	0	0	0	714	0	0	0	714	714
2E	8333	1666	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2F	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0
2G	8600	0	0	0	200	0	100	0	400	100	0	0	100	0	0	0	0	0	100	100	0	200	100	0
2H	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	7500
2K	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2M	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2N	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2O	422	302	0	0	543	0	271	211	574	4018	0	151	392	90	90	0	574	30	30	0	2175	90	30	0
2P	0	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7500	0
2R	6896	0	0	0	0	0	2068	0	0	0	0	689	0	0	0	0	0	0	344	0	0	0	0	0
2S	0	0	0	0	0	0	0	7187	312	0	0	937	0	0	0	0	0	0	1250	0	312	0	0	0
2T	0	0	0	0	370	0	493	4691	123	0	0	987	123	0	0	0	123	0	3086	0	0	0	0	0
2Z	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	_	6	E
36	0	0	DM
3C	0	DM	0
3G	DM	0	0

	_	2	4	6	8	A	C	D	E	F	G	H	I	L	M	N	O	P	R	S	T	Z
4_	0	0	2000	4000	2000	0	0	0	0	0	0	0	0	0	0	0	2000	0	0	0	0	0
42	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	0
48	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4A	1666	0	0	0	0	1666	0	0	1666	0	0	0	1666	0	3333	0	0	0	0	0	0	0
4C	0	0	0	0	256	0	3333	1794	0	256	256	1794	0	0	0	0	1794	512	0	0	0	0
4D	0	0	0	0	0	1500	2250	0	0	0	0	0	0	0	0	0	1500	0	0	250	750	3750
4E	0	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	0	5000	0	0	0	0	0
4G	5000	0	0	0	0	0	0	3750	0	0	0	0	0	0	0	0	1250	0	0	0	0	0
4H	0	0	0	0	0	3333	1111	0	0	0	0	0	0	0	0	0	555	0	0	0	555	4444
4L	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4O	47	15	3	0	235	108	215	6045	489	71	27	2182	11	3	7	1	63	327	71	13	55	0
4P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0	6666
4R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
4T	0	0	0	0	0	0	4000	0	0	0	0	0	0	0	0	0	6000	0	0	0	0	0

	_	3	6	F	H
69	DM	0	0	0	0
6E	6000	0	0	2000	2000
6H	0	3333	6666	0	0

	_	A	C
7_	0	DM	0
7G	DM	0	0
7S	0	0	DM

	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
8_	0	316	2091	790	755	35	246	615	70	790	193	35	70	17	17	0	1845	87	87	790	1142	0
82	8000	0	0	0	666	0	0	0	0	666	0	0	0	0	0	0	0	0	0	0	666	0
87	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	869	0	0	0	434	0	0	1739	0	5652	0	0	0	0	0	0	869	0	0	0	434	0
8A	102	11	5	24	5	0	16	1779	0	5	2	740	497	66	4354	433	24	2	1917	2	5	0
8C	505	101	0	707	202	6464	101	0	0	1414	101	0	0	0	0	0	303	0	0	0	101	0
8D	0	0	0	0	1851	1851	0	0	0	1851	0	0	0	0	0	0	740	0	0	1481	370	1851
8E	5540	540	0	135	945	135	135	135	0	810	0	0	0	0	0	0	540	0	135	0	945	0
8G	9820	11	3	38	7	3	36	9	1	0	30	0	6	0	0	0	12	0	4	1	11	0
8H	0	0	0	0	1111	1111	0	0	0	1111	0	0	0	0	0	0	2222	0	0	1111	1111	2222
8I	0	0	0	0	0	0	0	0	0	3333	0	3333	0	0	0	0	0	0	3333	0	0	0
8K	9090	0	0	0	0	0	0	0	0	909	0	0	0	0	0	0	0	0	0	0	0	0
8M	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8N	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8O	532	50	0	456	203	76	152	4593	25	25	126	126	253	0	329	0	0	25	2969	0	50	0
8P	0	0	0	0	0	0	0	0	0	4285	0	0	0	0	0	0	0	0	0	0	5714	0
8R	7500	0	0	0	833	0	0	0	0	0	0	0	0	0	0	833	833	0	0	0	0	0
8S	129	0	0	259	129	6298	0	0	0	779	0	0	0	0	0	0	2142	0	0	0	259	0
8T	33	66	0	564	564	4119	166	0	0	1794	33	33	0	0	0	0	2558	0	33	0	33	0

	_	2	6	A	G	R
9_	0	3333	3333	3333	0	0
98	0	0	0	0	DM	0
9A	0	0	0	0	0	DM
9G	DM	0	0	0	0	0

	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
A_	0	350	584	994	175	0	643	877	0	409	233	233	584	0	1520	116	1169	116	1111	292	584	0	0
A2	7692	0	0	0	769	0	0	0	0	512	0	0	0	0	0	0	769	0	256	0	0	0	0
A4	6666	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0	0	0

A8	875	0	0	0	3250	250	0	0	0	5000	0	0	0	0	125	0	250	0	0	0	250	0	0		
A9	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
AA	0	0	0	0	0	0	0	3333	0	0	0	0	2222	1111	1111	0	0	0	2222	0	0	0	0		
AC	0	0	0	714	0	4285	2142	0	0	714	0	714	0	0	714	0	714	0	0	0	0	0	0		
AD	0	0	0	0	3382	1176	0	0	0	2205	147	147	0	0	147	0	735	0	0	0	441	0	1617		
AE	7224	126	0	482	333	19	245	11	19	677	15	3	11	0	0	0	478	7	19	88	233	3	0		
AF	0	0	0	2500	0	0	0	1250	0	0	0	0	0	0	0	0	0	0	0	0	1250	0	5000		
AG	7307	384	0	384	0	0	384	384	384	0	769	0	0	0	0	0	0	0	0	0	0	0	0		
AH	294	0	0	0	2058	882	0	0	0	882	0	0	0	0	0	0	1176	0	0	0	294	0	4411		
AI	91	131	0	78	13	13	91	288	0	13	39	1376	589	91	576	13	0	26	6461	26	65	13	0		
AK	9650	0	0	72	72	0	0	0	0	14	0	0	29	0	0	0	72	14	29	14	29	0	0		
AL	9425	0	0	0	114	0	0	0	0	229	0	0	0	0	114	0	0	0	114	0	0	0	0		
AM	9428	4	0	22	12	2	2	8	0	35	0	10	8	2	0	438	14	0	8	0	2	0	0		
AN	8265	128	0	214	21	21	128	107	0	64	42	0	42	21	578	0	149	0	192	0	21	0	0		
AO	517	172	0	172	0	172	689	2586	0	172	344	689	1206	0	172	0	0	344	2758	0	0	0	0		
AP	0	0	0	0	0	0	0	0	0	1428	0	0	0	0	0	0	714	0	0	0	3571	0	4285		
AR	8206	14	0	56	786	10	0	14	0	421	0	14	3	3	24	3	351	0	0	24	56	10	0		
AS	3333	0	0	1666	0	0	0	0	0	3333	0	0	0	0	0	0	1666	0	0	0	0	0	0		
AT	0	0	0	0	1428	1428	0	0	0	2857	0	0	0	0	0	0	1428	0	1428	0	1428	0	0		
AV	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
AW	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
AY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0		

