Θεωρία Αναδρομικών Συναρτήσεων και Υπολογισιμότητας

Αθανάσιος Τζουβάρας

ΔΙΔΑΚΤΙΚΕΣ ΣΗΜΕΙΩΣΕΙΣ
(URL: http://users.auth.gr/ tzouvara)

Θεσσαλονίκη, Οκτώβριος 2004

Περιεχόμενα

Εισαγωγή

'Υπάρχουν' δύο ειδών μαθηματικά αντικείμενα: Τα αντικείμενα *πεπερασμένου τύπου* (finitistic) και τα *απειρικά* (non-finitistic). Δεν πρέπει να ταυτίζουμε τα πεπερασμένου τύπου αντικείμενα με τα πεπερασμένα σύνολα. Κάθε σύνολο πεπερασμένου τύπου είναι πεπερασμένο (ή ισοδύναμα, κάθε άπειρο σύνολο είναι απειρικό αντικείμενο) αλλά όχι αντίστροφα. Π.χ. το σύνολο $\{\sqrt{2}, 0\}$ είναι πεπερασμένο αλλά όχι πεπερασμένου τύπου, καθώς το $\sqrt{2}$ δεν είναι πεπερασμένου τύπου. Χονδρικά, πεπερασμένου τύπου αντικείμενο είναι αυτό που συνολικά περιέχει πεπερασμένου πλήθους μονάδες πληροφορίας (bits). Κατά συνέπεια, ο έλεγχος της ταυτότητας δύο τέτοιων αντικειμένων x, y, αν δηλαδή $x = y$, μπορεί να γίνει σε πεπερασμένο χρόνο, είτε από άνθρωπο είτε από μια μηχανή (πρόγραμμα). Αντίθετα, αν τα x, y είναι απειρικά, π.χ. δυό άπειρα σύνολα, ο έλεγχος της ισότητας $x = y$ παίρνει εν γένει άπειρο χρόνο (αν πρέπει να γίνει στοιχείο προς στοιχείο). Τα θεμελιώδη αντικείμενα πεπερασμένου τύπου είναι οι φυσικοί αριθμοί, δηλαδή τα στοιχεία του συνόλου

$$\mathbb{N} = \{0, 1, 2 \ldots\}.$$

Και κατόπιν ό,τι μπορεί να κατασκευασθεί, αναπαρασταθεί και κωδικοποιηθεί με φυσικούς αριθμούς. Τέτοια είναι: 1) Οι πεπερασμένες ακολουθίες φυσικών αριθμών. Κατά συνέπεια οι ακέραιοι και οι ρητοί αριθμοί (ως ζεύγη ακεραίων). 2) Τα πεπερασμένα σύνολα φυσικών αριθμών. 3) Τα πεπερασμένα σύνολα με στοιχεία πεπερασμένου τύπου αντικείμενα. Τα σύνολα αυτά στη θεωρία συνόλων λέγονται *κληρονομικά πεπερασμένα* (hereditarily finite). Είναι τα στοιχεία του συνόλου $V_\omega = \bigcup_{n\in\mathbb{N}} V_n$, όπου τα V_n ορίζονται επαγωγικά: $V_0 = \emptyset$, $V_{n+1} = P(V_n)$ ($P(X)$ παριστά το σύνολο των υποσυνόλων του X). 4) Αν $\Sigma = \{a, b, c, \ldots\}$, είναι ένα μηκενό σύνολο, το πολύ αριθμήσιμο, νοούμενο ως *αλφάβητο*, οι *λέξεις* που κατασκευάζονται με τα στοιχεία του Σ είναι πεπερασμένου τύπου αντικείμενα. Λέξεις είναι ακολουθίες γραμμάτων του αλφαβήτου: bbacca, aac, cbaca κλπ. Αντιστοιχώντας σε κάθε γράμμα μονοσήμαντα έναν φυσικό, π.χ. $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 2$, κλπ, οι λέξεις κωδικοποιούνται με ακολουθίες φυσικών που είναι πεπερασμένου τύπου αντικείμενα.

Απειρικό αντικείμενο είναι ό,τι περιέχει άπειρες μονάδες πληροφορίας. Π.χ. οι άπειρες μη περιοδικές ακολουθίες φυσικών, και ειδικότερα οι άρρητοι αριθμοί.

Οι αλγόριθμοι, οι κλασικοί τουλάχιστον με τους οποίους θα ασχοληθούμε εδώ, είναι εξ ορισμού μηχανικές διαδικασίες που εφαρμόζονται σε αντικείμενα πεπερασμένου τύπου. Αλλά και οι ίδιοι οι αλγόριθμοι είναι με τη σειρά τους αντικείμενα πεπερασμένου τύπου. Αυτό τους επιτρέπει να αφαρμόζονται και πάνω σε αλγορίθμους, πράγμα που έχει, όπως θα δούμε, πολύ ενδιαφέρουσες συνέπειες. Γι' αυτό στα επόμενα, τα βασικά σύνολα που εμπλέκονται είναι το $\mathbb{N}$ καθώς και τα καρτεσιανά γινόμενα $\mathbb{N}^k$, $k \geq 1$. Τα γράμματα $x, y, m, n, k, \ldots$ θα παριστούν φυσικούς αριθμούς. Τα στοιχεία του $\mathbb{N}^k$ είναι της μορφής $(x_1, \ldots, x_k)$, $x_i \in \mathbb{N}$. Για ευκολία θα χρησιμοποιούμε και διανυσματικό

συμβολισμό, γράφοντας απλώς $\overline{x}$ αντί για $(x_1, \ldots, x_k)$.

1 Η διαισθητική προσέγγιση του αλγορίθμου

1.1 Αλγοριθμικές συναρτήσεις και σύνολα

Αλγόριθμος είναι κάθε πεπερασμένο σύνολο οδηγιών-εντολών που απευθύνονται σε άνθρωπο ή μηχανή με σκοπό την κατασκευή ή ανεύρεση ενός αντικειμένου ή την απάντηση ενός ερωτήματος της μορφής ναι/όχι. Ο αλγόριθμος τροφοδοτείται με στοιχεία από ένα καλά ορισμένο σύνολο αντικειμένων πεπερασμένου τύπου. Τα στοιχεία αυτά λέγονται *είσοδοι* (inputs). Αμέσως με κάθε είσοδο ο αλγόριθμος αρχίζει να ''εκτελείται'', ή να ''τρέχει'', και μετά από κάποιο χρόνο δίνει μία το πολύ *έξοδο* (output), που είναι επίσης ένα αντικείμενο πεπερασμένου τύπου. Λέμε ''το πολύ'' για να συμπεριλάβουμε και την περίπτωση που δεν δίνει καμμία έξοδο για μια συγκεκριμένη είσοδο. Αν ο αλγόριθμος δίνει έξοδο για κάθε είσοδο, θα λέγεται *ολικός* (total). Μ' αυτή την ορολογία οι ολικοί αλγόριθμοι είναι τμήμα μόνον των αλγορίθμων γενικά.

Με τα σημερινά δεδομένα, και την κουλτούρα των υπολογιστών τόσο διαδεδομένη γύρω μας, η πιστότερη και ακριβέστερη εικόνα που μπορεί να έχει κανείς για τον αλγόριθμο, είναι αυτή ενός *προγράμματος υπολογιστή*. Φυσικά υπάρχουν και γενικότερες εικόνες: Κάθε είδους ''συνταγή'', από συνταγή μαγειρικής, και εξέταση αίματος, μέχρι ''συνταγή'' επίλυσης ενός γραμμικού συστήματος, είναι αλγόριθμος. Ο πιο γενικός ορισμός θα ήταν: Αλγόριθμος είναι κάτι που χρειάζεται αρκετή ευφυία και εμπειρία για να επινοήσεις, αλλά καθόλου ευφυία για να εκτελέσεις.

Ο παραπάνω είναι ο διαισθητικός/εμπειρικός ορισμός του αλγορίθμου. Διαισθητική προσέγγιση δεν σημαίνει μη αυστηρή. Σημαίνει μόνο ότι ο αλγόριθμος δεν είναι (ακόμη) κάποιο *συγκεκριμένο μαθηματικό αντικείμενο*. Δεν ανήκει δηλαδή ακόμη σε κάποια από τις γνωστές κατηγορίες μαθηματικών όντων (σύνολα, συναρτήσεις, κλπ). Όμως έστω και μ' αυτή την ασάφεια μπορούμε να πούμε αρκετά ενδιαφέροντα πράγματα για τη συμπεριφορά του. Αυτό θα κάνουμε σ' αυτό το κεφάλαιο.

Θα παριστάνουμε για τις ανάγκες αυτής της συζήτησης τους αλγορίθμους με τα κεφαλαία γράμματα A, B, Γ κλπ. Αντίθετα τα γράμματα X, Y, Z κλπ θα παριστάνουν υποσύνολα του $\mathbb{N}$ ή κάποιου $\mathbb{N}^k$. Έστω A ένας αλγόριθμος. Συμβολίζουμε με $in(A)$ και $out(A)$ τα σύνολα των εισόδων και εξόδων του A αντίστοιχα. Υστερα απ' όσα ειπώθηκαν στην εισαγωγή, χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $in(A) = \mathbb{N}^k$ και $out(A) \subseteq \mathbb{N}^l$ για κάποια $k, l \geq 0$. Αν $in(A) = \mathbb{N}^k$ και $\overline{x} \in in(A)$, ο συμβολισμός $A(\overline{x}) \downarrow$ σημαίνει ότι ο A σταματά και δίνει έξοδο οταν τροφοδοτηθεί με την είσοδο $\overline{x}$. Αν η έξοδος είναι ένα $\overline{y} \in out(A) \subseteq \mathbb{N}^l$, θα γράφουμε $A(\overline{x}) = \overline{y}$. Αν ο A δεν δίνει έξοδο στο $\overline{x}$, θα γράφουμε $A(\overline{x}) \uparrow$.

Βλέπουμε ότι ένας αλγόριθμος A με $in(A) = \mathbb{N}^k$ και $out(A) \subseteq \mathbb{N}^l$, παράγει μια συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}^l$. Η διαφορά της από τις συνηθισμένες συναρτήσεις που ξέρουμε

είναι ότι δεν είναι κατ' ανάγκη ολική, δηλαδή για ορισμένα $\overline{x} \in \mathbb{N}^k$ μπορεί να μην ορίζεται. Τέτοιες συναρτήσεις στα μαθηματικά τις λέμε *μερικές* και αποτελούν εξαίρεση μάλλον. Εδώ αντίθετα θα είναι ο κανόνας. Δηλαδή όταν λέμε *συνάρτηση* $f : \mathbb{N}^k \to \mathbb{N}^l$, θα εννοούμε *μερική* συνάρτηση, δηλ. μια αντιστοιχία f όπου σε κάθε $\overline{x} \in \mathbb{N}^k$ αντιστοιχεί ένα το πολύ $\overline{y} \in \mathbb{N}^l$. Π.χ η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ για την οποία $f(n) = \sqrt{n}$ είναι μερική. Το ίδιο και η συνάρτηση $g : \mathbb{N}^2 \to N$, όπου $g(m, n) = k$, όταν $m = n \cdot k$.

Το σύνολο X για το οποίο ορίζεται το $f(\overline{x})$ είναι το *πεδίο ορισμού* της f και συμβολίζεται $dom(f)$. Το *πεδίο τιμών* της f το συμβολίζουμε $rng(f)$. Εν γένει $dom(f) \subseteq \mathbb{N}^k$. Αν συμβεί $dom(f) = \mathbb{N}^k$, η f θα λέγεται *ολική*. Άρα οι ολικές συναρτήσεις θα είναι μέρος μόνον των συναρτήσεων γενικά. Όσο για την *ισότητα* των μερικών συναρτήσεων, ορίζεται ως εξής: Οι $f, g : \mathbb{N}^k \to \mathbb{N}^l$ είναι *ίσες* αν $dom(f) = dom(g)$ και για κάθε $\overline{x} \in dom(f)$, $f(\overline{x}) = g(\overline{x})$. (Σε πολλά βιβλία η ισότητα των μερικών συναρτήσεων συμβολίζεται με $\simeq$ αντί με $=$).

Ορισμός 1.1.1 Έστω συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}^l$. Η f θα λέγεται *αλγοριθμική* (computable) αν υπάρχει αλγόριθμος A τέτοιος ώστε για κάθε $\overline{x} \in \mathbb{N}^k$, $\overline{x} \in dom(f) \iff A(\overline{x}) \downarrow$ και αν $\overline{x} \in dom(f)$,τότε $f(\overline{x}) = A(\overline{x})$.

Παρατήρηση 1.1.2 Δεν πρέπει να ταυτίζουμε έναν αλγόριθμο A με τη συνάρτηση που παράγει. Ο λόγος είναι ότι υπάρχουν πολλοί (στην πραγματικότητα άπειροι) διαφορετικοί αλγόριθμοι που παράγουν την ίδια συνάρτηση. Πολύ περισσότερο, όπως θα δούμε αργότερα (Θεώρημα του Rice), δεν υπάρχει αλγόριθμος, που να αποφασίζει αν δυό αλγόριθμοι παράγουν την ίδια συνάρτηση.

Μια σημαντική κατηγορία αλγορίθμων είναι αυτοί απαντούν σε ερωτήματα της μορφής "$x \in X$;", όπου X κάποιο σύνολο. Οι έξοδοί τους προφανώς πρέπει να είναι "ναι" ή "όχι", δηλ. $out(A) \subseteq \{\text{ναι}, \text{όχι}\}$. Αυτοί λέγονται ναι/όχι αλγόριθμοι. Γράφοντας 1 αντί για "ναι" και 0 αντί για "όχι", δηλ. κάνοντας ώστε $out(A) \subseteq \{0, 1\}$, αμέσως βλέπουμε ότι αποτελούν απλώς μια ειδική περίπτωση των αλγορίθμων όπως ορίστηκαν παραπάνω. Πάντως θα εξακολουθήσουμε συχνά να γράφουμε $A(\overline{x}) = \text{ναι}$ ή $A(\overline{x}) = \text{όχι}$, καθώς βοηθάει τη διαίσθησή μας.