	_	2	4	7	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	V	Z
C_	0	319	744	0	1489	0	744	106	1702	212	319	638	638	106	212	0	0	0	1808	106	106	425	319	0	0
C2	7619	0	0	0	68	0	408	510	0	34	34	748	0	0	34	0	0	0	374	0	136	34	0	0	0
C4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0
C6	0	0	0	0	0	5000	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C7	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0
C8	401	6	0	2	10	0	989	42	6	17	0	8416	0	0	4	0	0	0	70	2	4	4	21	0	0
C9	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CA	487	155	0	0	332	0	0	44	110	2860	0	221	66	110	731	66	1064	133	66	0	3525	0	0	22	0
CC	74	419	0	0	3054	0	220	690	176	2	11	3784	90	4	16	32	6	2	1283	11	25	20	74	0	0
CD	397	19	0	0	19	0	1630	1272	0	39	0	2723	59	0	0	0	0	0	258	0	0	99	536	0	2942
CE	6666	0	0	0	0	0	2222	0	0	0	0	1111	0	0	0	0	0	0	0	0	0	0	0	0	0
CF	1212	0	0	0	0	0	1515	0	0	0	0	2424	0	0	0	0	0	0	909	0	0	0	3333	0	606
CG	9856	16	2	0	11	0	0	0	27	38	0	0	2	0	2	0	0	0	19	0	13	2	5	0	0
CH	488	44	0	0	0	0	1377	1022	44	0	0	2800	0	0	0	0	0	0	88	0	0	133	711	0	3288
CI	0	1428	0	0	0	0	0	1428	0	1428	0	0	0	2857	0	0	0	0	0	0	2857	0	0	0	0
CJ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0
CK	9375	0	0	0	0	0	625	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CL	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CM	8000	1000	0	0	0	0	1000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CN	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CO	1517	502	0	0	2454	3	166	55	346	3115	11	88	162	3	110	0	3	0	14	55	1351	3	33	0	0
CP	1643	0	0	0	0	0	1506	136	0	0	136	1095	136	0	0	0	0	0	547	0	0	273	3287	0	1232
CR	6400	400	0	0	0	0	400	800	0	400	0	800	0	0	0	0	0	0	800	0	0	0	0	0	0
CS	0	222	0	0	1777	0	666	2222	0	0	0	4000	0	0	0	0	0	0	1111	0	0	0	0	0	0
CT	130	0	0	0	1372	0	65	2875	130	0	0	4052	0	0	0	0	0	0	1241	0	0	130	0	0	0
CZ	0	0	0	0	6666	0	0	0	0	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	_	2	4	8	A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	Z
D_	0	158	634	317	793	317	0	158	0	317	158	0	0	158	0	0	0	2063	0	158	1587	3174	0
D2	0	0	0	0	5000	0	0	0	0	2500	0	0	0	0	0	0	0	2500	0	0	0	0	0
D8	0	0	0	0	2000	0	0	0	0	7000	0	0	0	0	0	0	0	0	0	0	0	1000	0
DA	104	35	0	32	7	17	10	1989	10	7	3	452	0	366	61	4481	513	25	0	1877	0	3	0
DC	5	23	0	1866	168	5574	5	2	2	745	2	2	2	2	0	2	0	1285	0	2	79	218	2
DD	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DE	6666	0	0	303	606	0	0	0	0	909	0	0	0	0	0	0	0	606	303	0	0	606	0
DF	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000
DG	9560	15	0	196	0	15	30	75	0	0	60	0	0	0	0	0	0	0	0	15	0	30	0
DH	322	0	0	0	2903	2903	0	0	0	645	0	0	0	0	0	0	0	967	0	0	322	1612	322
DI	0	1666	0	0	0	0	0	0	0	0	0	6666	0	0	0	0	0	0	0	1666	0	0	0
DM	7500	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0
DO	350	105	0	1155	332	140	210	4553	52	122	70	52	0	122	0	332	17	87	17	2136	52	87	0
DR	0	0	0	0	6666	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DS	198	49	0	891	396	4554	0	0	0	2079	0	0	0	0	0	0	0	1732	0	0	0	99	0
DT	30	50	0	1515	373	3373	10	10	10	2303	0	0	0	0	0	0	0	2272	10	20	10	0	10
DZ	75	32	0	353	428	2700	10	10	10	5198	0	0	0	0	0	0	0	1114	0	0	21	42	0

	_	2	3	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	W	Y	Z
E_	0	366	1	851	1	1266	1	262	37	818	360	46	321	405	0	5	1	0	0	1716	137	124	1218	2049	0	1	0
E2	7479	0	0	0	0	0	0	1300	162	0	0	0	569	0	0	0	0	0	0	81	0	81	81	162	0	0	81
E4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0
E8	1063	26	0	0	0	53	0	2180	26	26	26	0	6250	0	0	26	0	0	0	106	0	0	79	132	0	0	0
EA	123	30	0	0	0	0	0	0	30	0	1702	0	0	0	433	959	61	4210	464	30	0	1919	0	0	30	0	0
EC	217	217	0	0	0	0	0	0	8043	434	0	217	0	217	0	0	217	0	0	434	0	0	0	0	0	0	0
ED	33	0	0	0	0	0	0	3289	4761	0	143	0	719	0	11	0	0	11	0	166	0	0	166	697	0	0	0
EE	2432	810	0	0	0	1351	0	810	0	810	0	0	270	270	0	270	0	0	0	1621	0	0	0	1351	0	0	0
EF	344	0	344	0	0	0	0	1034	0	0	0	0	689	0	0	0	0	0	0	1034	0	0	344	5517	0	0	689
EG	9617	81	0	0	0	81	0	27	0	54	27	0	27	27	0	0	0	0	0	0	0	27	27	0	0	0	0
EH	109	0	0	0	0	109	0	2527	3736	0	0	0	549	0	0	0	0	0	0	329	0	0	659	1648	0	0	329
EI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0
EK	9000	0	0	0	0	1000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EO	867	330	0	0	0	805	0	247	185	371	3078	20	41	268	82	392	0	165	0	0	0	3057	41	41	0	0	0
EP	256	0	0	0	0	0	0	1025	0	0	0	0	512	0	0	0	0	0	0	256	0	0	512	7179	0	0	256
ER	5312	0	0	0	0	0	0	4062	0	0	0	0	0	0	0	0	0	0	0	625	0	0	0	0	0	0	0
ES	41	164	0	0	0	864	0	164	7078	41	123	0	781	82	0	0	0	0	0	658	0	0	0	0	0	0	0
ET	15	93	0	0	0	962	0	419	6863	62	108	0	683	77	15	31	0	0	0	590	46	15	15	0	0	0	0
EY	0	0	0	0	0	0	0	3333	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0	0	0

	_	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	P	R	S	T	Z
F_	0	0	1304	1304	434	0	869	0	434	869	434	0	0	0	0	434	434	0	1739	1739	0
F2	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F3	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0
F8	1666	0	0	0	1666	1666	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0
FA	0	0	0	526	0	0	0	1403	0	0	0	1228	877	1929	350	0	0	3508	0	175	0
FC	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	5000
FE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0
FG	7600	0	0	800	400	0	0	0	0	0	0	0	0	0	0	400	0	0	400	400	0
FK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FN	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FO	666	222	0	888	444	222	222	5111	0	0	0	0	0	222	0	0	0	1333	0	666	0
FS	0	0	0	714	0	5000	0	0	0	1428	0	0	0	0	0	2857	0	0	0	0	0
FT	64	128	0	1346	320	4615	0	0	64	1089	64	0	64	0	0	2243	0	0	0	0	0
FZ	0	133	0	666	933	2400	0	133	0	4000	0	0	0	0	0	1600	0	0	0	133	0

	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	O	P	R	S	T	Y	Z
G_	0	369	2601	1039	93	18	445	568	36	391	518	0	1	0	0	1751	243	193	560	1160	1	0
G2	6562	0	0	0	2812	0	0	0	0	0	0	0	0	0	0	312	0	0	312	0	0	0
G4	0	0	0	0	0	0	0	0	0	909	0	0	0	0	0	9090	0	0	0	0	0	0
G8	1646	182	0	60	3902	304	0	121	0	3292	0	0	60	0	0	121	0	0	60	243	0	0
GA	434	0	0	0	0	0	0	1304	0	434	0	2173	0	0	3478	0	0	2173	0	0	0	0
GC	0	0	1000	1000	0	4000	1000	1000	0	1000	0	0	0	0	0	0	1000	0	0	0	0	0
GD	87	0	0	35	2591	3992	17	35	0	665	17	0	0	0	0	630	0	0	227	1523	0	175
GE	4583	0	0	416	416	0	833	0	0	1250	0	0	0	0	0	833	0	0	625	1041	0	0
GF	0	0	0	0	666	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	6000	0	0