Ορισμός 1.1.3 Ένα σύνολο $X \subseteq \mathbb{N}^k$ λέγεται *αλγοριθμικό* (decidable) αν υπάρχει ολικός ναι/όχι αλγόριθμος A για το ερώτημα "$x \in X$;", δηλαδή, για κάθε $\overline{x} \in \mathbb{N}^k$,

$$\overline{x} \in X \;\Rightarrow\; A(\overline{x}) = \text{ναι}$$

καί

$$\overline{x} \notin X \;\Rightarrow\; A(\overline{x}) = \text{όχι}.$$

Έστω V ένα βασικό σύνολο, π.χ $V = \mathbb{N}^k$, και $X \subseteq V$. *Χαρακτηριστική συνάρτηση* του X, λέγεται η συνάρτηση $C_X : V \to \{0,1\}$ που ορίζεται ως εξής:

$$C_X(x) = \begin{cases} 1 & \text{αν } x \in X, \\ 0 & \text{αν } x \notin X. \end{cases}$$

Σημειώστε ότι κάθε χαρακτηριστική συνάρτηση είναι ολική. Η παρακάτω είναι προφανής.

Πρόταση 1.1.4 *Ένα σύνολο $X \subseteq \mathbb{N}^k$ είναι αλγοριθμικό αν και μόνον αν η χαρακτηριστική του συνάρτηση είναι (ολική) αλγοριθμική.*

Πρόταση 1.1.5 *Ένα σύνολο $X \subseteq \mathbb{N}^k$ είναι αλγοριθμικό αν και μόνον το $-X$ (δηλ. το $\mathbb{N}^k - X$) είναι αλγοριθμικό.*

Απόδειξη. Αν A είναι ολικός ναι/όχι αλγόριθμος για το X, τότε ο αλγόριθμος B ο οποίος δίνει "ναι" (αντ. "όχι") εκεί όπου ο A δίνει "όχι" (αντ. "ναι"), είναι ολικός αλγόριθμος για το $-X$. QED

Παραδειγματα

1) Κάθε σταθερή συνάρτηση, π.χ. $f(\overline{x}) = c$ για κάθε $\overline{x} \in \mathbb{N}^k$, είναι ολική αλγοριθμική. Επίσης η *συνάρτηση διαδοχής* των φυσικών αριθμών $S(n) = n + 1$. Το ίδιο η *πρόσθεση* και ο *πολλαπλασιασμός*. Για κάθε n και κάθε $m \leq n$, ορίζονται οι *προβολές* $\pi_{nm} : \mathbb{N}^n \to \mathbb{N}$, όπου $\pi_{nm}(x_1, \ldots, x_n) = x_m$. Προφανώς οι π_{nm} είναι ολικές αλγοριθμικές. (Οι σταθερές συναρτήσεις, οι προβολικές και η S, παίζουν βασικό ρόλο στον ορισμό της κλάσης των *αναδρομικών* συναρτήσεων που είναι μία από τις μαθηματικές τυποποιήσεις των αλγοριθμικών συναρτήσεων. Μ' αυτές θα ασχοληθούμε στο επόμενο κεφάλαιο.)

2) Ο γνωστός ευκλείδειος αλγόριθμος είναι ένας ολικός αλγόριθμος για τον υπολογισμό του μέγιστού κοινού διαιρέτη των $m, n \in \mathbb{N}$, $\text{ΜΚΔ}(m, n)$. Συνεπώς η συνάρτηση $\text{ΜΚΔ} : \mathbb{N}^2 \to \mathbb{N}$ είναι ολική αλγοριθμική.

3) Κάθε πεπερασμένο σύνολο είναι αλγοριθμικό. Πράγματι, έστω $X = \{\overline{x}_1, \ldots, \overline{x}_n\}$. Για το ερώτημα "$\overline{x} \in X$;" ο αλγόριθμος είναι: Εξέτασε βήμα-βήμα αν $\overline{x} = \overline{x}_1, \ldots, \overline{x} = \overline{x}_n$. Επειδή τα $\overline{x}$, $\overline{x}_i$ είναι *πεπερασμένου τύπου* (εδώ είναι που η ιδιότητα αυτή είναι αναγκαία), ο έλεγχος κάθε ισότητας $\overline{x} = \overline{x}_i$ γίνεται σε πεπερασμένο χρόνο.

4) Για το ερώτημα "είναι ο n πρώτος;", υπάρχει ως γνωστόν ολικός ναι/όχι αλγόριθμος. Άρα το σύνολο των πρώτων αριθμών είναι αλγοριθμικό.

5) Η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, όπου

$$f(n) = \text{το } n\text{-οστό δεκαδικό ψηφίο του } \pi,$$

είναι ολική αλγοριθμική. Το ίδιο και η συνάρτηση

$$g(n) = \left\{ \begin{array}{ll} 1 & \text{αν } f(n) = 7, \\ 0 & \text{αλλιώς.} \end{array} \right\}$$

6) Έστω η συνάρτηση

$$h(n) = \left\{ \begin{array}{ll} 1 & \text{αν υπάρχουν ακριβώς } n \text{ διαδοχικά 7 στο δεκαδ. μέρος του } \pi, \\ 0 & \text{αλλιώς.} \end{array} \right.$$

Εδώ ο μόνος γνωστός αλγόριθμος είναι ο εξής προφανής: Για κάθε n, ψάξε ένα-ένα τα δεκαδικά του π. Αν συναντήσεις n διαδοχικά 7, γράψε έξοδο 1. Αν όχι, τότε ο αλγόριθμος δεν τερματίζει στο n. Η h είναι εξ ορισμού ολική συνάρτηση, όμως ο παραπάνω αλγόριθμος *δεν ξέρουμε* αν είναι ολικός, και συνεπώς δεν ξέρουμε αν η h είναι αλγοριθμική σύμφωνα με τον ορισμό 1.1.1. (Για να το ξέρουμε θα έπρεπε να έχουμε εποπτεία ολόκληρου του δεκαδικού μέρους του π). Αυτή είναι μια κάπως παράδοξη κατάσταση, που έχει να κάνει με την διαφορά ανάμεσα στην κλασσική λογική που χρησιμοποιούμε (στα μαθηματικά και την καθημερινή ζωή) και που δέχεται ότι από ένα ζεύγος αντιφατικών προτάσεων ϕ και $\neg\phi$ μία ακριβώς είναι αληθής, και στη ''λογική των αλγορίθμων'', για την οποία το παραπάνω δεν ισχύει. Έτσι, ενώ για την κλασσική λογική η παραπάνω συνάρτηση είναι *ολική*, που σημαίνει ότι για κάθε n, *ή υπάρχουν* n διαδοχικά 7 στο π *ή δεν υπάρχουν*, για τον αλγόριθμο, αυτό δεν συμβαίνει ενόσω δεν μπορεί να πιστοποιήσει είτε το ένα είτε το άλλο.

7) Ένα πιο χτυπητό παράδειγμα για το φαινόμενο που αναφέραμε στο παράδειγμα 6 είναι η εξής συνάρτηση: Έστω

$$h(n) = \left\{ \begin{array}{ll} 1 & \text{αν η εικασία του Goldbach είναι αληθής,} \\ 0 & \text{αλλιώς.} \end{array} \right.$$

Λόγω κλασσικής λογικής, η παραπάνω συνάρτηση είναι ολική και μάλιστα *σταθερή*, άρα αλγοριθμική. Δεδομένου όμως ότι η εικασία του Goldbach είναι άλυτο μέχρι αυτή τη στιγμή πρόβλημα, κανένας από τους *γνωστούς* αλγορίθμους δεν παράγει την h. Μ' άλλα λόγια η h είναι αλγοριθμική χωρίς γνωστό αλγόριθμο!

8) Έστω $g : \mathbb{N}^{k+1} \to \mathbb{N}$ συνάρτηση $k+1$ μεταβλητών. Γράφουμε $g(\overline{x}, y)$ αντί $g(x_1, \ldots, x_k, y)$. Αν, δοθέντος $\overline{x}$, υπάρχει y τέτοιο ώστε $g(\overline{x}, y) = 1$, προφανώς θα υπάρχει ένα *ελάχιστο* y_0 τέτοιο ώστε $g(\overline{x}, y_0) = 1$. Συμβολίζουμε τότε

$$y_0 = (\mu y)(g(\overline{x}, y) = 1).$$

Ο τελεστής μ λέγεται *τελεστής ελαχιστοποίησης* (minimization), ή *μ-τελεστής*. Ορίζεται τότε η εξής (μερική) συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$:

$$f(\overline{x}) = \left\{ \begin{array}{ll} (\mu y)(g(\overline{x}, y) = 1) & \text{αν} \quad (\exists y)(g(\overline{x}, y) = 1), \\ \text{δεν ορίζεται αλλιώς,} & \end{array} \right.$$

Η f προφανώς είναι αλγοριθμική, όταν η g είναι τέτοια. Για να υπολογίσουμε το $f(\overline{x})$, αρκεί να υπολογίσουμε διαδοχικά τα $g(\overline{x},0)$, $g(\overline{x},1)$, κλπ, μέχρι να βρούμε (αν βρούμε) το πρώτο m για το οποίο $g(\overline{x},m)=1$. Τότε $f(\overline{x})=m$. Η ιδιότητα $g(\overline{x},y)=1$ λέγεται *κανονική* (regular) αν $(\forall\overline{x})(\exists y)(g(\overline{x},y)=1)$. Όταν η $g(\overline{x},y)=1$ είναι κανονική, προφανώς η f είναι ολική, αλλιώς δεν ορίζεται σε κάποια σημεία.

9) Το πιο ακραίο παράδειγμα μερικής αλγοριθμικής συνάρτησης είναι η συνάρτηση *που δεν ορίζεται πουθενά*, δηλαδή έχει πεδίο ορισμού $\emptyset$. Ας την παραστήσουμε με Ω. Η Ω μπορεί να ορισθεί με πολλούς τρόπους με τη βοήθεια του τελεστή μ, π.χ. ως εξής: $\Omega(x)=(\mu y)(x+y+2=1)$. Παρά τον τετριμμένο χαρακτήρα της η Ω είναι αρκετά χρήσιμη (δες π.χ. το Θεώρημα του Rice).

10) Υπάρχουν μη αλγοριθμικές συναρτήσεις και σύνολα; Ναι και μάλιστα πάρα πολλά, αν και δεν είναι εύκολο να δώσουμε συγκεκριμένο παράδειγμα. Είναι πολύ σημαντικό να πούμε από τώρα και να έχουμε συνεχώς στο μυαλό μας ότι ο κάθε αλγόριθμος, εκτός από το ότι εφαρμόζεται σε πεπερασμένου τύπου αντικείμενα, *είναι και ο ίδιος* αντικείμενο πεπερασμένου τύπου (αν και αυτή τη στιγμή πιθανόν να μην είναι εντελώς φανερό, θα γίνει όμως στα επόμενα). Αρκεί να παρατηρήσουμε ότι ο αλγόριθμος, ως πεπερασμένη ακολουθία εντολών, είναι πεπερασμένη ακολουθία λέξεων ενός αλφάβητου, και απ' όσα είπαμε στην εισαγωγή κωδικοποιείται με μια n-άδα φυσικών αριθμών. Δεδομένου τώρα ότι υπάρχουν μόνο αριθμησίμου πλήθους αντικείμενα πεπερασμένου τύπου, ενώ τα σύνολα όλων των υποσυνόλων του $\mathbb{N}$, και όλων των συναρτήσεων $f:\mathbb{N}\to\mathbb{N}$ είναι μη αριθμήσιμα, συμπεραίνουμε αμέσως ότι μόνο ένα ελάχιστο μέρος των υποσυνόλων αυτών και των συναρτήσεων είναι αλγοριθμικά. Από την άλλη μεριά, για να δώσουμε παράδειγμα τέτοιου συνόλου ή συνάρτησης, θα πρέπει να το ''περιγράψουμε''. Αλλά οι ''περιγραφές '' συνήθως αυτό που κάνουν είναι να δίνουν έναν αλγόριθμο, πράγμα ακριβώς που εμείς θέλουμε να αποφύγουμε. Γι' αυτό και τα παραδείγματα δεν είναι εύκολα. Στα επόμενα πάντως θα εμφανιστούν πολλά τέτοια σύνολα και συναρτήσεις.

Σημειώστε τώρα ότι υπάρχει κάποια ασυμμετρία ανάμεσα στους ορισμούς της αλγοριθμικής συνάρτησης και του αλγοριθμικού συνόλου. Η αλγοριθμική συνάρτηση απαιτεί την ύπαρξη απλώς αλγορίθμου (όχι κατ' ανάγκη ολικού), ενώ το αλγοριθμικό σύνολο απαιτεί *ολικό* ναι/όχι αλγόριθμο, ή ισοδύναμα ολικό αλγόριθμο για την χαρακτηριστική συνάρτηση. Θα δούμε σε λίγο ότι το ακριβές ανάλογο της αλγοριθμικής συνάρτησης δεν είναι το αλγοριθμικό σύνολο, αλλά μια ασθενέστερη έννοια, το *αλγοριθμικά απαριθμήσιμο*. Προηγουμένως ας θυμηθούμε ότι στη Θεωρία Συνόλων, και στα μαθηματικά γενικότερα, μαθαίνουμε να ορίζουμε τη συνάρτηση ως ένα σύνολο ζευγών. Συγκεκριμένα, είναι βολικό να δεχόμαστε ότι για κάθε συνάρτηση f, $f=\{(x,y):y=f(x)\}$. Αυτή είναι η *εκτατική* (extensional) έννοια της συνάρτησης. Από τη σκοπιά όμως της Θεωρίας Αλγορίθμων, αυτό δεν ισχύει. Εδώ η συνάρτηση f δεν είναι σύνολο, αλλά μια

διαδικασία αντιστοίχισης μιας εξόδου $f(x)$ σε μια είσοδο x, που καθορίζεται από έναν νόμο (αλγόριθμο). Έμφαση δίνεται στην ''περιγραφή'' (intension) του νόμου αντιστοιχίας. Βέβαια, για κάθε f, πάλι ορίζεται ένα σύνολο $\{(x,y) : y = f(x)\}$, όμως δεν το ταυτίζουμε με την f. Το λέμε *γράφημα* της f και το συμβολίζουμε $G(f)$. Δηλαδή σε κάθε f αντιστοιχεί το σύνολο

$$G(f) = \{(x,y) : y = f(x)\}.$$

Ένα φυσικό ερώτημα είναι: Ποιά η σχέση ανάμεσα στην αλγοριθμικότητα της f και εκείνη του συνόλου $G(f)$; Για απλότητα γραφής συχνά στα επόμενα θεωρούμε συναρτήσεις $f : \mathbb{N} \to \mathbb{N}$ αντί $f : \mathbb{N}^k \to \mathbb{N}^l$. Αυτό σε τίποτα δεν βλάπτει τη γενικότητα, και τα ίδια ισχύουν για τη γενικότερη περίπτωση.

Πρόταση 1.1.6 *Έστω $f : \mathbb{N} \to \mathbb{N}$. (i) Αν το $G(f)$ είναι αλγοριθμικό, η f είναι αλγοριθμική. Το αντίστροφο γενικά δεν ισχύει. (ii) Αν όμως η f είναι ολική τότε ισχύει και το αντίστροφο του (i) δηλαδή*

$$f \text{ αλγοριθμική} \iff G(f) \text{ αλγοριθμικό.}$$

Απόδειξη. (i) Έστω $G(f)$ αλγοριθμικό με αλγόριθμο B. Έστω ο αλγόριθμος A:

$$A(m) = \begin{cases} n & \text{αν} \quad B(m,n) = \text{ναι}, \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Ο A δουλεύει ως εξής: Δοθέντος m, εξετάζουμε διαδοχικά τις εξόδους $B(m,0)$, $B(m,1)\ldots$. Για το πρώτο n που θα βρούμε (αν βρούμε) τέτοιο ώστε $B(m,n) = \text{ναι}$, θέτουμε $A(m) = n$. Ενδέχεται για κάποιο m, να μην υπάρχει n τέτοιο ώστε $B(m,n) = \text{ναι}$ (σε περίπτωση που το $G(f)$ είναι γράφημα μερικής συνάρτησης), οπότε ο A δεν είναι ολικός. Είναι εύκολο να δούμε ότι ο A είναι αλγόριθμος για την f. Πράγματι, $f(m)\downarrow$ και $f(m) = n \iff (m,n) \in G(f) \iff B(m,n) = \text{ναι} \iff A(m)\downarrow$ και $A(m) = n$. Άρα f αλγοριθμική.

(ii) Έστω ότι η f είναι ολική συνάρτηση. Η κατεύθυνση $\Leftarrow$ της ισοδυναμίας ισχύει λόγω του (i). Για το αντίστροφο, έστω A ένας ολικός αλγόριθμός της f. Δηλαδή $f(m) = n \Leftrightarrow A(m) = n$. Θεωρούμε τον εξής αλγόριθμο B με $in(B) \subseteq \mathbb{N}^2$:

$$B(m,n) = \begin{cases} \text{ναι αν} & A(m) = n, \\ \text{όχι αν} & A(m) \neq n. \end{cases}$$

Αφού ο A είναι ολικός και ο B είναι ολικός και προφανώς $B(m,n) = \text{ναι} \Leftrightarrow (m,n) \in G(f)$, άρα $G(f)$ αλγοριθμικό. (Αν η f δεν είναι ολική, ο A δεν είναι ολικός, και προφανώς ο B δεν είναι ολικός, οπότε δεν μπορούμε να συμπεράνουμε την αλγοριθμικότητα του $G(f)$.) QED.

Ορισμός 1.1.7 Ένα σύνολο $X \subseteq \mathbb{N}^k$ λέγεται *αλγοριθμικά απαριθμήσιμο* ή για συντομία *α.α.* (effectively enumerable ή listable), αν υπάρχει ναι/όχι αλγόριθμος A (όχι κατ' ανάγκη ολικός) τέτοιος ώστε για κάθε $\overline{x} \in \mathbb{N}^k$,

$$\overline{x} \in X \Leftrightarrow A(\overline{x}) \downarrow \text{ καί } A(\overline{x}) = \text{ναι}.$$

Παρατηρήστε ότι από την παραπάνω ισοδυναμία, $\overline{x} \notin X$ δεν συνεπάγεται $A(\overline{x}) = $ όχι, αλλά $A(\overline{x}) \uparrow$ ή $A(\overline{x}) = $ όχι. Από τον ορισμό αυτό και τον ορισμό 1.1.3 προκύπτει ότι *κάθε αλγοριθμικό σύνολο είναι α.α.* Διαισθητικά ένα α.α. σύνολο είναι ''μισο-αλγοριθμικό'' με την εξής έννοια:

Πρόταση 1.1.8 *Το $X \subseteq \mathbb{N}^k$ είναι αλγοριθμικό αν και μόνον αν το X και το $-X$ (δηλ. το $\mathbb{N}^k - X$) είναι α.α.*

Απόδειξη. Έστω X αλγοριθμικό. Από την Πρόταση 1.1.5, το $-X$ είναι επίσης αλγοριθμικό. Άρα (εξ ορισμού) τα X, $-X$ είναι α.α. Αντίστροφα έστω ότι τα X, $-X$ είναι α.α. με αλγορίθμους π.χ. A, B αντίστοιχα. Θεωρήστε τον αλγόριθμο Γ:

$$\Gamma(\overline{x}) = \begin{cases} \text{ναι} & \text{αν } A(\overline{x}) = \text{ναι}, \\ \text{όχι} & \text{αν } B(\overline{x}) = \text{ναι}. \end{cases}$$

Προφανώς ο Γ είναι ολικός αλγόριθμος για το X. QED

Ο όρος ''αλγοριθμικά απαριθμήσιμο'' προέρχεται από μια ισοδύναμη περιγραφή αυτών των συνόλων που συχνά χρησιμοποιείται και ως ορισμός τους.

Προηγουμένως θα χρειαστεί για πρώτη φορά να μιλήσουμε για τον *χρόνο αναμονής* μέχρι να πάρουμε έξοδο σε μία είσοδο, μια έννοια θεμελιώδη στη θεωρία αλγορίθμων. Αν ο αλγόριθμος είναι ένα πρόγραμμα, τότε ο χρόνος αναμονής για την έξοδο $A(\overline{x})$, είναι ο αριθμός των *βημάτων* που κάνει το πρόγραμμα μέχρι να υπολογίσει το $A(\overline{x})$ (υποθέτοντας ότι κάνει ένα βήμα ανά μονάδα χρόνου). Αυτή η έννοια του βήματος μπορεί να γίνει απόλυτα σαφής στις διάφορες τυποποιήσεις του αλγορίθμου, ιδίως στις μηχανές Turing. Σε κάθε αλγόριθμο A με $in(A) = \mathbb{N}^k$ και $out(A) \subseteq \mathbb{N}^l$, αντιστοιχεί ένας *ολικός* ναι/όχι αλγόριθμος T_A με $in(T_A) \subseteq \mathbb{N}^{k+l+1}$ που ορίζεται ως εξής:

$$T_A(\overline{x}, \overline{y}, z) = \begin{cases} \text{ναι αν} & A(\overline{x}) = \overline{y} \text{ σε } \leq z \text{ βήματα}, \\ \text{όχι αλλιώς}, & \end{cases}$$

όπου η έκφραση ''$A(\overline{x}) = \overline{y}$ σε $\leq z$ βήματα'' σημαίνει: Ο αλγόριθμος A με είσοδο $\overline{x}$ δίνει έξοδο $\overline{y}$ το πολύ σε z βήματα. Θα ονομάζουμε τον T_A *αλγόριθμο αναμονής* του A. Ότι ο A είναι ολικός (ακόμα κι όταν ο A δεν είναι ολικός) είναι φανερό απ' τον ορισμό. Σε κάθε είσοδο $(\overline{x}, \overline{y}, z)$ του T_A, δεν έχουμε παρά να δώσουμε στον A είσοδο $\overline{x}$ και να

περιμένουμε το πολύ z μονάδες χρόνου. Αν σ' αυτό το διάστημα δεν έρθει απάντηση, ή ερθει και είναι διάφορη του $\overline{y}$, ο T_A απαντά ''όχι'', αλλιώς απαντά ''ναι''. Προφανώς ισχύει για κάθε $\overline{x}$

$$A(\overline{x}) = \overline{y} \Longleftrightarrow (\exists z)(T_A(\overline{x}, \overline{y}, z) = \text{ναι}). \tag{1}$$

Αν ο A είναι ναι/όχι αλγόριθμος, ο T_A είναι απλούστερος. Συγκεκριμένα ορίζουμε:

$$T_A(\overline{x}, z) = \begin{cases} \text{ναι αν} \quad A(\overline{x}) = \text{ναι σε } \leq z \text{ βήματα}, \\ \text{όχι αλλιώς}. \end{cases}$$

Οπότε η (1) γίνεται

$$A(\overline{x}) = \text{ναι} \Longleftrightarrow (\exists z)(T_A(\overline{x}, z) = \text{ναι}). \tag{2}$$

Πρόταση 1.1.9 *Το $X \subseteq \mathbb{N}^k$ είναι α.α. αν και μόνον αν είναι πεδίο τιμών μιας ολικής αλγοριθμικής συνάρτησης $f : \mathbb{N} \to \mathbb{N}^k$.*

Απόδειξη. Για απλότητα έστω $X \subseteq \mathbb{N}$ (η απόδειξη για το $\mathbb{N}^k$ δεν έχει καμμιά διαφορά) και έστω $X = rng(f)$, όπου $f : \mathbb{N} \to \mathbb{N}$ ολική αλγοριθμική. Μ' άλλα λόγια $X = \{f(0), f(1), \ldots\}$. Ο προφανής αλγόριθμος A για το X είναι: Δοθέντος $x \in \mathbb{N}$, έλεγξε αν $x = f(0)$, αν $x = f(1)$, ..., $x = f(n), \ldots$. (Επειδή f ολική αλγοριθμική, το $f(n)$ υπολογίζεται πάντα.) Αν για κάποιο n, $x = f(n)$ ο αλγόριθμος απαντά ''ναι''. Αλλιώς δεν απαντά. Δηλαδή:

$$A(x) = \begin{cases} \text{ναι αν} \quad (\exists n)(x = f(n)), \\ \text{δεν ορίζεται αλλιώς}. \end{cases}$$

Προφανώς $x \in X \Longleftrightarrow A(x) \downarrow$ και $A(x) = \text{ναι}$. Άρα το X είναι α.α.

Αντίστροφα, έστω $X \subseteq \mathbb{N}$ α.α. και A ένας αλγόριθμός του. Θέλουμε να βρούμε ολική αλγοριθμική $f : \mathbb{N} \to \mathbb{N}$ τέτοια ώστε $X = rng(f)$. Η ιδέα θα ήταν να εισάγουμε ένα-ένα τα $0, 1, \ldots, n, \ldots$ στον A και να περιμένουμε τις εξόδους $A(0)$, $A(1), \ldots, A(n), \ldots$. Κάθε φορά που θα έρχεται μία έξοδος $A(k) = \text{ναι}$, και με τη σειρά που έρχεται, να βάζουμε το k στην αντίστοιχη θέση μιας ακολουθίας $x_0, x_1, \ldots, x_n, \ldots$. Οπότε, αν $f(n) = x_n$, $X = rng(f)$ και f είναι ολική αλγοριθμική. Η ιδέα είναι σωστή γενικά, μόνο που για κάθε $k \in \mathbb{N}$ *δεν ξέρουμε πόσο χρόνο πρέπει να περιμένουμε* για να πάρουμε απάντηση (διότι μπορεί να μην πάρουμε ποτέ απάντηση). Γιά κάθε είσοδο k στον A, πρέπει να εξαντλήσουμε όλες τις δυνατές χρονικές αναμονές και σ' αυτό είναι χρήσιμος ο αλγόριθμος αναμονής T_A του A. Από την (2) πιο πάνω έχουμε ότι $T_A(m, n) = \text{ναι}$ σημαίνει ότι $A(m) = \text{ναι}$ το πολύ σε n βήματα. Άρα αρκεί να τροφοδοτήσουμε τον T_A με όλα τα ζεύγη (m, n) της μορφής $m \leq n$ με την εξής σειρά: $(0,0)$, $(0,1)$, $(1,1)$, $(0,2)$, $(1,2)$, $(2,2)$, κλπ. Κάθε φορά που για το ζεύγος (m, n)

έρχεται απάντηση ''ναι'', και με τη σειρά που έρχεται, βάζουμε το m στην αντίστοιχη θέση της σχηματιζόμενης ακολουθίας $x_0, x_1, \ldots$. Μ' αυτόν τον τρόπο αν $m \in X$, όσο χρόνο και να πάρει για την απάντηση του $A(m)$, ο αλγόριθμος θα το συλλάβει. Εστω ότι η απάντηση έρχεται σε χρόνο k. Αν $k \geq m$, το ζεύγος $(m,k) \in in(T_A)$ και $T_A(m,k)$ =ναι. Αν $k < m$, τότε προφανώς $T_A(m,m)$ =ναι (αφού η απάντηση έρχεται σε $\leq m$ βήματα). Άρα σε κάθε περίπτωση το m θα συμπεριληφθεί στα στοιχεία της ακολουθίας. Συνεπώς $X = \{x_0, x_1, \ldots\}$ και αν $f(n) = x_n$, f ολική αλγοριθμική και $X = rng(f)$. Αν θέλει κανείς να είναι πιο αυστηρός, η f ορίζεται επαγωγικά ως εξής:

$f(n) = m$, αν υπάρχει k τέτοιο ώστε $T_A(m,k)$=ναι και το ζεύγος (m,k) είναι το n-οστό μ' αυτήν την ιδιότητα στην παραπάνω διάταξη των ζευγών. QED

Η διάταξη των ζευγών (m,n), με $m \leq n$ στην πιο πάνω απόδειξη μπορεί να γραφεί και ως εξής:

$$
\begin{array}{llll}
(0,0) & & & \\
(0,1), & (1,1) & & \\
(0,2), & (1,2), & (2,2) & \\
(0,3), & (1,3), & (2,3), & (3,3) \\
\multicolumn{4}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots}
\end{array}
$$

Η αναζήτηση γίνεται από πάνω προς τα κάτω και από αριστερά προς τα δεξιά. Λόγω του σχήματος της διάταξης, αλγόριθμοι αυτού του είδους λέγονται *ουρά περιστεριού* (dovetailing) και θα χρησιμοποιηθούν αρκετές φορές στη συνέχεια. Τη διάταξη επίσης αυτή των ζευγών (m,n), $m \leq n$, $((0,0),(1,0),(1,1),\ldots)$ θα τη λέμε ουρά περιστεριού και θα την παριστάνουμε $<_{DT}$. Αυστηρά μιλώντας για ζεύγη (x,y), (z,u) με $x \leq y$, $z \leq u$,

$$(x,y) <_{DT} (z,u) \iff (y < u) \text{ ή } (y = u \text{ και } x < z)^1.$$

Πρόταση 1.1.10 *Έστω $f : \mathbb{N} \to \mathbb{N}$. Η f είναι αλγοριθμική αν και μόνον αν το $G(f)$ είναι α.α.*

Απόδειξη. Έστω $f : \mathbb{N} \to \mathbb{N}$ αλγοριθμική και έστω A ένας αλγόριθμός της. Θεωρούμε τον αλγόριθμο B:

$$B(m,n) = \begin{cases} \text{ναι} & \text{αν } A(m)\downarrow \text{ και } A(m) = n \\ \text{δεν ορίζεται αλλιώς.} & \end{cases}$$

[1] Φυσικά αντί για τη διάταξη $<_{DT}$ μπορεί κανείς να πάρει μια *οποιαδήποτε* διάταξη *όλων* των ζευγών (m,n) υπό μορφή ακολουθίας και να τα εξετάσει ένα-ένα. Π.χ. μπορεί να διατάξει τα (m,n) ως εξής: $(0,0),(0,1),(1,0)(0,2),(1,1),(2,0),(0,3),\ldots$. Απλώς η διάταξη $\leq$ είναι ''οικονομικότερη'', αφού περιλαμβάνει τα μισά μόνο από τα ζεύγη του $\mathbb{N}^2$.