GG	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
GH	20	0	0	41	2695	3024	0	0	0	823	0	0	0	0	0	1131	0	0	205	1995	0	61			
GK	8571	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1428	0	0	0	0	0	0			
GM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
GN	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
GO	877	0	0	526	526	175	2456	1929	0	0	1228	0	175	0	175	175	0	1578	0	175	0	0			
GP	140	0	0	140	1408	140	0	0	140	0	0	0	0	0	0	422	0	0	281	7183	0	140			
GR	5882	0	0	588	0	0	0	588	0	588	0	0	0	0	0	588	0	0	588	1176	0	0			
GS	0	93	0	280	93	7476	0	0	0	560	0	0	0	0	0	1401	0	0	0	93	0	0			
GT	0	0	0	194	350	6536	155	0	0	428	233	0	0	0	0	2101	0	0	0	0	0	0			
	_	2	4	6	8	9	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z	
H_	0	392	784	0	588	0	784	0	196	0	0	588	0	0	0	0	0	0	1764	0	0	2549	2352	0	
H2	6666	0	0	0	0	0	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
H3	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
H4	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	
H6	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
H8	588	0	0	0	0	0	4705	0	0	0	0	2352	588	0	588	0	0	0	1176	0	0	0	0	0	
HA	96	27	6	0	48	0	0	13	20	2308	6	13	0	483	628	41	3559	207	27	13	2487	6	0	0	
HC	7	43	0	0	2786	7	215	4204	0	7	0	849	0	0	7	0	7	0	1670	0	7	14	165	7	
HD	0	0	0	0	0	0	3636	3636	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1818	909	
HE	6363	0	0	0	0	0	909	909	0	0	0	0	0	0	0	0	0	0	1818	0	0	0	0	0	
HF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	
HG	9054	0	23	0	472	0	0	0	94	70	0	0	70	0	0	0	0	0	70	23	0	47	70	0	
HH	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
HI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	
HM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	
HO	303	160	0	0	1443	0	285	142	267	4385	71	142	160	35	71	17	231	0	0	35	2014	89	142	0	
HP	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	
HR	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
HS	121	121	0	0	1151	0	363	4363	0	60	0	1272	0	0	0	0	0	0	2484	0	0	0	60	0	
HT	76	65	0	0	1154	0	490	3300	10	10	0	2156	32	0	10	0	0	0	2679	0	0	0	10	0	
HX	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	
HZ	114	52	0	0	313	0	794	2246	0	10	0	3970	10	0	0	0	0	0	2413	0	10	31	31	0	
	_	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	P	R	S	T	Z				
I_	0	0	1250	0	1250	0	3750	0	0	1250	0	0	0	0	0	1250	0	0	0	1250	0				
I2	5294	0	0	0	1764	0	0	588	0	588	0	0	0	0	0	0	0	1764	0	0	0				
I8	2000	0	0	0	1000	0	0	0	0	7000	0	0	0	0	0	0	0	0	0	0	0				
IA	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
IC	0	4000	0	2000	0	4000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
ID	0	0	0	0	0	2222	0	0	0	2222	0	0	0	0	0	0	0	0	0	1111	4444				
IE	5714	714	0	1785	0	0	0	0	0	714	0	0	357	357	0	357	0	0	0	0	0				
IG	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
IH	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	5000				
II	0	187	0	125	0	0	0	312	0	0	62	1312	750	62	750	62	0	6312	62	0	0				
IK	9310	0	0	172	0	0	0	0	0	0	0	0	172	172	0	172	0	0	0	0	0				
IL	8888	0	0	0	0	0	0	0	0	0	0	0	0	0	1111	0	0	0	0	0	0				
IM	9843	0	0	0	0	0	0	0	0	156	0	0	0	0	0	0	0	0	0	0	0				
IN	2142	0	0	1428	0	0	0	714	0	0	0	0	0	0	0	0	0	5000	0	714	0				
IO	3333	0	0	3333	0	0	0	0	3333	0	0	0	0	0	0	0	0	0	0	0	0				
IP	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
IR	7817	81	0	65	602	0	0	65	16	374	0	97	0	65	81	684	16	0	16	16	0				
IS	0	0	0	5000	0	2500	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0				
IT	2000	0	0	0	2000	0	0	0	0	6000	0	0	0	0	0	0	0	0	0	0	0				
IY	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
	_																								
JR	DM																								
	_	2	4	8	A	C	D	E	F	G	H	K	L	O	P	R	S	T	Y						
K_	0	1052	918	1403	165	20	175	134	61	1393	794	0	0	1764	371	51	660	1021	10						
K8	4444	0	0	0	0	0	0	0	0	4444	0	0	0	0	0	1111	0	0	0						
KA	1428	0	0	0	0	0	0	0	0	0	0	2857	1428	1428	0	2857	0	0	0						
KC	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0						
KG	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0						
KK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0						
KM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0						
KO	2857	0	0	0	0	0	1428	1428	0	0	0	2857	0	0	0	1428	0	0	0						
KP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0						
KR	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0						
KS	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0						
KT	0	0	0	0	0	0	0	0	0	5000	0	5000	0	0	0	0	0	0	0						
	_	2	4	8	A	C	D	F	G	H	O	P	R	S	T										
L_	0	924	1092	1092	420	0	336	0	1008	336	2100	168	84	756	1680										
LA	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LD	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0										
LE	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LG	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LI	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0										
LM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LN	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LR	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0										
LT	0	0	0	3333	0	3333	0	3333	0	0	0	0	0	0	0										
	_	2	4	8	A	C	D	E	F	G	H	I	K	M	N	O	P	R	S	T	Y				
M_	0	226	829	791	395	26	177	80	32	527	385	2	6	2	0	2775	197	24	1282	2231	2				
M2	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
M8	1818	0	0	0	909	0	0	909	0	6363	0	0	0	0	0	0	0	0	0	0	0				
MA	0	0	0	0	0	0	0	6250	0	0	0	1250	0	1250	1250	0	0	0	0	0	0				
MC	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
MD	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0				
ME	2500	2500	0	2500	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0				
MG	9473	0	0	0	0	0	0	0	0	0	0	0	0	0	526	0	0	0	0	0	0				
MI	0	0	0	0	0	0	0	0	0	2000	0	0	0	0	0	0	0	8000	0	0	0				
MK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
ML	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
MN	9952	0	0	0	0	0	0	0	0	47	0	0	0	0	0	0	0	0	0	0	0				
MO	1250	0	0	2500	0	0	2500	2500	0	0	0	0	0	0	0	0	0	1250	0	0	0				
MR	2500	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	2500	0	0	0	2500	0				
MT	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	0				
	_	2	4	8	A	C	D	E	F	G	H	M	O	P	R	S	T	Z							
N_	0	177	724	821	611	0	128	128	32	450	450	0	2254	273	64	1078	2801	0							
N2	6666	0	0	0	0	0	0	0	0	0	0	0	3333	0	0	0	0	0							
N8	1666	0	0	0	2500	0	0	0	0	5833	0	0	0	0	0	0	0	0							
NA	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0							
NC	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0							
ND	0	0	0	0	5000	1666	0	0	0	1666	0	0	0	0	0	0	0	1666							
NE	6666	0	0	0	0	0	0	0	0	1666	0	0	1666	0	0	0	0	0							
NG	7500	0	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	0							
NH	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	0	0	0	5000							
NK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0							
NL	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0							
NM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0							
NO	2857	1428	0	2857	1428	0	0	1428	0	0	0	0	0	0	0	0	0	0							
NR	8823	0	0	0	0	0	0	0	0	1176	0	0	0	0	0	0	0	0							
NT	0	0	0	0	0	5000	0	0	0	5000	0	0	0	0	0	0	0	0							
	_	2	4	7	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z	

O_	0	370	770	9	1687	331	9	1141	1082	97	253	829	19	48	9	9	0	858	175	800	468	1024	0	0
O2	7774	31	0	0	31	1128	62	31	31	0	219	0	0	0	0	31	0	156	0	282	0	219	0	0
O4	384	0	0	0	384	384	0	0	0	0	0	1153	0	0	0	0	0	7692	0	0	0	0	0	0
O8	1014	16	0	0	38	3082	174	27	103	0	5171	5	0	0	0	0	0	196	5	21	38	103	0	0
O9	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OA	241	120	0	0	211	30	0	332	1631	0	120	60	483	151	30	3232	453	60	30	2809	0	0	0	0
OC	69	138	0	0	657	242	5467	1176	34	173	346	380	34	34	0	69	0	692	311	0	34	138	0	0
OD	45	1	0	0	10	3251	3976	0	21	3	597	16	5	0	0	3	0	619	0	3	146	957	0	338
OE	6654	118	4	0	383	337	65	853	20	32	312	104	2	6	0	0	0	328	38	22	208	504	2	0
OF	863	71	0	0	143	1942	0	0	0	0	647	0	0	0	0	0	0	863	0	0	287	4100	0	1079
OG	8181	82	0	0	247	82	0	743	0	0	0	330	0	0	0	0	0	0	82	82	165	0	0	0
OH	97	6	3	0	24	3061	2897	24	21	0	811	0	3	0	0	0	0	860	6	3	176	1570	0	433
OI	0	238	0	0	0	0	476	238	0	0	0	0	2619	0	0	4285	0	0	0	1904	238	0	0	0
OK	9808	0	0	0	63	127	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OL	6363	0	0	0	0	0	0	0	0	0	0	0	909	0	0	0	0	0	0	0	0	2727	0	0
OM	9788	0	0	0	0	70	0	0	0	0	0	0	0	70	0	0	0	70	0	0	0	0	0	0
ON	8571	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1428	0	0	0	0
OO	597	298	149	0	597	298	149	746	2388	0	0	298	149	0	0	447	0	0	149	3432	0	298	0	0
OP	230	0	0	0	211	1535	19	0	0	38	499	0	0	0	0	0	0	690	0	0	364	5738	0	671
OR	8042	29	0	0	80	894	25	12	16	0	338	0	0	12	0	0	0	317	0	4	59	165	0	0
OS	517	0	0	0	0	172	4482	172	0	0	2586	172	0	0	0	0	0	1724	0	0	0	172	0	0
OT	68	204	0	0	68	680	4149	136	0	0	1564	68	0	0	0	0	0	3061	0	0	0	0	0	0
OY	5000	0	0	0	0	0	0	0	0	0	2500	0	0	0	0	0	0	2500	0	0	0	0	0	0
OZ	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	_	2	8	A	C	D	E	F	G	H	I	K	M	N	O	R	S	T	Y
P_	0	285	857	857	0	0	0	285	285	857	0	0	0	0	2000	0	571	4000	0
P2	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0
P8	0	357	0	7142	0	0	0	0	1071	0	0	0	0	357	357	357	357	0	0
PA	192	0	128	0	0	64	2371	0	0	0	1858	320	2115	128	192	2628	0	0	0
PC	0	0	2000	0	2000	0	0	0	2000	0	0	0	0	0	2000	0	2000	0	0
PD	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PF	0	0	0	3333	0	0	0	0	1111	0	0	0	0	0	2222	0	0	3333	0
PG	5666	166	2166	166	0	833	0	0	0	0	0	0	0	0	166	0	0	833	0
PH	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0	0
PI	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0	0	0	0
PO	97	97	1073	585	390	195	4780	0	0	48	48	97	146	0	0	1951	146	341	0
PS	0	0	1029	441	6029	0	0	0	294	0	0	0	0	0	2205	0	0	0	0
PT	43	87	1343	540	5343	0	0	29	948	14	0	0	0	0	1591	14	29	0	14
PZ	45	0	407	904	3665	45	0	0	2262	45	45	0	0	0	2307	0	45	226	0