Προφανώς ο B είναι αλγόριθμος για το $G(f)$, δηλ. $(m,n) \in G(f) \iff B(m,n) \downarrow$ και $B(m,n) =$ ναι. Άρα $G(f)$ α.α. Αντίστροφα, έστω B αλγόριθμος για το $G(f)$. Έστω T_B ο αλγόριθμος αναμονής του B, με εισόδους $((m,n),k)$. Τότε

$$f(m) = \begin{cases} n, \text{ αν } (\exists k)(T_B((m,n),k) = \text{ναι}), \\ \text{δεν ορίζεται, αλλιώς.} \end{cases}$$

Συνεπώς ένας αλγόριθμος για την f είναι ο εξής A:

$$A(m) = \begin{cases} n \quad \text{αν } (\exists k)(T_B((m,n),k) = \text{ναι}), \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Ο A είναι η εξής ουρά περιστεριού: Έστω $(0,0)$, $(0,1)$, $(1,1), \ldots$, η διάταξη $<_{DT}$ των ζευγών (n,k) με $n \leq k$. Γιά κάθε $m \in \mathbb{N}$, εισάγουμε στον T_B μία-μία τις εισόδους $(m,0,0)$, $(m,0,1)$, $(m,1,1)$ κλπ. Αν και όταν ο T_B απαντήσει ''ναι'' σε κάποιο (m,n,k), γράφουμε $A(m) = n$. Αλλιώς $A(m) \uparrow$. Προφανώς ο A είναι αλγόριθμος για τη f. QED

Εκτός από αυτή της Πρότασης 1.1.9, υπάρχουν κι άλλες ισοδύναμες περιγραφές των α.α. συνόλων.

Πρόταση 1.1.11 *Έστω $X \subseteq \mathbb{N}$ άπειρο. Τα παρακάτω είναι ισοδύναμα:*

(α) Το X είναι α.α.

(β) Το X είναι πεδίο τιμών μιας αλγοριθμικής συνάρτησης.

(γ) Το X είναι πεδίο ορισμού μιας αλγοριθμικής συνάρτησης.

(δ) Το X είναι πεδίο τιμών μιας ολικής 1-1 αλγοριθμικής συνάρτησης.

Απόδειξη. (α) $\Rightarrow$ (β): Αυτό έπεται αμέσως από την Πρόταση 1.1.9.

(β)$\Rightarrow$ (γ): Έστω $X = rng(f)$, όπου f αλγοριθμική, με αλγόριθμο A. Θέλουμε να ορίσουμε ένα είδος ''αντίστροφου'' αλγορίθμου B, δηλαδή, αν $B(m) = n$, τότε $A(n) = m$. Επειδή η f δεν είναι κατ' ανάγκη 1-1, χρησιμοποιούμε τον αλγόριθμο αναμονής T_A του A. Ο B είναι η εξής ουρά περιστεριού: Δοθέντος m, τροφοδοτούμε τον T_A διαδοχικά με τις τριάδες (n,m,k), για όλα τα ζεύγη (n,k) με $n \leq k$, διατεταγμένα με τη διάταξη $\leq_{DT}$ που ορίστηκε πιο πάνω. Αν (n,k) είναι το ελάχιστο ζεύγος στην παραπάνω διάταξη για το οποίο $T_A(n,m,k) =$ ναι (αν υπάρχει τέτοιο ζεύγος), θέτουμε $B(m) = n$. Διαφορετικά $B(m) \uparrow$. Συνοπτικά ο B γράφεται:

$$B(m) = \begin{cases} n \quad \text{αν } \exists k \; T_A(n,m,k) = \text{ναι και } (n,k) \text{ είναι το ελάχιστο ζεύγος} \\ \qquad \text{στην διάταξη } <_{DT} \text{ μ' αυτή την ιδιότητα,} \\ \text{δεν ορίζεται αλλιώς} \end{cases}$$

Προφανώς αν $B(m) = n$, τότε $A(n) = m$. Συνεπώς αν g είναι η συνάρτηση που ορίζει ο B, τότε $dom(g) \subseteq rng(f)$. Αλλά και αντίστροφα, αν $m \in rng(f)$, τότε $T_A(x, m, y)$=ναι για κάποιο ζεύγος (x, y). Άρα αν (n, k) είναι το ελάχιστο τέτοιο ζεύγος στη διάταξη $\leq_{DT}$, τότε $B(m) = n$, δηλαδή $g(m) = n$, και συνεπώς $m \in dom(g)$. Οπότε $dom(g) = rng(f) = X$.

(γ)⇒ (α): Έστω $X = dom(f)$, όπου f αλγοριθμική με αλγόριθμο A. Θεωρήστε τον αλγόριθμο B:

$$B(n) = \begin{cases} \text{ναι} & \text{αν } A(n)\downarrow, \\ \text{δεν ορίζεται αλλιώς} \end{cases}$$

Τότε $n \in X \iff n \in dom(f) \iff A(n)\downarrow \iff B(n)\downarrow$ και $B(n) =$ ναι. Άρα X α.α.

(δ)⇒ (α): Άμεσο από την Πρόταση 1.1.9.

(α)⇒ (δ): Πάλι από την Πρ. 1.1.9 υποθέτουμε ότι $X = rng(f)$, όπου f ολική αλγοριθμική. Θέλουμε να βρούμε 1-1 ολική αλγοριθμική g τέτοια ώστε $X = rng(g)$. Η g ορίζεται ως εξής:

$g(0) = f(0)$ και

$g(n+1) = f(m)$, όπου m είναι ο ελάχιστος x για τον οποίο

$$f(x) \notin \{g(0), \ldots, g(n)\}.$$

[Συνοπτικότερα η τελευταία σχέση γράφεται με τη χρήση του τελεστού ελαχιστοποίησης μ ως εξής:

$g(n+1) = f((\mu x)[f(x) \notin \{g(0), \ldots, g(n)\}])$.]

Επειδή το $X = rng(f)$ είναι άπειρο (εδώ μας χρειάζεται η απειρότητα του X), για κάθε n, $X - \{g(0), \ldots, g(n)\} \neq \emptyset$, άρα πάντα θα υπάρχει x τέτοιο ώστε $f(x) \notin \{g(0), \ldots, g(n)\}$, και συνεπώς η g ορίζεται σ' όλο το $\mathbb{N}$. Προφανώς η g είναι αλγοριθμική, 1-1 και $rng(g) = rng(f) = X$ (αποδείξτε το τελευταίο). QED

Ο καλύτερος χαρακτηρισμός που δώσαμε μέχρι τώρα για τα (άπειρα) α.α. συνολα $X \subseteq \mathbb{N}$ είναι ότι αποτελούν πεδίο τιμών μιας ολικής 1-1 αλγοριθμικής $f : \mathbb{N} \to \mathbb{N}$. Μήπως μπορούμε να βελτιώσουμε τον χαρακτηρισμό, και να έχουμε π.χ. *αύξουσα* f αντί για 1-1; Η απάντηση είναι όχι. Αν αντικαταστήσουμε την συνθήκη 1-1 με ''αύξουσα'' παίρνουμε *αλγοριθμικά* σύνολα και όχι απλώς α.α.

Θυμίζουμε ότι η $f : \mathbb{N} \to \mathbb{N}$ λέγεται *αύξουσα* αν $m < n \Rightarrow f(m) \leq f(n)$ και *αυστηρά αύξουσα* αν $m < n \Rightarrow f(m) < f(n)$. Κατ'αρχήν έχουμε το ακόλουθο.

Πρόταση 1.1.12 *Αν $X \subseteq \mathbb{N}$ αλγοριθμικό, υπάρχει $f : \mathbb{N} \to \mathbb{N}$ ολική αλγοριθμική και αύξουσα, τέτοια ώστε $X = rng(f)$. Αν το X είναι άπειρο, η παραπάνω f είναι αυστηρά αύξουσα. (Μ' άλλα λόγια, κάθε άπειρο αλγοριθμικό $X \subseteq \mathbb{N}$ έχει μία αλγοριθμική γνησίως αύξουσα απαρίθμηση των στοιχείων του.)*

Απόδειξη. Έστω $X \subseteq \mathbb{N}$ αλγοριθμικό. Ορίζουμε:

$f(0) =$ ελάχιστο στοιχείο του X,
$f(n+1) =$ ελάχιστο στοιχείο του $X - \{f(0), \ldots, f(n)\}$
αν $X - \{f(0), \ldots, f(n)\} \neq \emptyset$,
$= f(n)$ αλλιώς.

Επειδή X αλγοριθμικό είναι εύκολο να δούμε ότι η f είναι ολική αλγοριθμική. Επίσης η f είναι αύξουσα και $X = rng(f)$. Τέλος, ο μόνος λόγος για να μην είναι η f αυστηρά αύξουσα, θα ήταν το X να είναι πεπερασμένο. QED

Ισχύει και το αντίστροφο του προηγουμένου. Προηγουμένως χρειαζόμαστε το εξής απλό:

Λήμμα 1.1.13 *Αν η $f : \mathbb{N} \to \mathbb{N}$ είναι αυστηρά αύξουσα, τότε $f(n) \geq n$ για κάθε $n \in \mathbb{N}$.*

Απόδειξη. Με επαγωγή στο n. Προφανώς $f(0) \geq 0$. Έστω $f(n) \geq n$. Από την υπόθεση $f(n+1) > f(n)$. Άρα $f(n+1) > f(n) \geq n$, οπότε $f(n+1) \geq n+1$. QED

Πρόταση 1.1.14 *Αν η $f : \mathbb{N} \to \mathbb{N}$ είναι αυστηρά αύξουσα, το $X = rng(f)$ είναι αλγοριθμικό.*

Απόδειξη. Όπως έχουμε δει, $n \in X \iff (\exists m)(f(m) = n)$. Όμως από το προηγούμενο Λήμμα, $f(m) \geq m$, δηλαδή αν $f(m) = n$ τότε $m \leq n$. Άρα η παραπάνω ισοδυναμία γράφεται στην περίπτωση που η f είναι αυστηρά αύξουσα:

$$n \in X \iff (\exists m \leq n)(f(m) = n).$$

Αυτό σημαίνει ότι για να ελέγξουμε αν $n \in X$, αρκεί να ελέγξουμε μόνο αν $n = f(0)$, $n = f(1), \ldots, n = f(n)$ (δηλαδή η αναζήτηση είναι φραγμένη). Αυτό προφανώς συνιστά ολικό ναι/όχι αλγόριθμο για το ερώτημα "$n \in X$;". QED

Από τις Προτάσεις 1.1.12 και 1.1.14 προκύπτει το ακόλουθο:

Πόρισμα 1.1.15 *Ένα άπειρο $X \subseteq \mathbb{N}$ είναι αλγοριθμικό αν και μόνον αν έχει μία αυστηρά αύξουσα απαρίθμηση (είναι πεδίο τιμών μιας αύστηρά αύξουσας $f : \mathbb{N} \to \mathbb{N}$).*

Ασκήσεις

1.1.1 Δείξτε ότι το σύνολο των αλγοριθμικών υποσυνόλων του $\mathbb{N}$ (ή του $\mathbb{N}^k$) είναι κλειστό ως προς ένωση, τομή, συμπλήρωμα και καρτεσιανό γινόμενο.

1.1.2 Δείξτε ότι αν τα X, Y είναι α.α., το ίδιο είναι και τα $X \cup Y$, $X \cap Y$, $X \times Y$.

1.1.3 Αν $X \subseteq \mathbb{N}$ αλγοριθμικό και $f : \mathbb{N} \to \mathbb{N}$ ολική αλγοριθμική, τι συμπεραίνετε για τα σύνολα $f(X) = \{f(x) : x \in X\}$ και $f^{-1}(X) = \{x : f(x) \in X\}$;

1.1.4 Έστω X_n, $n \in \mathbb{N}$, αλγοριθμικά σύνολα. Είναι το $\bigcup_n X_n$ αλγοριθμικό;

1.1.5 Δείξτε ότι κάθε άπειρο α.α.σύνολο $X \subseteq \mathbb{N}$ περιέχει ένα αλγοριθμικό υποσύνολο. (Χρησιμοποιήστε το Πόρισμα 1.1.15.)

1.1.6 Περιγράψτε τον ολικό αλγόριθμο της συνάρτησης f που απαριθμεί το X στην απόδειξη της πρότασης 1.1.12

1.1.7 Αν f, g ολικές αλγοριθμικές και το σύνολο X ορίζεται από τη σχέση

$$n \in X \iff (\exists x \leq g(n))(f(x) = 0),$$

δείξτε ότι το X είναι αλγοριθμικό.

1.1.8 Δείξτε ότι το $X \subseteq \mathbb{N}$ είναι α.α. αν και μόνον αν υπάρχει αλγοριθμικό $Y \subseteq \mathbb{N}^2$ τέτοιο ώστε για κάθε $x \in \mathbb{N}$, $x \in X \iff (\exists n)((n, x) \in Y)$.

1.1.9 Δείξτε ότι συνάρτηση g που ορίστηκε στην απόδειξη της πρότασης 1.1.11 έχει το ίδιο πεδίο τιμών με την f, δηλαδή $rng(g) = rng(f) = X$.

1.2 Αλγοριθμικοί ισομορφισμοί

Έστω $X \subseteq \mathbb{N}^k$ και $Y \subseteq \mathbb{N}^l$. Μία ολική συνάρτηση $f : X \to Y$ λέγεται *αλγοριθμικός ισομορφισμός* (α.ι. για συντομία) αν είναι αλγοριθμική, 1-1 και επί. Αν περιοριστούμε σε συναρτήσεις $f : \mathbb{N}^k \to \mathbb{N}^k$ είναι εύκολο να δει κανείς ότι η σύνθεση α.ι. είναι α.ι., η αντίστροφη α.ι. είναι α.ι. και φυσικά η ταυτοτική απεικόνιση είναι α.ι. Άρα το σύνολο των α.ι. στο $\mathbb{N}^k$ είναι μια ομάδα. Πρώτα όμως πρέπει να βεβαιώσουμε την ύπαρξη μη τετριμμένων α.ι. Η παρακάτω πρόταση είναι πολύ παλιά (οφείλεται στον Cantor) και δίνει έναν α.ι. μεταξύ του $\mathbb{N}$ και του $\mathbb{N}^2$.

Πρόταση 1.2.1 *Η συνάρτηση $J : \mathbb{N}^2 \to \mathbb{N}$ που ορίζεται από τη σχέση*

$$J(m, n) = \frac{(m + n)(m + n + 1)}{2} + m$$

είναι α.ι. Επίσης υπάρχουν ολικές αλγοριθμικές $K : \mathbb{N} \to \mathbb{N}$, $L : \mathbb{N} \to \mathbb{N}$ έτσι ώστε για κάθε q, $(K(q), L(q)) = J^{-1}(q)$.

Απόδειξη. Γράφουμε τα στοιχεία του $\mathbb{N}^2$ υπό μορφή άπειρου πίνακα ως εξής:

$$\begin{array}{cccc}
(0,0) & (0,1) & (0,2) & (0,3)\cdots \\
(1,0) & (1,1) & (1,2) & (2,3)\cdots \\
(2,0) & (2,1) & (2,2) & (2,3)\cdots \\
(3,0) & (3,1) & (3,2) & (3,3)\cdots \\
\cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots
\end{array}$$

Κατόπιν απαριθμούμε τα στοιχεία του πίνακα κινούμενοι κατά μήκος των διαγωνίων από ΒΑ προς ΝΔ, δηλαδή ως εξής:

$(0,0)$, $(0,1)$, $(1,0)$, $(0,2)$, $(1,1)$, $(2,0), \ldots$. Κάθε διαγώνιος περιέχει ζεύγη με άθροισμα στοιχείων σταθερό. Αν σε μια διαγώνιο υπάρχουν ζεύγη (m,n) με $m+n=k$, τότε η διαγώνιος έχει $k+1$ στοιχεία. Συνεπώς αν το ζεύγος (m,n) κατέχει την q-οστή θέση στην παραπάνω ακολουθία, τότε $q = 1+2+\cdots(m+n)+m = \frac{(m+n)(m+n+1)}{2}+m$. Αυτό δείχνει ότι η απεικόνιση $J(m,n)$ παρέχει ακριβώς τη θέση του ζεύγους (m,n) στην πιο πάνω απαρίθμηση, άρα είναι 1-1 και επί.

Αν $J(m,n)=q$, τότε $(m,n) = J^{-1}(q)$. Τα m,n μπορούν να ανακτηθούν από το q με αλγοριθμικό τρόπο. Αν θέσουμε $m+n=s$, τότε εύκολα βλέπουμε ότι πρέπει $\frac{s(s+1)}{2} \leq q < \frac{(s+1)(s+2)}{2}$. Δοθέντος q, υπάρχει μοναδικό s μ' αυτή την ιδιότητα, το οποίο προφανώς υπολογίζεται αλγοριθμικά. Τότε όμως $m = q - \frac{s(s+1)}{2}$ και $n = s-m$. Άρα αρκεί να θέσουμε $K(q) = q - \frac{s(s+1)}{2}$ και $L(q) = s - K(q)$. QED

Με τη βοήθεια της J μπορούμε να ορίσουμε για κάθε $k \geq 2$ έναν α.ι. $J_k : \mathbb{N}^k \to \mathbb{N}$. Οι J_k ορίζονται επαγωγικά ως εξής:

$J_2 = J$,

$J_{k+1}(x_1, \ldots, x_{k+1}) = J(x_1, J_k(x_2, \ldots, x_{k+1}))$.

Επαγωγικά αποδεικνύεται ότι κάθε J_k είναι α.ι. Τέλος αν $\mathbb{N}^{<\omega} = \bigcup_{k\geq 0} \mathbb{N}^k$ είναι το σύνολο όλων των πεπερασμένων ακολουθιών φυσικών αριθμών, ορίζουμε $J_\omega : \mathbb{N}^{<\omega} \to \mathbb{N}$ ως εξής: Γιά κάθε $n \in \mathbb{N}$ και κάθε $(x_1, \ldots, x_n) \in \mathbb{N}^n$,

$$J_\omega(x_1, \ldots, x_n) = J(n, J_n(x_1, \ldots, x_n)).$$

Εύκολα αποδεικνύεται (δες ασκήσεις) ότι ο J_ω είναι 1-1 και επί.

Όπως και στην περίπτωση του J, αποδεικνύεται ότι για κάθε k υπάρχουν αλγοριθμικές $K_i : \mathbb{N} \to \mathbb{N}$, $1 \leq i \leq k$, τέτοιες ώστε για κάθε $q \in \mathbb{N}$, $(K_1(q), \ldots, K_k(q)) = J_k^{-1}(q)$.

Με τη βοήθεια των J_k, μία συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}^l$ μπορεί να ''μετατραπεί'' σε μία συνάρτηση $g : \mathbb{N} \to \mathbb{N}$, θέτοντας $g = J_l \circ f \circ J_k^{-1}$ με την εξής έννοια: Η f είναι (ολική) αλγοριθμική αν και μόνον αν η g είναι ολική αλγοριθμική.

Ασκήσεις

1.2.1 Δείξτε ότι οι συναρτήσεις J_n, $n \geq 2$ και J_ω είναι 1-1 και επί.

1.2.2 Δείξτε αλγεβρικά ότι η J είναι 1-1.

1.2.3 Βρείτε τα $J^{-1}(147)$ και $J_3^{-1}(223)$.

1.2.4 Δείξτε ότι το $X \subseteq \mathbb{N}^k$ είναι α.α. αν και μόνον αν το $J_k(X)$ είναι α.α.

1.2.5 Έστω $f : \mathbb{N} \to \mathbb{N}$. Γιά κάθε $k \geq 1$, έστω $f^{(k)} : \mathbb{N}^k \to \mathbb{N}$ η συνάρτηση που ορίζεται ως εξής: $f^{(k)}(x_1, \ldots, x_k) = (f(x_1), \ldots, f(x_k))$. Οι $f^{(k)}$ λέγονται συναρτήσεις *επαγόμενες* από την f. Δείξτε ότι αν η f είναι α.ι., το ίδιο είναι και οι επαγόμενες από αυτή.

1.2.6 Έστω G_k η ομάδα των α.ι. του $\mathbb{N}^k$. Αν $G_1^{(k)} = \{f^{(k)} : f \in G_1\}$, δείξτε ότι η $G_1^{(k)}$ είναι υποομάδα της G_k.

1.3 Αλφάβητα, λέξεις, κωδικοποιήσεις

Αυτό που κάνουν οι συναρτήσεις J_n της § 1.2 είναι να ''πακετάρουν'' την πληροφορία που υπάρχει στην n-άδα $(x_1, \ldots, x_n)$ σ' ένα μοναδικό στοιχείο του $\mathbb{N}$ $J_n(x_1, \ldots, x_n)$. Και φυσικά με τρόπο που να μπορεί να ''ξεπακεταριστεί'', δηλαδή να επιστρέψουμε από τον αριθμό στη n-άδα. Τέτοιες αλγοριθμικές και αντιστρέψιμες διαδικασίες αντιπροσώπευσης ενός αντικειμένου πεπερασμένου τύπου από ένα άλλο λέγονται *κωδικοποιήσεις*. Π.χ. κάθε αλγοριθμικός ισομορφισμός $f : X \to Y$ είναι μια κωδικοποίηση των στοιχείων του X με στοιχεία του Y. Το $f(x)$ λέγεται *κώδικας* του x. Η αντίστροφη αντιστοιχία $f(x) \mapsto x$ λέγεται *αποκωδικοποίηση*. Ειδικά οι κωδικοποιήσεις ζευγών φυσικών αριθμών με ένα φυσικό αριθμό, δηλαδή οι ολικές αλγορθμικές 1-1 συναρτήσεις $f : \mathbb{N}^2 \to \mathbb{N}$ (όχι κατ' ανάγκη επί), λέγονται *συναρτήσεις ζεύγους* (pairing functions). Η $J(m,n) = \frac{(m+n)(m+n+1)}{2}$ που είδαμε παραπάνω είναι μία τέτοια, αλλά δεν είναι η μόνη. Άλλες συναρτήσεις ζεύγους είναι οι εξής:

$G_2(m,n) = 2^m \cdot 3^n$,
$h(m,n) = 2^{m+n+2} + 2^{n+1}$,
$e(m,n) = 2^m(2n+1)$.

Η G_2 γενικεύεται στην $G_k : \mathbb{N}^k \to \mathbb{N}$ ως εξής: Αν p_n, είναι ο n-οστός πρώτος αριθμός, θέτουμε

$$G_k(x_1, \ldots, x_k) = p_1^{x_1} \cdots p_k^{x_k} = \Pi_{i=1}^k p_i^{x_i}.$$

(Η αρίθμηση μιας ακολουθίας γίνεται άλλοτε ξεκινώντας από το 1, $x_1, x_2, \ldots$, κι άλλοτε ξεκινώντας από το 0, $x_0, x_1, \ldots$. Έτσι και για τους πρώτους, άλλοτε γράφουμε $p_1, p_2, \ldots$, όπου $p_1 = 2$, κι άλλοτε $p_0, p_1, \ldots$, όπου $p_0 = 2$. Η διαφορά δεν είναι ουσιαστική.) Η G_k είναι κωδικοποίηση (όχι επί) των στοιχείων του $\mathbb{N}^k$. Η G_k είναι καλύτερη από την J_k από την άποψη ότι ο ορισμός της είναι πιο άμεσος και απλός από εκείνον της J_k. (Για να υπολογίσουμε το $J_k(\overline{x})$ πρέπει πρώτα να υπολογίσουμε μια ακολουθία $J_2(\overline{x}_2)$, $J_3(\overline{x}_3), \ldots, J_{k-1}(\overline{x}_{k-1})$.) Παρατηρήστε ότι η συγκεκριμένη κωδικοποίηση αξιοποιεί το θεμελιώδες θεώρημα της Θεωρίας Αριθμών, ότι κάθε ακέραιος έχει μονοσήμαντη ανάλυση σε γινόμενο πρώτων.

Επίσης για την κωδικοποίηση των στοιχείων του $\mathbb{N}^{<\omega}$, είδαμε ήδη τη συνάρτηση J_ω, όμως και πάλι μια παραλλαγή των παραπάνω G_k είναι προτιμότερη. Ορίζουμε την

$G : \mathbb{N}^{<\omega} \to \mathbb{N}$ ως εξής: Γιά κάθε $n \in \mathbb{N}$ και κάθε $x_1, \ldots, x_n$,

$$G(x_1, \ldots, x_n) = \Pi_{i=1}^{n} p_i^{x_i+1}.$$

Η συνάρτηση G οφείλεται στον K. Gödel και συχνά ο $G(x_1, \ldots, x_n)$ αναφέρεται ως *αριθμός Gödel* της n-άδας $(x_1, \ldots, x_n)$.

Ο λόγος για τον οποίο στον πιο πάνω ορισμό βάζουμε $p_i^{x_i+1}$ αντί για $p_i^{x_i}$, είναι για να κάνουμε την G 1-1. Αλλιώς θα είχαμε π.χ. $G(2,5,1) = G(2,5,1,0) = G(2,5,1,0,0) = \cdots$. Το ίδιο πράγμα μπορεί να επιτευχθεί και διαφορετικά. Π.χ. να θέσουμε $G(x_1, \ldots, x_n) = 2^n \Pi_{i=2}^{n+1} p_i^{x_{i-1}}$ (δες [3], σελ. 23).

Συχνά αντί για $G(x_1, \ldots, x_n)$ χρησιμοποιείται ο συμβολισμός

$$\langle x_1, \ldots, x_n \rangle,$$

ο οποίος έχει το πλεονέκτημα να είναι πιο διαφανής και αναγνώσιμος σε επανειλημμένες κωδικοποιήσεις της μορφής π.χ. $\langle x, \langle \langle y_1, \ldots, y_n \rangle, z \rangle \rangle$, το οποίο αλλιώς γράφεται $G(x, G(G(y_1, \ldots, y_n), z))$. Οι αντίστροφες συναρτήσεις της $\langle\rangle$ γράφονται $()_i$, δηλαδή

$$\langle x_1, \ldots, x_n \rangle = y \iff \forall i \leq n \ (y)_i = x_i$$

(δες άσκηση 2.3.3 παρακάτω).

Θα μπορούσαμε να ταυτίσουμε τις κωδικοποιήσεις με τους αλγοριθμικούς ισομορφισμούς αν περιοριζόμασταν σε στοιχεία των συνόλων $\mathbb{N}^k$. Όμως η κωδικοποίηση είναι γενικότερη έννοια και εφαρμόζεται σε μεγαλύτερη ποικιλία συνόλων. Π.χ. το σύστημα Morse που χρησιμοποιούνταν παλιότερα στις επικοινωνίες, κωδικοποιεί τα γράμματα του αλφαβήτου μιας φυσικής γλώσσας, όπως η Αγγλική ή η Ελληνική, με ακολουθίες από τελείες και παύλες. Λόγου χάρη ο κώδικας του S είναι τρείς τελείες, και ο κώδικας του O τρείς παύλες. Π.χ η ακολουθία $\cdots / - - - / \cdots$ σημαίνει SOS.