	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y
R_	0	190	576	546	1528	59	190	112	49	468	268	6	8	0	0	0	2520	143	47	1256	2025	4
R2	8888	0	0	0	0	0	0	0	0	555	0	0	0	0	0	555	0	0	0	0	0	0
R8	1500	0	0	0	1750	0	0	250	0	6250	0	0	250	0	0	0	0	0	0	0	0	0
RA	206	13	0	68	0	0	13	1793	0	27	41	524	1117	41	4165	275	41	27	1627	0	13	0
RC	625	1250	0	625	625	5000	0	0	0	1875	0	0	0	0	0	0	0	0	0	0	0	0
RD	0	0	0	0	1428	1428	0	0	0	2857	0	0	0	0	0	0	0	0	0	0	4285	0
RE	8750	0	0	0	625	0	0	0	0	625	0	0	0	0	0	0	0	0	0	0	0	0
RF	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	5000	0	0	0	0	0	0
RG	9593	0	0	121	0	0	0	162	0	0	40	0	40	0	0	0	40	0	0	0	0	0
RH	0	0	0	0	5000	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RI	909	0	0	909	0	909	0	0	0	909	0	4545	0	909	0	0	909	0	0	0	0	0
RK	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RL	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RN	8571	0	0	0	0	0	0	0	0	0	0	0	1428	0	0	0	0	0	0	0	0	0
RO	841	155	0	2024	249	31	249	3177	0	62	218	62	467	0	311	31	31	0	1962	62	62	0
RP	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0
RR	3333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3333	0	3333	0	0	0
RS	227	0	0	454	0	7045	0	0	0	1363	0	0	0	0	227	0	681	0	0	0	0	0
RT	84	252	84	252	252	5042	0	252	0	1596	252	0	0	0	0	0	1512	0	336	84	0	0
RY	3333	0	0	0	0	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0

	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Y	Z
S_	0	625	1562	937	0	312	312	0	0	0	312	0	0	0	0	0	3750	312	0	312	1562	0	0
S2	3529	0	0	1176	1176	1176	0	0	0	1176	0	0	0	0	0	0	1764	0	0	0	0	0	0
S8	988	0	0	58	2209	0	0	0	0	6162	0	0	0	0	0	0	232	58	58	116	116	0	0
SA	335	0	0	268	0	0	335	2281	0	0	0	268	469	335	1946	268	67	67	3355	0	0	0	0
SC	146	83	0	3080	313	1869	580	4	20	1794	187	0	8	0	0	0	1807	62	16	4	16	0	4
SD	0	0	0	0	1013	810	0	0	0	810	0	0	0	0	0	0	135	0	0	67	608	0	6554
SE	6000	0	0	2000	0	0	0	0	0	1000	0	0	0	0	0	0	0	0	0	0	1000	0	0
SF	0	0	0	0	0	0	0	0	0	6666	0	0	0	0	0	0	0	0	0	0	0	0	3333
SG	9594	0	0	36	0	36	147	36	0	0	0	0	0	0	0	0	36	36	0	73	0	0	0
SH	0	0	0	0	724	289	0	0	0	724	0	0	0	0	0	0	289	0	0	434	434	0	7101
SM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SO	1988	178	11	1396	167	67	692	2905	78	100	536	0	44	11	89	0	0	67	1575	33	33	22	0
SP	0	0	0	0	0	0	0	0	0	1666	0	0	0	0	0	0	0	0	0	0	0	0	8333
SR	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SS	0	0	0	3333	0	3333	0	0	0	3333	0	0	0	0	0	0	0	0	0	0	0	0	0
ST	0	588	0	588	0	3529	0	0	0	2352	588	0	0	0	0	0	2352	0	0	0	0	0	0
SY	0	0	0	0	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	_	2	4	7	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
T_	0	384	384	0	1538	0	0	769	384	0	1153	384	0	769	0	0	0	2692	0	0	769	769	0
T2	4393	0	0	0	1515	0	909	303	151	0	909	0	0	0	0	0	0	606	151	909	151	0	0
T4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
T8	543	13	0	0	27	1983	40	0	40	0	6929	0	13	27	0	13	0	339	13	0	0	13	0
TA	171	42	0	0	128	0	21	107	2269	42	21	64	171	813	299	1970	471	149	42	3169	42	0	0
TC	21	133	0	2	3207	371	1503	491	2	30	1857	228	2	8	0	2	0	2017	76	15	6	19	0
TD	49	0	0	0	0	1637	769	0	24	0	545	49	0	0	0	0	0	223	0	0	24	397	6277
TE	5925	555	0	0	185	1111	0	0	925	0	185	0	0	0	0	0	0	370	0	185	0	555	0
TF	0	0	0	0	0	1000	500	500	0	0	0	0	0	0	0	0	0	500	0	0	0	0	7500
TG	9457	21	21	0	97	0	0	184	0	0	10	108	0	0	0	0	0	10	75	10	0	0	0
TH	0	0	0	0	0	1100	478	0	95	0	669	0	0	0	0	0	0	717	0	0	95	382	6459
TI	0	0	0	0	3333	0	0	0	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0
TK	8000	0	0	0	2000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TM	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TO	754	238	0	0	1341	96	62	951	3077	75	79	754	16	113	16	71	0	46	117	2113	16	54	0
TP	188	0	0	0	0	1320	0	0	0	0	0	0	0	0	0	0	0	377	0	0	377	2264	5471
TR	5000	0	0	0	0	1000	0	500	0	0	1500	0	0	0	0	0	0	0	0	500	500	1000	0
TS	0	0	0	0	1500	0	3500	0	0	0	2500	0	0	0	0	0	0	2000	500	0	0	0	0
TT	0	909	0	0	909	0	1818	0	0	0	4545	909	0	0	0	0	0	909	0	0	0	0	0
TY	5000	0	0	0	0	5000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TZ	0	0	0	0	0	0	0	0	0	0	5000	5000	0	0	0	0	0	0	0	0	0	0	0

	_	E
VE	5000	5000

	O
W_	DM

	_
XG	DM

	_	2	4	A	D	E	G	K	M	O	R	S
Y_	0	1250	1250	5000	0	0	1250	0	0	0	0	1250
YA	0	0	0	0	0	0	0	2500	0	0	7500	0
YE	0	0	0	0	0	0	0	0	0	DM	0	0
YG	DM	0	0	0	0	0	0	0	0	0	0	0
YO	0	0	0	0	1666	1666	0	0	1666	0	5000	0