Γενικότερα η κωδικοποίηση λέξεων και φράσεων μιας γλώσσας (συνήθως μιας μαθηματικής γλώσσας με κώδικες φυσικούς) αποδείχτηκε ότι έχει τεράστια σημασία για τα μαθηματικά. Είδη στην Εισαγωγή αναφέρθηκε ότι κάθε μηκενό, το πολύ αριθμήσιμο σύνολο Σ, μπορεί να θεωρηθεί *αλφάβητο* μιας γλώσσας. Τα στοιχεία του Σ είναι τα *σύμβολα* του αλφαβήτου. Οι *λέξεις* (ή *φράσεις*) είναι ορισμένες πεπερασμένες ακολουθίες συμβόλων που υπακούουν στους *κανόνες σχηματισμού* (formation rules) της γλώσσας. Π.χ. το αλφάβητο της Ελληνικής είναι το $\Sigma = \{\alpha, \beta, \ldots, \omega\} \cup \{$κόμμα, τελεία, διάστημα, ερωτηματικό, κλπ$\}$ καί μία λέξη (φράση) είναι η ακολουθία ''Δεν μπορώ σήμερα, να έρθω αύριο;'' Οι αριθμοί του δεκαδικού συστήματος είναι λέξεις του αλφαβήτου $\Sigma = \{0, 1, \ldots, 9\}$. Οι αριθμοί του δυαδικού συστήματος είναι λέξεις του αλφαβήτου $\Sigma = \{0, 1\}$. Στο πρώτο παράδειγμα, η γλώσσα έχει πολύπλοκους κανόνες σχηματισμού, με αποτέλεσμα πολλές ακολουθίες συμβόλων να μην είναι λέξεις (π.χ. οι ακολουθίες ''κχαφλ'' ή ''σπίτι βασικός θά''). Στο δευτερο και τρίτο παράδειγμα

όμως κάθε πεπερασμένη ακολουθία $a_1a_2\cdots a_n$, όπου $a_i \in \{0,1,\ldots,n\}$ ή $a_i \in \{0,1\}$, είναι αριθμός (λέξη) του δεκαδικού ή δυαδικού συστήματος αντίστοιχα. Σ' αυτές τις περιπτώσεις οι λέξεις ταυτίζονται με τις πεπερασμένες ακολουθίες συμβόλων του Σ και το σύνολό τους το συμβολίζουμε με Σ^*. Το Σ^* είναι η ελεύθερη ημιομάδα με γεννήτορες τα στοιχεία του Σ.

Αν τώρα $\Sigma = \{a_1, a_2, \ldots\}$ είναι μια αρίθμηση του Σ και θεωρήσουμε τον φυσικό αριθμό n κώδικα του a_n, οι λέξεις μετρέπονται σε πεπερασμένες ακολουθίες του $\mathbb{N}$, δηλαδή στοιχεία του $\mathbb{N}^{<\omega}$. Έτσι η κωδικοποίηση των λέξεων του Σ, ανάγεται σε κωδικοποίηση των στοιχείων του $\mathbb{N}^{<\omega}$, η οποία όπως είδαμε πιο πάνω είναι εφικτή μέσω της J_ω ή της συνάρτησης Gödel G. Έτσι για κάθε λέξη $a_{i_1}\cdots a_{i_n}$, μπορούμε να θέσουμε

$$G(a_{i_1}\cdots a_{i_n}) = G(i_1,\cdots,i_n) = \Pi_{k=1}^{n} p_k^{i_k+1}.$$

Η κωδικοποίηση μη αριθμητικών εννοιών, όπως οι λέξεις μιας γλώσσας, με αριθμούς λέγεται συχνά και *αριθμητικοποίηση* ή *αριθμοποίηση* (arithmetization).

Με τόν τον παραπάνω τρόπο όλη η σύνταξη μιας γλώσσας μπορεί να αριθμοποιηθεί, δηλαδή να εκφρασθεί με αριθμούς και σχέσεις μεταξύ αυτών. Αυτές οι *κωδικοποιητικές ικανότητες του* $\mathbb{N}$ κάνουν την αντίστοιχη θεωρία που το εκφράζει, δηλαδή τη Θεωρία της Αριθμητικής του Peano (PA), ή, όπως, είναι ευρύτερα γνωστή, τη Θεωρία Αριθμών, να είναι μια θεωρία-κλειδί: Αν T είναι μια θεωρία στην οποία μπορούμε να ορίσουμε τους φυσικούς αριθμούς και να αποδείξουμε τις βασικές τους ιδιότητες, (δηλαδή αν $\mathrm{PA} \subseteq \mathrm{T}$), τότε (μέσω της κωδικοποίησης της γλώσσας της T με αριθμούς), η T μπορεί να ''μιλήσει'' για να τον εαυτό της και να ''πει'' μια πρόταση την οποία δεν μπορεί να αποδείξει. Αυτό είναι το 1ο Θεώρημα μη πληρότητας του Gödel. Στην απόδειξή του ρόλο-κλειδί παίζει η αριθμητικοποίηση της γλώσσας.

Ασκήσεις

1.3.1 Έστω $n \geq 2$ ένας φυσικός, και έστω $\mathbb{N}_n = \{0,1,\ldots,n-1\}$. Θεωρώντας το $\mathbb{N}_n$ αλφάβητο, κάθε λέξη του $\mathbb{N}_n$ παριστά ένα στοιχείο του $\mathbb{N}$ στο n-αδικό σύστημα. Συγκεκριμένα, αν $x_1,\ldots,x_k \in \mathbb{N}_n$, η λέξη $x_1\cdots x_k$ παριστά τον αριθμό

$$x_1n^{k-1} + x_2n^{k-2} + \cdots + x_{k-1}n + x_k = \Sigma_{i=1}^{k} x_i n^{k-i}.$$

Είναι η απεικόνιση

$$\mathbb{N}_n^* \ni \ x_1\cdots x_k \ \mapsto \Sigma_{i=1}^{k} x_i n^{k-i} \in \mathbb{N} \tag{3}$$

1-1; Είναι επί; Είναι κωδικοποίηση;

1.3.2 Στην προηγούμενη άσκηση πάρτε στη θέση του συνόλου $\mathbb{N}_n = \{0,1,\ldots,n-1\}$, το σύνολο $\mathbb{N}'_n = \{1,\ldots,n\}$ και δείξτε ότι η

$$\mathbb{N}_n'^* \ni \ x_1\cdots x_k \ \mapsto \Sigma_{i=1}^{k} x_i n^{k-i} \in \mathbb{N} - \{0\} \tag{4}$$

είναι τώρα 1-1 και επί.

2 Πρώτη τυποποίηση των αλγοριθμικών συναρτήσεων: Αναδρομικές συναρτήσεις

Δύο είναι οι βασικές τυποποιήσεις (δηλαδή μαθηματικοποιήσεις) της εμπειρικής έννοιας του αλγορίθμου: Η μία μέσω των αναδρομικών συναρτήσεων και η άλλη μέσω των μηχανών Turing. Σ' αυτό το κεφάλαιο θα μιλήσουμε για τις αναδρομικές συναρτήσεις. Με τις μηχανές Turing θα ασχοληθούμε στο επόμενο.

2.1 Περί αναδρομής γενικά

Αναδρομή (recursion), χονδρικά, λέγεται η επαναληπτική εφαρμογή ενός κανόνα, όπου σε κάθε βήμα (εκτός του πρώτου) χρησιμοποιούμε σαν είσοδο (input) την έξοδο (output) του προηγουμένου. Στις ακολουθίες για παράδειγμα, εκτός από εκείνες που ορίζονται με έναν αναλυτικό τύπο (π.χ. $a_n = \frac{n+1}{n}$, $a_n = (1+\frac{1}{n})^n$), έχουμε εκείνες που ορίζονται αναδρομικά, δηλαδή ο n-οστός όρος a_n είναι συνάρτηση του a_{n-1}, ή των a_{n-1} και a_{n-2} κλπ. Π.χ. οι ακολουθίες

$$a_0 = \sqrt{3}, \quad a_{n+1} = \sqrt{3a_n},$$

$$a_0 = 1, \quad a_1 = 2, \quad a_{n+1} = \frac{a_n + a_{n-1}}{2}.$$

Θυμούμενοι ότι η ακολουθία είναι μια συνάρτηση με $f(n) = a_n$, το τελευταίο σχήμα γράφεται

$$f(0) = 1, \quad f(1) = 2, \quad f(n+1) = \frac{f(n) + f(n-1)}{2}.$$

Δηλαδή σε κάθε βήμα εκτός των δύο πρώτων χρησιμοποιούμε τις εξόδους των βημάτων $n-1$ και n ως εισόδους στο βήμα $n+1$. Θεωρούμε δε τη συγκεκριμένη f αλγοριθμική, επειδή το $f(n+1)$ παράγεται από τα $f(n-1)$, $f(n)$ μέσω *πρόσθεσης* και η πρόσθεση είναι προφανώς αλγοριθμική. Όμως μπορούμε να δούμε ότι η και η συνάρτηση $f : \mathbb{N}^2 \to \mathbb{N}$, όπου $f(x, y) = x + y$, είναι επίσης αναδρομική. Ορίζεται με το σχήμα:

$$f(x, 0) = x, \quad f(x, y+1) = f(x, y) + 1.$$

Εδώ, θεωρώντας το x παράμετρο, υπολογίζουμε το $f(x, y+1)$ μέσω του $f(x, y)$ και της συνάρτησης διαδοχής $x \mapsto x + 1$. Είναι η τελευταία αναδρομική; Η $x \mapsto x + 1$ είναι απ' τις πιο απλές αλγοριθμικές συναρτήσεις στο $\mathbb{N}$, δεν ανάγεται σε άλλες απλούστερες, γι' αυτό *δεχόμαστε* εξ ορισμού ότι είναι αναδρομική.

Όμοια οι συναρτήσεις $x \cdot y$ και x^y είναι αναδρομικές αναγόμενες στις $+$ και $\cdot$ αντίστοιχα.

Αναδρομικός ορισμός της $g(x, y) = x \cdot y$: $g(x, 0) = 0$, $g(x, y+1) = g(x, y) + x$. (Αναδρομή με τη βοήθεια της $+$ που είναι ήδη αναδρομική.)

Αναδρομικός ορισμός της $h(x,y) = x^y$: $h(x,0) = 1$, $h(x,y+1) = h(x,y) \cdot x$. (Αναδρομή με τη βοήθεια της $\cdot$ που είναι ήδη αναδρομική.)

Αν θέλαμε να δώσουμε το κύριο γνώρισμα της αναδρομής, θα μπορούσαμε να πούμε ότι είναι η *επανάληψη*, ένα γνώρισμα πολύ κοινό στις μηχανικές διαδικασίες. Θα δούμε παρακάτω ότι κατά μία έννοια η αναδρομή μπορεί να αναχθεί πλήρως στη επανάληψη.

2.2 Βασικές αναδρομικές συναρτήσεις (primitive recursive functions)

Η αναδρομή, χωρίς να εξαντλεί, όπως θα δούμε, την αλγοριθμικότητα, αποτελεί μια πολύ σημαντική συνιστώσα της. Τα παραδείγματα που είδαμε πιο πάνω θα τα συμπεριλάβουμε σε ένα γενικό *Σχήμα Βασικής Αναδρομής*.

Ορισμός 2.2.1 (Σχήμα Βασικής Αναδρομής) Έστω $f : \mathbb{N}^{k+1} \to \mathbb{N}$, όπου γράφουμε $f(\overline{x}, y)$, το διάνυσμα $\overline{x}$ έχει μήκος k, και παίζει το ρόλο παραμέτρων. Έστω επίσης $g : \mathbb{N}^k \to \mathbb{N}$ και $h : \mathbb{N}^{k+2} \to \mathbb{N}$. Θα λέμε ότι η f *παράγεται με βασική αναδρομή από τις* g *και* h αν για κάθε $\overline{x} \in \mathbb{N}^k$ και $y \in \mathbb{N}$,
$f(\overline{x}, 0) = g(\overline{x})$ και
$f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$.

Επίσης η κλάση των αλγοριθμικών συναρτήσεων είναι κλειστή ως προς τη *σύνθεση*. Χονδρικά, άν f, g αλγοριθμικές και η $f \circ g$ ορίζεται, η $f \circ g$ είναι αλγοριθμική. Επειδή η σύνθεση πάντως παίρνει γενικότερες μορφές, θα την ορίσουμε με το παρακάτω *Σχήμα Σύνθεσης*.

Ορισμός 2.2.2 (Σχήμα Σύνθεσης) Έστω $h : \mathbb{N}^m \to \mathbb{N}$ και $g_i : \mathbb{N}^k \to \mathbb{N}$, $i = 1, \ldots, m$. Λέμε ότι η συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$ είναι *σύνθεση* των h και g_i, αν $f(\overline{x}) = h(g_1(\overline{x}), \ldots, g_m(\overline{x}))$. Συμβολικά γράφουμε τότε $f = h \circ (g_1, \ldots, g_m))$.

Κάποιες συναρτήσεις είναι αλγοριθμικές με εξώφθαλμο, τετριμμένο, και γενικά μη αναγώγιμο τρόπο. Αυτές είναι (α) η *συνάρτηση διαδοχής* $S : \mathbb{N} \to \mathbb{N}$ με $S(x) = x + 1$, (β) οι *σταθερές συναρτήσεις* $c_k : \mathbb{N} \to \mathbb{N}$, για κάθε $k \in \mathbb{N}$, όπου $c_k(x) = k$ για κάθε $x \in \mathbb{N}$, και (γ) οι *προβολές*, δηλαδή οι συναρτήσεις $\pi_{nm} : \mathbb{N}^n \to \mathbb{N}$, για $1 \leq m \leq n$, όπου $\pi_{nm}(x_1, \ldots, x_n) = x_m$. Η συνάρτηση S, οι c_k και οι π_{nm} λέγονται *αρχικές συναρτήσεις* (initial functions).

Ορισμός 2.2.3 Το σύνολο $\mathcal{PR}$ των *βασικών αναδρομικών συναρτήσεων* (β.α. για συντομία) είναι το ελάχιστο σύνολο C (δηλαδή η τομή όλων των συνόλων C) με τις ιδιότητες:
(i) Το C περιέχει όλες τις αρχικές συναρτήσεις.

(*ii*) Το C είναι κλειστό ως προς το σχήμα βασικής αναδρομής, δηλαδή αν $g, h \in C$ και η f ορίζεται με βασική αναδρομή από τις g, h, τότε $f \in C$.

(*iii*) Το C είναι κλειστό ως προς τη σύνθεση, δηλαδή αν $h : \mathbb{N}^m \to \mathbb{N}$ και $g_i : \mathbb{N}^k \to \mathbb{N}$, $i = 1, \ldots, m$, ανήκουν στο C, τότε η $f = h \circ (g_1, \ldots, g_m)$ ανήκει στο C.