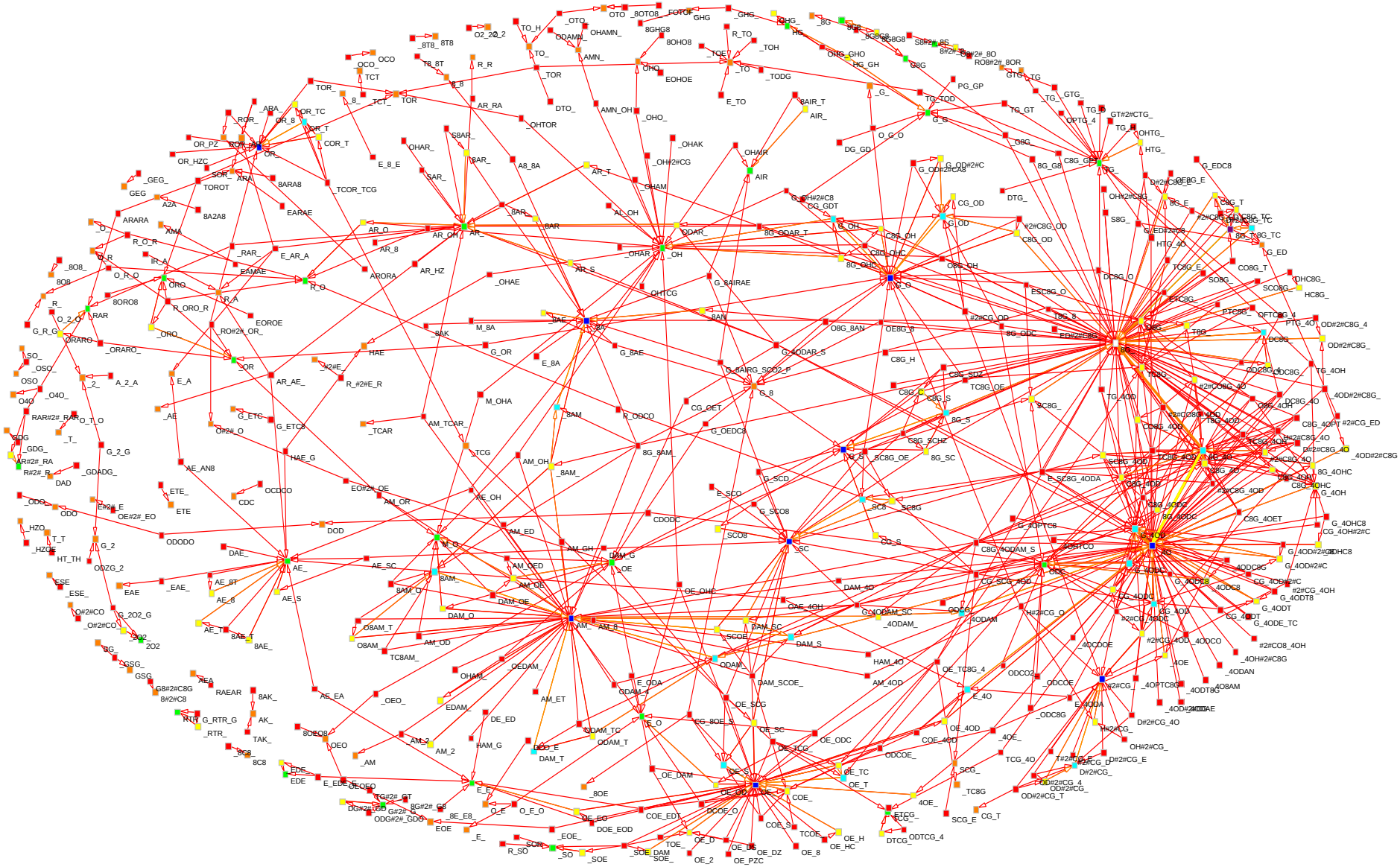
	_	2	4	8	A	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	Z
Z_	0	1500	500	0	0	0	0	0	500	2000	0	0	0	0	0	0	3000	0	500	500	1500	0
Z2	5555	0	0	0	0	1111	0	0	0	2222	1111	0	0	0	0	0	0	0	0	0	0	0
Z8	886	0	0	126	886	126	0	0	0	7721	0	0	0	0	0	0	126	0	0	0	126	0
ZA	209	69	0	69	69	0	0	2447	0	0	0	139	1048	209	2447	489	69	0	2657	0	69	0
ZC	0	88	0	1834	194	1005	52	0	0	5149	17	17	0	0	17	0	1569	17	17	17	0	0
ZD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	0	0	0	0	5000
ZE	7500	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ZF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM
ZG	9852	21	10	73	0	0	21	10	0	0	0	0	0	0	0	0	0	0	0	10	0	0
ZH	3333	0	0	0	0	0	0	0	0	3333	0	0	0	0	0	0	3333	0	0	0	0	0
ZI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	DM	0	0	0	0	0
ZO	929	251	0	1809	226	75	25	3768	0	125	25	0	326	0	75	0	75	0	2160	50	75	0
ZR	DM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ZS	1666	0	0	0	0	3333	0	0	0	1666	0	0	0	0	0	0	3333	0	0	0	0	0
ZT	0	0	0	0	1538	2307	0	0	0	4615	0	0	0	0	0	0	1538	0	0	0	0	0

Graphes connexes des motifs symétriques et redondants

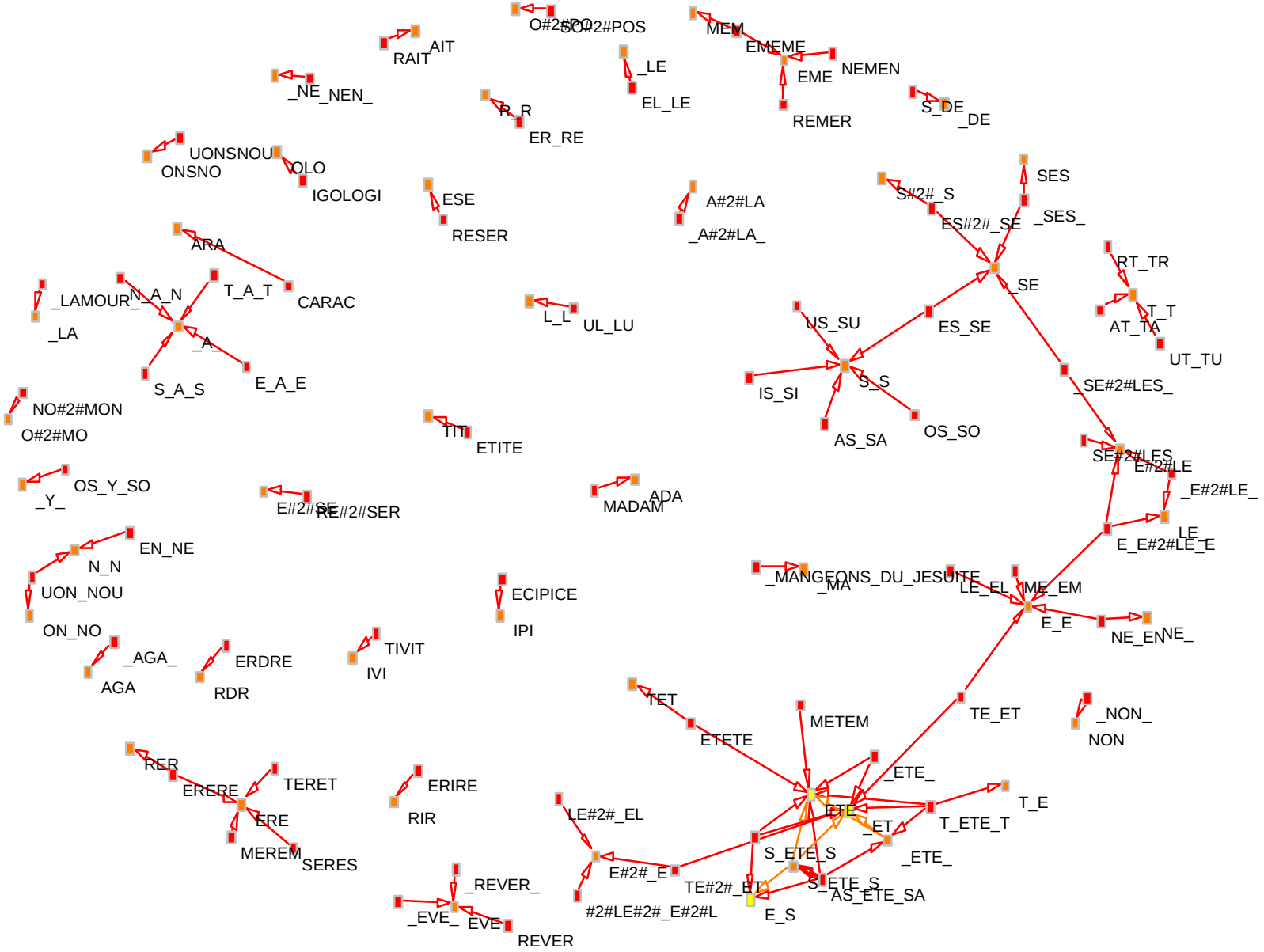
(page 274)

14 novembre 1998 —Première édition

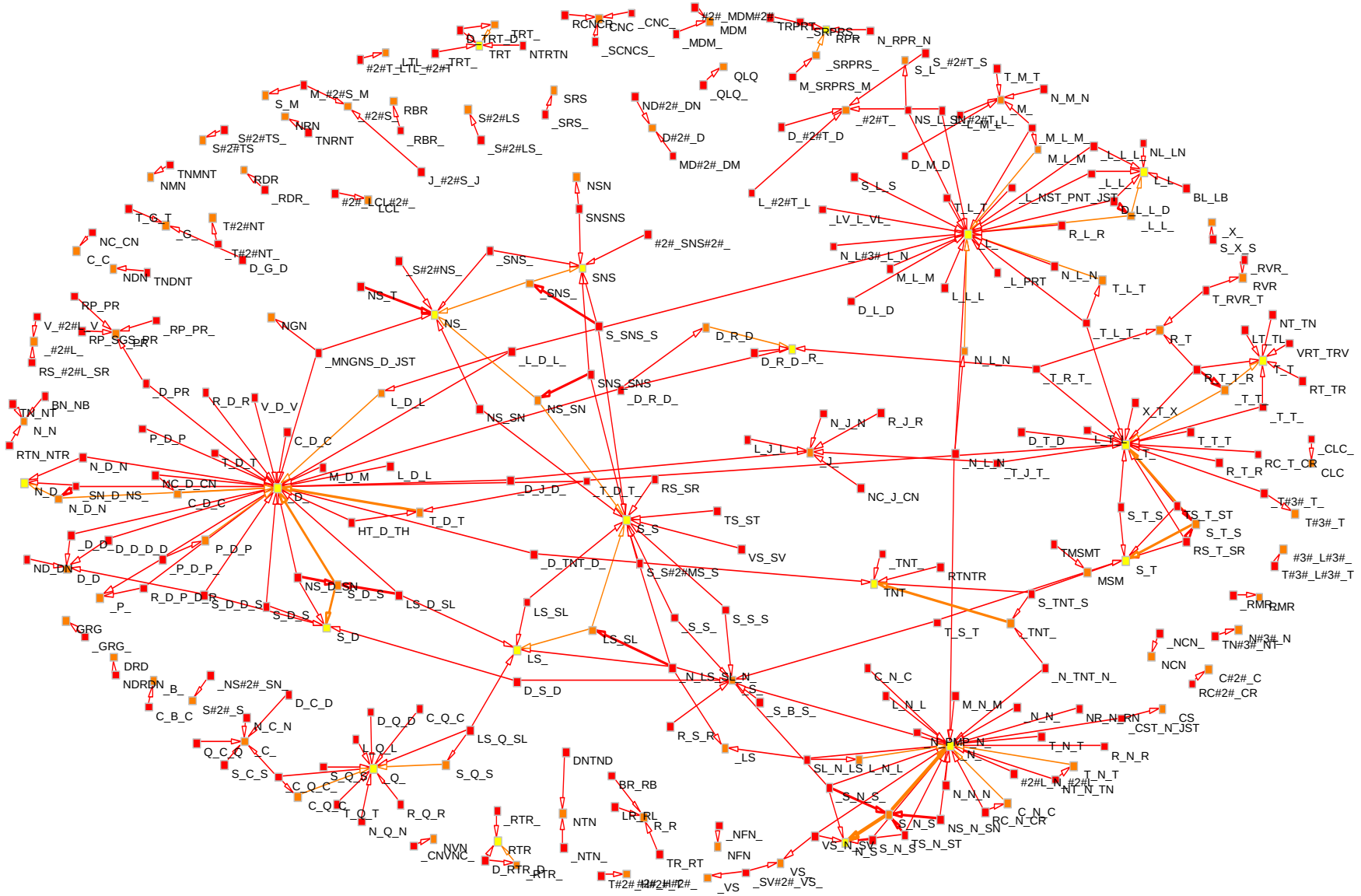
Ms408 version FRIEDMAN avec espaces



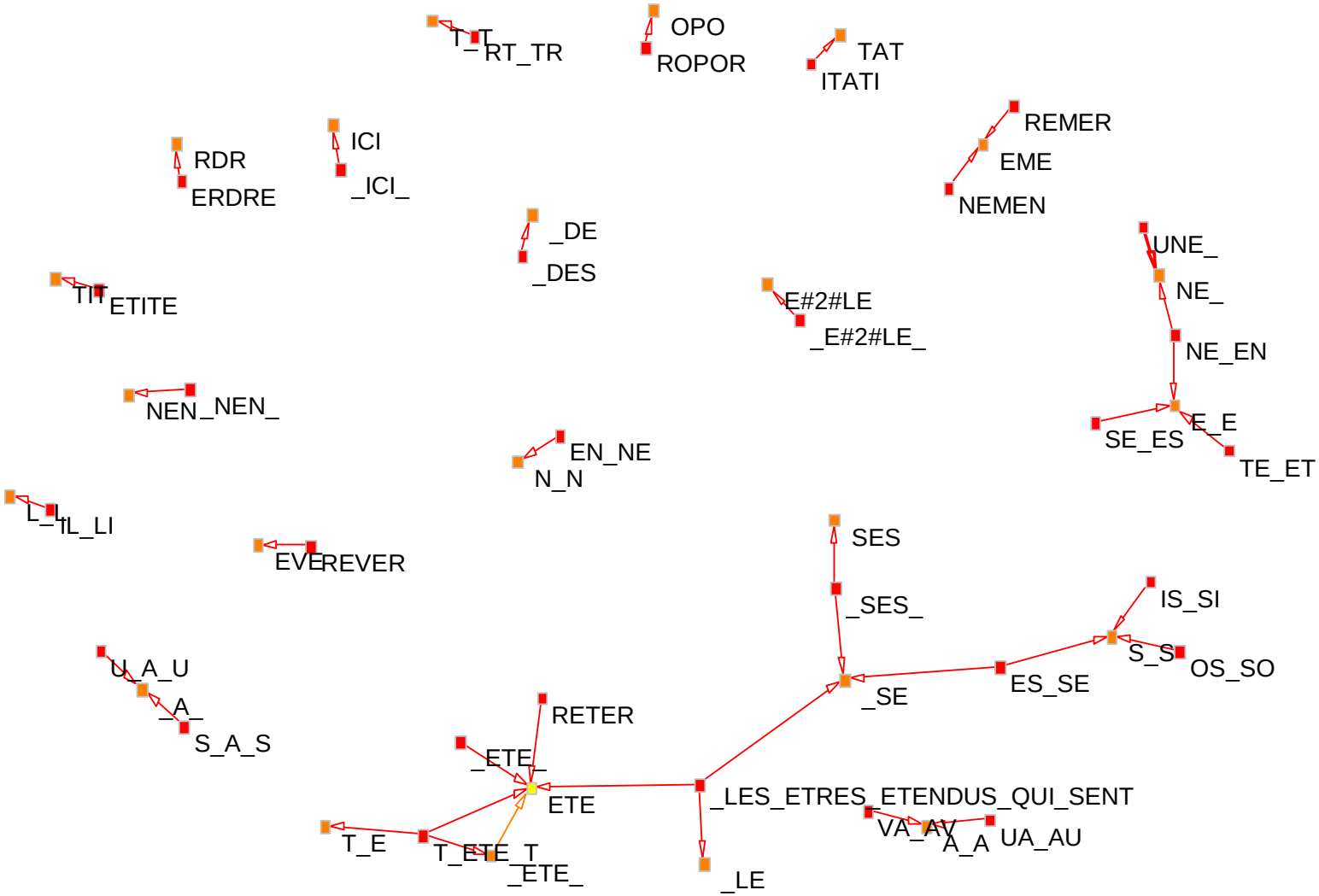
Candide en français avec voyelles



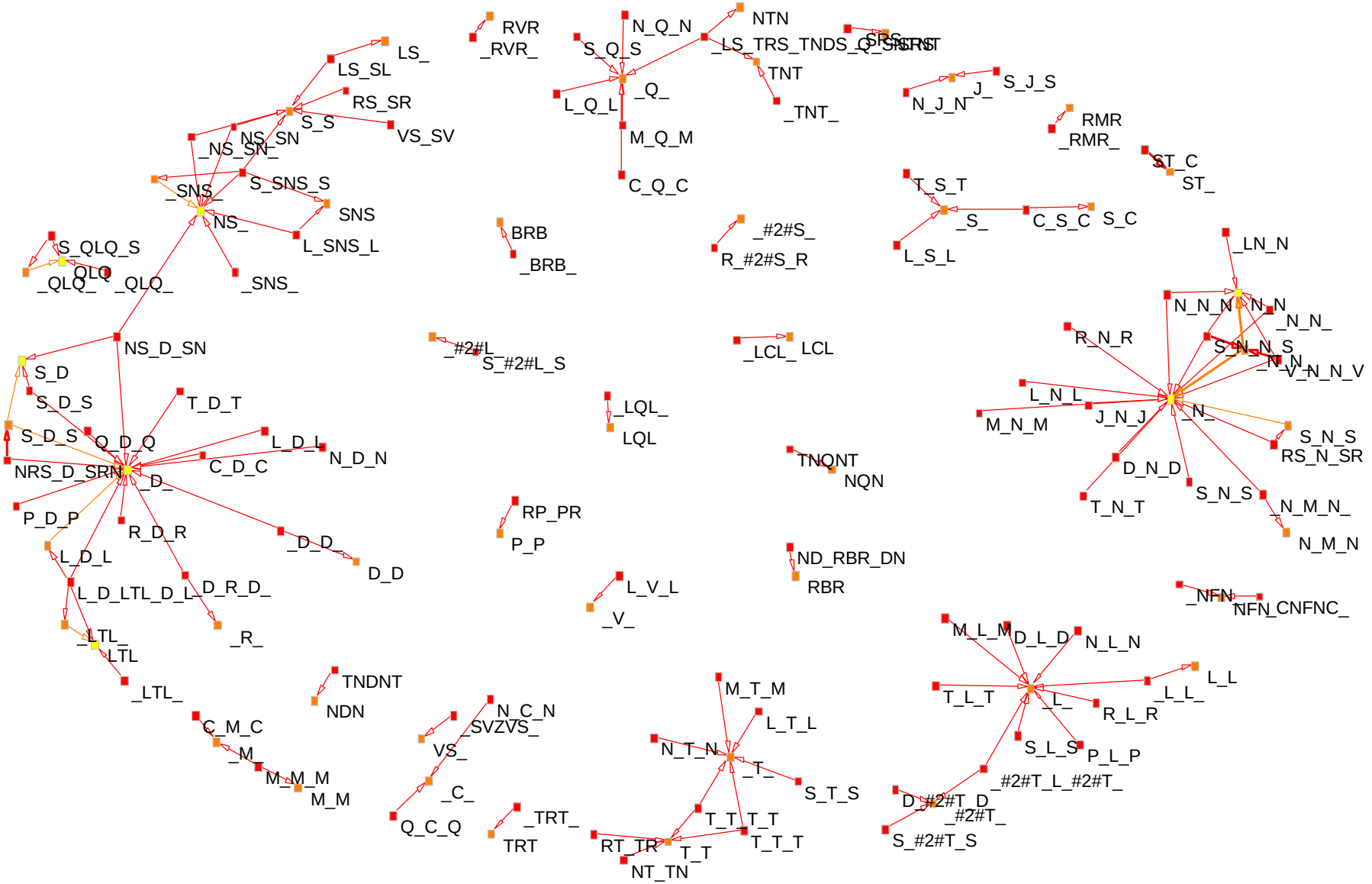
Candide en français sans voyelles



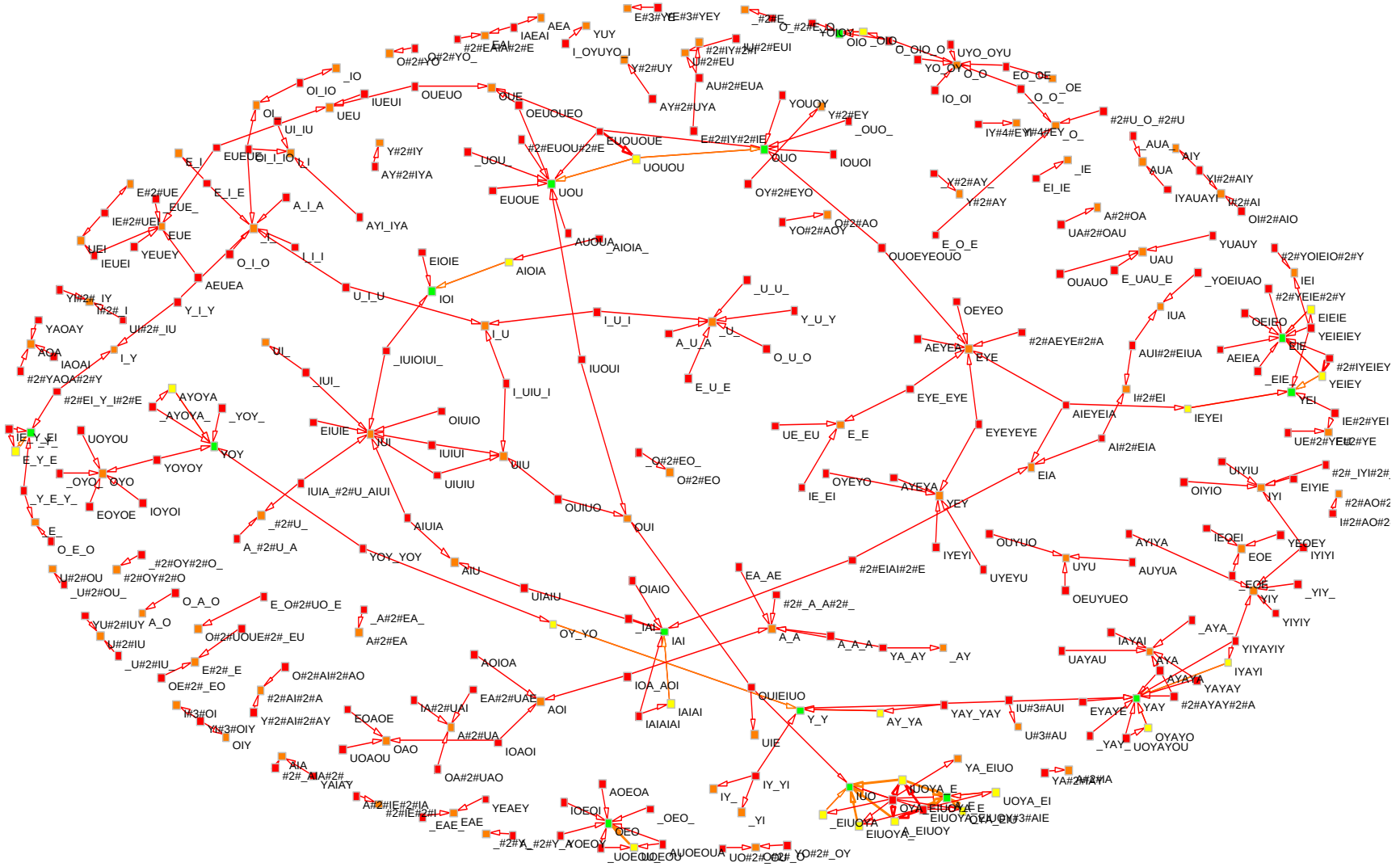
Micromega en français avec voyelles