Παρατήρηση 2.2.4 (1) Ένας ισοδύναμος ορισμός των β.α. συναρτήσεων είναι: Η f είναι β.α. αν υπάρχει μία πεπερασμένη ακολουθία συναρτήσεων $f_1, \ldots, f_n$, τέτοια ώστε: (α) $f_n = f$ και (β) για κάθε $i \leq n$, η f_i είτε είναι αρχική, είτε προέρχεται από δύο προηγούμενες f_k, f_j, $(k, j < i)$ με βασική αναδρομή, είτε πρέρχεται από άλλες προηγούμενες με σύνθεση.

(2) Αντί για όλες τις σταθερές συναρτήσεις θα μπορούσαμε να θεωρήσουμε αρχική μόνο την c_0, $(c_0(x) = 0$ για κάθε $x)$ αφού $c_1(x) = Sc_0(x)$, δηλαδή $c_1 = S \circ c_0$, και γενικά $c_k = S^k \circ c_0$.

Παρατήρηση 2.2.5 (1) Κάθε β.α. συνάρτηση είναι της μορφής $f : \mathbb{N}^k \to \mathbb{N}$, δηλαδή στο $\mathcal{PR}$ όπως ορίστηκε πιο πάνω δεν περιλαμβάνονται συναρτήσεις $f : \mathbb{N}^k \to \mathbb{N}^l$. Ο περιορισμός αυτός δεν είναι ουσιαστικός, και γίνεται για λόγους απλότητας. Κάθε συνάρτηση της μορφής $f : \mathbb{N}^k \to \mathbb{N}^l$, αποτελείται από *συνιστώσες* συναρτήσεις $g_i : \mathbb{N}^k \to \mathbb{N}$, $i \leq l$, δηλαδή $f(\overline{x}) = (g_1(\overline{x}), \ldots, g_l(\overline{x}))$. Αυτό το γράφουμε συμβολικά $f = (g_1, \ldots, g_l)$. Αν θέλουμε λοιπόν να συμπεριλάβουμε τέτοιες συναρτήσεις, μπορούμε να επεκτείνουμε το $\mathcal{PR}$ στο $\mathcal{PR}^*$ το οποίο ορίζεται ως εξής: Η $f : \mathbb{N}^k \to \mathbb{N}^l$ ανήκει στο $\mathcal{PR}^*$, αν $f = (g_1, \ldots, g_l)$ και $g_i \in \mathcal{PR}$, για $i \leq l$.

(2) Κάθε β.α. συνάρτηση είναι *ολική*. Αυτό εύκολα προκύπτει από τον προηγούμενο ορισμό και το γεγονός ότι όλες οι αρχικές συναρτήσεις είναι ολικές.

Το $\mathcal{PR}$ αποτελεί μια πρώτη προσέγγιση της κλάσης των αλγοριθμικών συναρτήσεων. Στα παρακάτω παραδείγματα δείχνουμε πως μια πληθώρα συναρτήσεων που χρησιμοποιούμε στην πράξη ανήκουν σ' αυτό.

Παραδειγματα

(1) Κάθε σταθερή συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$ είναι β.α.

Έστω $f(\overline{x}) = a$ για κάθε $\overline{x} \in \mathbb{N}^k$. Τότε $f(\overline{x}) = c_a(\pi_{k1}(\overline{x})) = a$, άρα $f = c_a \pi_{k1}$, και αφού $c_a, \pi_{k1} \in \mathcal{PR}$, $f \in \mathcal{PR}$.

(2) Η ταυτοτική συνάρτηση είναι β.α.

Η $f(x) = x = \pi_{11}(x)$. Άρα $f = \pi_{11}$.

(3) Η πρόσθεση είναι β.α.

Έστω $f(x, y) = x + y$. Όπως είδαμε ήδη η f ορίζεται ως εξής: $f(x, 0) = x$ και $f(x, y + 1) = f(x, y) + 1$. Αυτές γράφονται και ως εξής:

$f(x, 0) = \pi_{11}(x)$,

$f(x, y+1) = S\pi_{33}(x, y, f(x, y))$.
Τώρα βλέπουμε ότι η f παράγεται με βασική αναδρομή από τις $g = \pi_{11}$ και $h = S\pi_{33}$. Η h είναι σύνθεση β.α., άρα β.α., και η g είναι β.α., άρα η $+$ είναι β.α.

(4) Ο πολλ/σμός είναι β.α.
Έστω $f(x, y) = x \cdot y$. Τότε
$f(x, 0) = 0 = c_0(x)$,
$f(x, y+1) = f(x, y) + x = \pi_{33}(x, y, f(x, y)) + \pi_{31}(x, y, f(x, y)) = (\pi_{33} + \pi_{31})(x, y, f(x, y))$.
Εδώ έχουμε $g = c_0$ και $h = \pi_{33} + \pi_{31}$. Η τελευταία είναι σύνθεση των π_{33}, π_{31} και $+$, που ειναι β.α.

(5) Η x^y είναι β.α.
Έστω $f(x, y) = x^y$. Τότε
$f(x, 0) = 1 = c_1(x)$,
$f(x, y+1) = f(x, y) \cdot x = \pi_{33}(x, y, f(x, y)) \cdot \pi_{31}(x, y, f(x, y)) = (\pi_{33} \cdot \pi_{31})(x, y, f(x, y))$.
Άρα $g = c_1$ και $h = \pi_{33} \cdot \pi_{31}$.

(6) Η $f(x) = x!$ είναι β.α.
Η f ορίζεται ως εξής:
$f(0) = 1$,
$f(y+1) = f(y) \cdot (y+1)$.
Το σχήμα αυτό προκύπτει από το σχήμα βασικής αναδρομής χωρίς παραμέτρους, άρα χρειαζόμαστε μία h έτσι ώστε $h(y, f(y)) = f(y+1) = f(y) \cdot (y+1)$. Όμως το $f(y) \cdot (y+1)$ γράφεται $f(y) \cdot (y+1) = \pi_{22}(y, f(y)) \cdot S\pi_{21}(y, f(y))$, δηλαδή $h = \pi_{22} \cdot S\pi_{21}$.

(7) Η συνάρτηση του προηγουμένου (predecessor), $pd(x)$, είναι β.α.
Αυτή ορίζεται ως εξής:
$pd(0) = 0$,
$pd(x+1) = x$.
Άρα $pd(x+1) = \pi_{21}(x, pd(x))$.

(8) Η συνάρτηση διαφοράς, $x \dot{-} y$, είναι β.α.
Η $\dot{-}$ ορίζεται ως εξής: $x \dot{-} y = x - y$ αν $x \geq y$, και $x \dot{-} y = 0$ αν $x < y$. Ή, αναδρομικά:
$x \dot{-} 0 = x$,
$x \dot{-} (y+1) = pd(x \dot{-} y)$.

(9) Οι συναρτήσεις προσήμου $sign(x)$ και συμπροσήμου $cosign(x)$ είναι β.α.
Οι $sign(x)$ και $cosign(x)$ ορίζονται ως εξής:

$sign(0) = 0$, $sign(x+1) = 1$,
$cosign(0) = 1$, $cosign(x+1) = 0$,
και προφανώς είναι β.α.

(10) Έστω $f : \mathbb{N}^{k+1} \to \mathbb{N}$ β.α. Τότε και οι συναρτήσεις άθροισης και γινομένου $g, h : \mathbb{N}^{k+1} \to \mathbb{N}$, όπου $g(\overline{x}, y) = \Sigma_{z \le y} f(\overline{x}, z)$ και $h(\overline{x}, y) = \Pi_{z \le y} f(\overline{x}, z)$,είναι β.α. Η g ορίζεται ανδρομικά ως εξής:
$g(\overline{x}, 0) = f(\overline{x}, 0)$,
$g(\overline{x}, y+1) = g(\overline{x}, y) + f(\overline{x}, y+1)$.
Εύκολα βλέπουμε ότι παράγεται με βασική αναδρομή και σύνθεση από την f, την $+$ και αρχικές συναρτήσεις. Το ίδιο και η h. Άρα είναι β.α. Γενικότερα, οι συναρτήσεις $g(\overline{x}, y) = \Sigma_{z \le h(\overline{x}, y)} f(\overline{x}, z)$ και $g(\overline{x}, y) = \Pi_{z \le h(\overline{x}, y)} f(\overline{x}, z)$, όπου h β.α., είναι β.α. (λόγω σύνθεσης)

(11) Αν η f ορίζεται με περιπτώσεις (by cases) από άλλες β.α., είναι β.α.
Έστω f_i, g_i, $1 \le i \le m$, β.α., έτσι ώστε για κάθε $\overline{x}$ υπάρχει ακριβώς ένα i τέτοιο ώστε $g_i(\overline{x}) = 0$, και έστω ότι η f ορίζεται ως εξής:

$$f(\overline{x}) = \begin{cases} f_1(\overline{x}) & \text{αν} \quad g_1(\overline{x}) = 0 \\ f_2(\overline{x}) & \text{αν} \quad g_2(\overline{x}) = 0 \\ \cdots\cdots & \cdots \quad \cdots\cdots\cdots \\ f_m(\overline{x}) & \text{αν} \quad g_m(\overline{x}) = 0. \end{cases}$$

Χρησιμοποιώντας τις συναρτήσεις $cosign(x)$ που ορίσαμε πιο πάνω, είναι εύκολο να δούμε ότι η f γράφεται:

$$f(\overline{x}) = cosign(g_1(\overline{x})) \cdot f_1(\overline{x}) + \cdots + cosign(g_m(\overline{x})) \cdot f_m(\overline{x}).$$

Το δεξιό μέλος της τελευταίας είναι σύνθεση β.α., άρα η f είναι β.α.

(12) Οι συναρτήσεις πηλίκου και υπολοίπου είναι β.α.
Έστω $quo(x, y)$ και $rem(x, y)$ παριστούν το πηλίκο και το υπόλοιπο αντίστοιχα της διαίρεσης του y με το x. Για $x \neq 0$ έχουμε:
$quo(x, 0) = 0$,

$$quo(x, y+1) = \begin{cases} quo(x,y) + 1 & \text{αν} \quad y+1 = (quo(x,y)+1) \cdot x, \\ quo(x,y) & \text{αν} \quad y+1 \neq (quo(x,y)+1) \cdot x. \end{cases}$$

Άρα η quo παράγεται με βασική αναδρομή από την c_0 και την $h(x, y, z)$, όπου $h(x, y, z) = z+1$ αν $y+1 = (z+1)x$ και $h(x, y, z) = z$ αλλιώς. Ο ορισμός αυτός είναι μία παραλλαγή του ορισμού με περιπτώσεις, άρα h β.α. Κατά συνέπεια και η quo είναι β.α.

Τέλος η $rem(x, y)$ γράφεται: $rem(x, y) = y \dot{-} x \cdot quo(x, y)$, συνεπώς είναι β.α.

(13) Οι συναρτήσεις J_k, $k \ge 2$ είναι β.α.

Η J παράγεται από τις $+, \cdot$ και quo και αρχικές με σύνθεση. Για τις J_k, $k > 2$, με επαγωγή στο k.

(14) Η φραγμένη ελαχιστοποίηση είναι β.α.

Έστω $h : \mathbb{N}^{k+1} \to \{0, 1\}$ β.α. τέτοια ώστε

$$(\forall \overline{x} \in \mathbb{N}^k)(\forall y \in \mathbb{N})(\exists z \leq y)(h(\overline{x}, z) = 0).$$

Τότε η συνάρτηση $f : \mathbb{N}^{k+1} \to \mathbb{N}$

$$f(\overline{x}, y) = (\mu z \leq y)(h(\overline{x}, z) = 0)$$

είναι β.α. [ο συμβολισμός $(\mu z \leq y)A(\cdots)$ σημαίνει: "Το ελάχιστο z μικρότερο του y τέτοιο ώστε $A(\cdots)$".]

Παρατηρούμε ότι αν k είναι το ελάχιστο $z \leq y$ τέτοιο ώστε $h(\overline{x}, z) = 0$, τότε

$$h(\overline{x}, 0) = 1,\ h(\overline{x}, 1) = 1, \ldots, h(\overline{x}, k-1) = 1,\ h(\overline{x}, k) = 0.$$

Αν για κάθε $i \leq y$ φτιάξουμε το γινόμενο $\Pi_{z \leq i} h(\overline{x}, z)$, τότε $\Pi_{z \leq i} h(\overline{x}, z) = 1$ για $i < k$, ενώ $\Pi_{z \leq i} h(\overline{x}, z) = 0$ για $i \geq k$. Επί πλέον το άθροισμα όλων αυτών των γινομένων είναι k αν και μόνον αν $f(\overline{x}, y) = k$, δηλαδή

$$f(\overline{x}, y) = k \iff \Sigma_{i \leq y} \Pi_{z \leq i} h(\overline{x}, z) = k.$$

Συνεπώς $f(\overline{x}, y) = \Sigma_{i \leq y} \Pi_{z \leq i} h(\overline{x}, z)$, και από το παράδειγμα (10) έπεται ότι η f είναι β.α.

Γενικότερα αν $g : \mathbb{N}^k \to \mathbb{N}$ είναι β.α., τότε η

$$f(\overline{x}) = (\mu y \leq g(\overline{x}))(h(\overline{x}, y) = 0)$$

είναι β.α. (λόγω σύνθεσης).

(15) Η επανάληψη (iteration) μιας β.α. είναι β.α.

Εδώ θα δουλέψουμε στο $\mathcal{PR}^*$ αντί για το $\mathcal{PR}$, επειδή το πεδίο τιμών της f πρέπει να είναι υποσύνολο του πεδίου ορισμού. Έστω $f : X \to X$, όπου X κάποιο από τα σύνολα $\mathbb{N}^k$. Η *επανάληψη* της f είναι η συνάρτηση $f^I : X \times \mathbb{N} \to X$, που ορίζεται ως εξής:

$$f^I(x, 0) = x, \quad f^I(x, n+1) = f(f^I(x, n)).$$

Αμέσως βλέπουμε ότι η f^I προκύπτει με βασική αναδρομή από την f και αρχικές συναρτήσεις, άρα αν η f είναι β.α., το ίδιο είναι κα η f^I. Συχνά γράφουμε $f^n(x)$ αντί για $f^I(x, n)$.

(16) Η $|x - y|$ είναι β.α.

Παρατηρήστε ότι $|x-y| = (x \dot{-} y) + (y \dot{-} x)$.

(17) Η $\min(x,y)$ είναι β.α.

Αυτή γράφεται: $\min(x,y) = x \cdot cosign(x \dot{-} y) + y \cdot sign(x \dot{-} y)$.