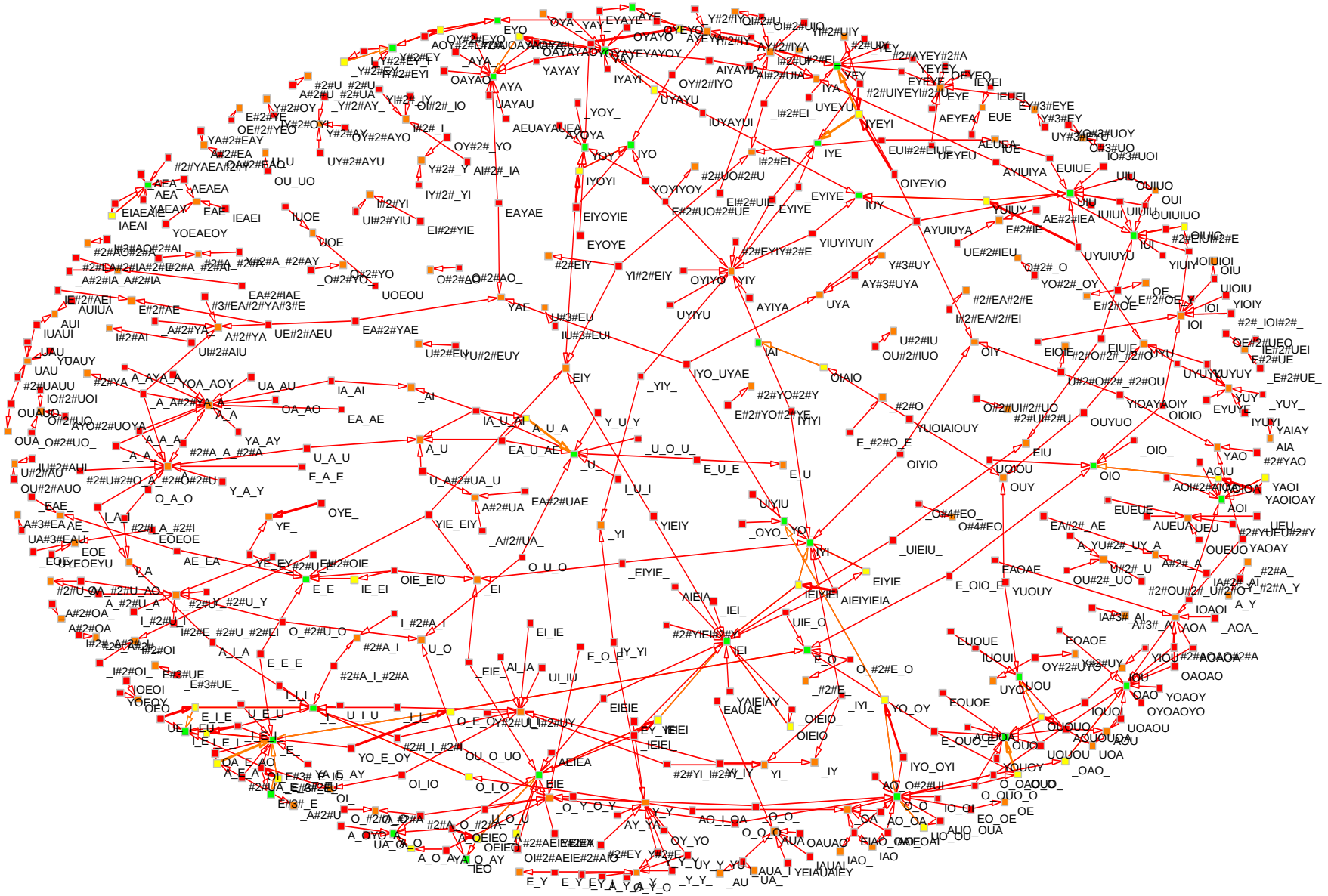
Micromega en français sans voyelles



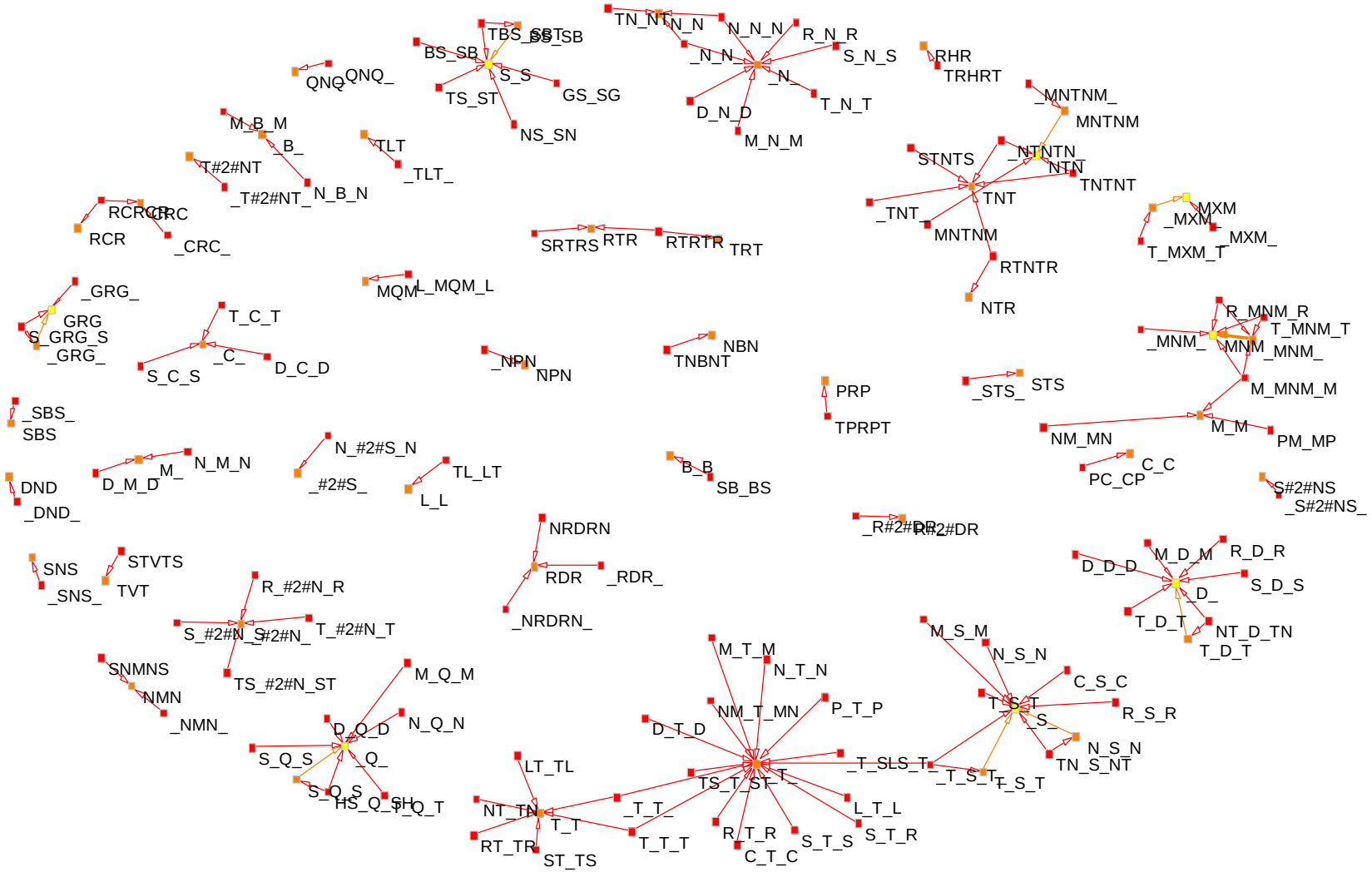
Antigone en anglais avec voyelles et polysubstitutions



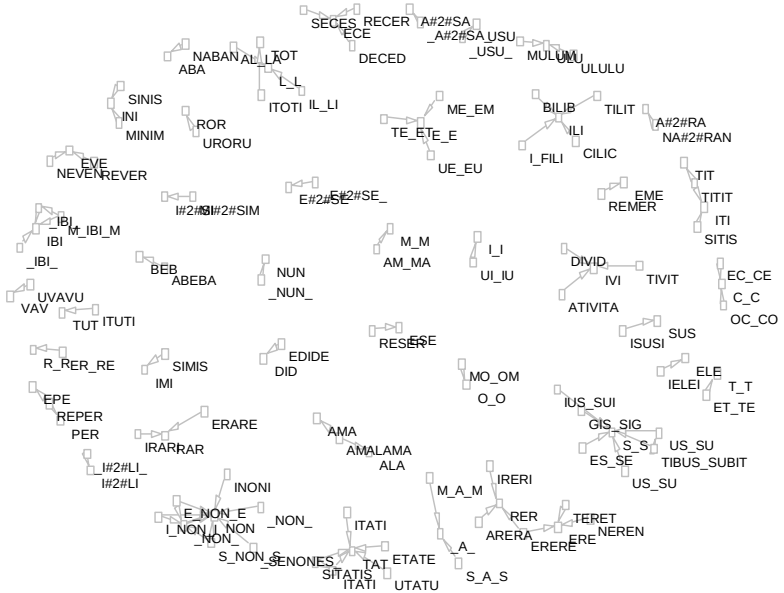
Candide en français avec voyelles et polysubstitutions



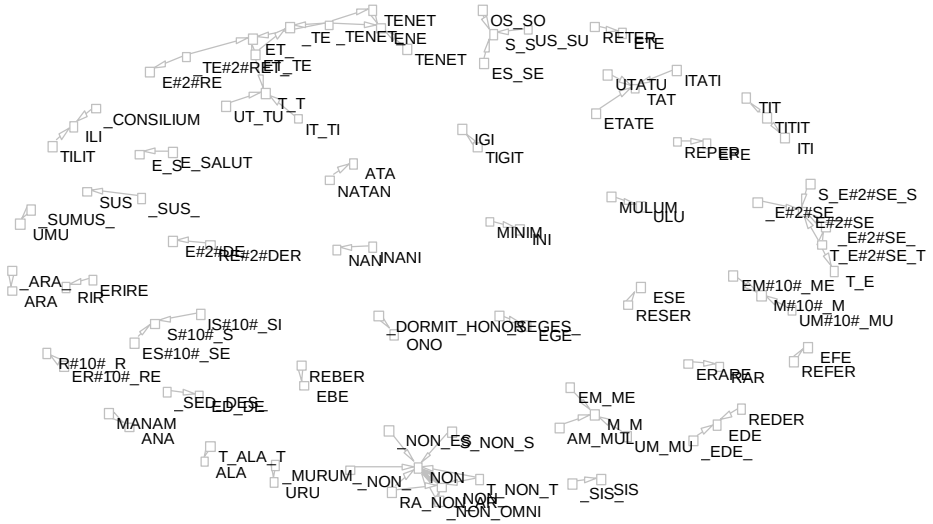
Einhardi en latin sans voyelles



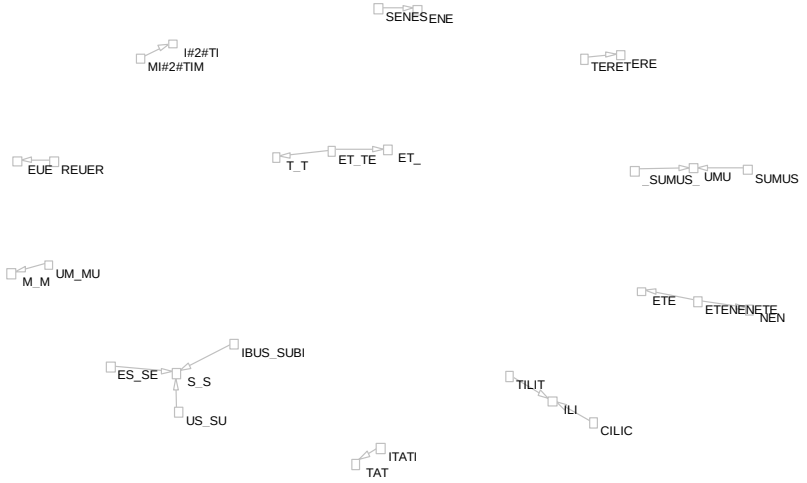
Einhardi en latin avec voyelles



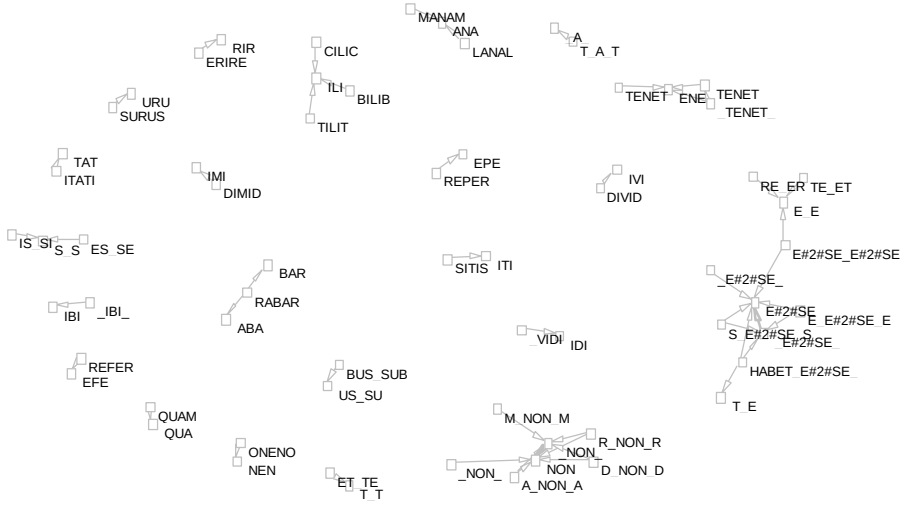
Anonymous en latin avec voyelles



Abroathis en latin avec voyelles



Dantes en latin avec voyelles



Erreur ! Argument de commutateur inconnu.

.

14 novembre 1998 —Première édition