2.3 Βασικά αναδρομικά σύνολα

Ορισμός 2.3.1 Ένα σύνολο $X \subseteq \mathbb{N}^k$ λέγεται *βασικό αναδρομικό ή β.α. για συντομία, αν η χαρακτηριστική του συνάρτηση C_X είναι β.α.*

Τα σύνολα που μας ενδιαφέρουν εδώ δεν είναι τυχαία υποσύνολα του $\mathbb{N}^k$, αλλά αντιστοιχούν σε κάποια *ιδιότητα ή σχέση* $\phi(\overline{x})$ η οποία τα ορίζει, δηλαδή είναι της μορφής $X = \{\overline{x} : \phi(\overline{x})\}$. Στην παράγραφο αυτή δεν θα ορίσουμε αυστηρά τις ιδιότητες ϕ. Αυτό θα γίνει στήν § 5 ενότητα. Διαισθητικά οι ιδιότητες είναι της μορφής π.χ. ''x μικρότερο του y'', ''x διαιρεί τον y'', ''x πρώτος '' κλπ. Συχνά αντί για ''β.α. σύνολο '' λέμε ''β.α. ιδιότητα ή σχέση''. Π.χ. έχουμε:

Πρόταση 2.3.2 *Η ισότητα και η ανισότητα στο $\mathbb{N}$ είναι β.α. σχέσεις. Το ίδιο και η σχέση διαιρετότητας.*

Απόδειξη. Έστω $C_=$ και $C_<$ οι χαρακτ. συναρτήσεις των συνόλων $\{(x,y) : x = y\}$ και $\{(x,y) : x < y\}$ αντίστοιχα. Αρκεί να δείξουμε ότι είναι β.α. Όμως είναι εύκολο να δούμε ότι $C_=(x,y) = cosign|x-y|$ και $C_<(x,y) = sign(y \dot{-} x) = sign|y - min(x,y)|$. Δεδομένου ότι οι $sign$, min κλπ είναι β.α., το ίδιο είναι και οι $C_=$ και $C_<$. Όμοια η χαρακτ. συνάρτηση του συνόλου $\{(x,y) : x|y\}$ γράφεται: $C_|(x,y) = cosign(rem(x,y))$, όπου rem η συνάρτηση υπολοίπου. QED

Πρόταση 2.3.3 *Αν τα X, Y είναι β.α., το ίδιο συμβαίνει με τα σύνολα $-X$, $X \cup Y$, $X \cap Y$, $X \times Y$. Επίσης αν $X \subseteq \mathbb{N}^{k+1}$, για $k \geq 1$, είναι β.α., και $Y = \{(\overline{x}, z) : (\forall y \leq z)(\overline{x}, y) \in X\}$, $Z = \{(\overline{x}, z) : (\exists y \leq z)(\overline{x}, y) \in X\}$, τα Y, Z είναι β.α. (Αυτό το εκφράζουμε λέγοντας ότι τα β.α. σύνολα είναι κλειστά ως προς φραγμένους ποσοδείκτες.)*

Απόδειξη. Παρατηρήστε ότι:
$C_{-X}(x) = cosign(C_X(x))$,
$C_{X\cup Y}(x) = sign(C_X(x) + C_Y(x))$,
$C_{X\cap Y}(x) = C_X(x) \cdot C_Y(x)$,
$C_{X\times Y}(x,y) = C_X(x) \cdot C_Y(y)$.
Βλέπουμε ότι οι C_{-X}, $C_{X\cup Y}$, $C_{X\cap Y}$, $C_{X\times Y}$ είναι συνθέσεις β.α. και άρα είναι β.α. Έστω $Y = \{(\overline{x}, z) : (\forall y \leq z)(\overline{x}, y) \in X\}$. Τότε για κάθε $(\overline{x}, z) \in \mathbb{N}^{k+1}$,

$$C_Y(\overline{x}, z) = 1 \iff (\forall y \leq z)(C_X(\overline{x}, y) = 1) \iff \Pi_{y\leq z} C_X(\overline{x}, y) = 1.$$

Αυτό σημαίνει ότι η $\Pi_{y\leq z}C_X(\overline{x},y)$ είναι η χαρακτ. συνάρτηση του Y. Αυτή όμως είναι β.α., αφού η C_X είναι β.α., όπως είδαμε στο παράδειγμα (10) της § 2.2. Για το $Z=\{(\overline{x},z):(\exists y\leq z)(\overline{x},y)\in X\}$ παρατηρήστε ότι το συμπληρωμά του $-Z$ είναι όπως το προηγούμενο Y. Άρα είναι β.α. και όπως είδαμε προηγουμένως, και το Z είναι β.α. QED

Πρόταση 2.3.4 *(α) Το σύνολο $Prime=\{n:n$ πρώτος$\}$ είναι β.α.*

(β) Για κάθε $n\in\mathbb{N}$, έστω p_n ο $n+1$-οστός πρώτος , δηλαδή $p_0=2$, $p_1=3$, $p_2=5$ κλπ. Η συνάρτηση $p:\mathbb{N}\to\mathbb{N}$, όπου $p(n)=p_n$ είναι β.α.

Απόδειξη. (α) Αρκεί να δείξουμε ότι το συμπλήρωμα του $Prime$ είναι β.α. Όμως ο $n\notin Prime$ αν και μόνον αν υπάρχει $1<x<n$ τέτοιος ώστε $x|n$. Αυτό γράφεται ως εξής:

$$n\notin Prime \iff (\exists x\leq n)(\exists y\leq n)((x+2)(y+2)=n).$$

Αφού η ιδιότητα $(x+2)(y+2)=n$ είναι β.α., λόγω της πρότασης 2.3.2, και η $(\exists x\leq n)(\exists y\leq n)((x+2)(y+2)=n)$ είναι β.α., το σύνολο $-Prime$ είναι β.α.

(β) Η $p(n)$ ορίζεται αναδρομικά ως εξής:

$p(0)=2$,

$p(n+1)=(\mu x)(x>p(n)$ και $x\in Prime)$.

Αλλά τότε, $p(n+1)=h(p(n))$, όπου h η συνάρτηση

$$h(x)=(\mu y)(y>x \text{ και } y\in Prime) \tag{5}$$

είναι β.α. Τώρα αφού οι ιδιότητες $y>x$ και $y\in Prime$ είναι β.α. όπως είδαμε στις Προτάσεις 2.3.2 και 2.3.3, αρκεί να δείξουμε ότι στην (5) ο τελεστής μ είναι ουσιαστικά φραγμένος (δηλαδή έχουμε φραγμένη αναζήτηση), οπότε από το παράδειγμα 14 της §2.2 προκύπτει ότι η h είναι β.α. Αρκεί συνεπώς να βρούμε β.α. g τέτοια ώστε

$$h(x)=(\mu y\leq g(x))(y>x \text{ και } y\in Prime). \tag{6}$$

Μια τέτοια συνάρτηση που φράσσει την αναζήτηση είναι π.χ. η $g(x)=x!+1$, η οποία, από το παράδειγμα 6 της §2.2 είναι β.α. (η ιδέα προέρχεται από την απόδειξη του θεωρήματος του Ευκλείδη). Ότι η (5) συνεπάγεται την (6) αποδεικνύεται ως εξής: Έστω q ένας πρώτος διαιρέτης του $g(x)=x!+1$. Αν $q\leq x$, τότε $q|x!$, άρα $q|(x!+1-x!)=1$, άτοπο. Άρα $q>x$. Εξ άλλου προφανώς $q\leq g(x)$. Συνεπώς για κάθε x υπάρχει πρώτος q, τέτοιος ώστε $x<q\leq g(x)$. Αυτό δείχνει ότι η h που ορίζεται από την (5) ικανοποιεί την (6). QED

Ασκήσεις

2.3.1 Η συνάρτηση πηλίκου $quo(x,y)$ μπορεί να ορισθεί και ως εξής: $quo(x,y) =$ ο μέγιστος z τέτοιος ώστε $x \cdot z \leq y$. Γράψτε με σχέσεις αυτόν τον ορισμό και δώστε μια άλλη απόδειξη ότι η *quo* είναι β.α.

2.3.2 Έστω $sqrt(x) =$ ο μέγιστος y τέτοιος ώστε $y^2 \leq x$. Δείξτε ότι είναι β.α.

2.3.3 Έστω $x > 0$. Για κάθε $i \geq 0$, έστω $(x)_i = y \dot{-} 1$, όπου y ο εκθέτης του p_i στην ανάλυση του x σε γινόμενο πρώτων παραγόντων. (Για $x = 0$ μπορούμε να θέσουμε $(x)_i = 0$.) Δείξτε ότι η σχέση $(x)_y = z$ είναι β.α. Δείξτε ότι για κάθε πεπερασμένη ακολουθία $x_0, \ldots, x_n$ υπάρχει y τέτοιο ώστε $(y)_i = x_i$ για κάθε $i = 0, \ldots, n$. Δείξτε ότι ο y είναι ο αριθμός Gödel της ακολουθίας $(y)_0, \ldots, (y)_k$, όπου p_k είναι ο μέγιστος πρώτος που διαιρεί τον y (δηλαδή $y = \Pi_{i \leq n} p_i^{x_i+1}$).

2.3.4 Δείξτε ότι οι αντίστροφες συναρτήσεις K, L της συνάρτησης ζεύγους $J : \mathbb{N}^2 \to \mathbb{N}$ είναι β.α.

Πλήρης, διπλή και πολλαπλή αναδρομή. Το Σχήμα Βασικής Αναδρομής που χρησιμοποιήθηκε στον ορισμό των β.α. συναρτήσεων εξαρτά την τιμή της f στο $y+1$, μόνο από την τιμή της στο y ($f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$). Όμως σε πολλές περιπτώσεις το $f(\overline{x}, y+1)$, εξαρτάται από περισσότερες τιμές ή και από όλες τις προηγούμενες τιμές $f(\overline{x}, z)$, $z \leq y$. Τέτοια αναδρομή λέγεται *πλήρης*. Π.χ. πολύ συχνά έχουμε αναδρομή της μορφής:

$f(\overline{x}, 0) = g_0(\overline{x})$,
$f(\overline{x}, 1) = g_1(\overline{x})$,
$f(\overline{x}, y+2) = h(\overline{x}, y, f(\overline{x}, y), f(\overline{x}, y+1))$.

Επίσης μπορεί να έχουμε διπλή ή πολλαπλή αναδρομή όπως στο εξής παράδειγμα:

Έστω $g_0, g_1 : \mathbb{N} \to \mathbb{N}$ και $h : \mathbb{N}^4 \to \mathbb{N}$ και έστω $f : \mathbb{N}^2 \to \mathbb{N}$ η συνάρτηση που ορίζεται με διπλή αναδρομή ως εξής:

$f(m, 0) = g_0(m)$,
$f(0, n) = g_1(n)$,
$f(m+1, n+1) = h(m, n, f(m+1, n), f(m, n+1))$.

Τί γίνεται με τις συναρτήσεις αυτές; Είναι β.α. όταν οι συναρτήσεις που τις παράγουν είναι β.α.; Η απάντηση είναι ''ναι''. Δηλαδή το σχήμα βασικής αναδρομής καλύπτει και την πλήρη και την πολλαπλή αναδρομή, μόνο που η απόδειξη είναι αρκετά περίπλοκη. Και το βασικό εργαλείο για να το αποδείξει κανείς είναι η κωδικοποίηση. Αν $f(\overline{x}, y)$ είναι μια συνάρτηση, μπορούμε να δημιουργήσουμε μία άλλη που να μας πληροφορεί για όλη την *ιστορία* της τιμής $f(\overline{x}, y)$, δηλαδή για όλη την ακολουθία $f(\overline{x}, 0)$, $f(\overline{x}, 1), \ldots, f(\overline{x}, y)$. Δοθείσης της $f : \mathbb{N}^{k+1} \to \mathbb{N}$, ορίζουμε την $f^* : \mathbb{N}^{k+1} \to \mathbb{N}$ ως εξής: $f^*(\overline{x}, y) = \Pi_{i \leq y} p_i^{f(\overline{x}, i)+1}$. Μ' άλλα λόγια (δες άσκηση 2.3.3), για κάθε $\overline{x}$, y και $i \leq y$,

$$(f^*(\overline{x}, y))_i = f(\overline{x}, i).$$

Δηλαδή ο αριθμός $f^*(\overline{x}, y)$ είναι κώδικας της ''ιστορίας '' $f(\overline{x}, 0)$, $f(\overline{x}, 1), \ldots, f(\overline{x}, y)$. Δεδομένου ότι, όπως είδαμε παραπάνω, η εκθετική συνάρτηση ειναι β.α., η συναρτηση $p(n)$ απαρίθμησης των πρώτων είναι β.α. και το γινόμενο $\Pi_{i \leq y}$ οδηγεί από β.α. σε β.α., η f^* είναι β.α. όταν η f είναι β.α.

Έστω f, g, h συναρτήσεις σαν αυτές που αναφέρονται στο Σχήμα Βασικής Αναδρομής (ορισμός 2.2.1). Θα λέμε ότι η f παράγεται από τις g και h με *πλήρη αναδρομή* αν

$f(\overline{x}, 0) = g(\overline{x})$ και

$f(\overline{x}, y+1) = h(\overline{x}, y, f^*(\overline{x}, y))$.

Μ' άλλα λόγια, για τον ορισμό του $f(\overline{x}, y+1)$ μπορεί να αξιοποιηθεί όλη η ιστορία του βήματος $f(\overline{x}, y)$, κι όχι μόνο το βήμα αυτό. Η παρακάτω πρόταση λέει ότι το σχήμα πλήρους αναδρομής δεν είναι ισχυρότερο από το σχήμα βασικής αναδρομής.

Πρόταση 2.3.5 *Έστω ότι g, h είναι β.α. Αν η f παράγεται από τις g, h με πλήρη αναδρομή, τότε η f είναι β.α.*

Απόδειξη. Έστω ότι η f παράγεται με πλήρη αναδρομή από τις g και h, δηλαδή

$f(\overline{x}, 0) = g(\overline{x})$,

$f(\overline{x}, y+1) = h(\overline{x}, y, f^*(\overline{x}, y))$,

όπου f η ιστορία της f. Για να δείξουμε ότι η f είναι β.α. αρκεί να δείξουμε ότι η f^* είναι β.α., διότι τότε ή f παράγεται από τις g, h, f^* με σύνθεση. Τώρα για την f^* έχουμε:

$f^*(\overline{x}, 0) = 2^{f(\overline{x},0)+1} = 2^{g(\overline{x})+1}$,

$f^*(\overline{x}, y+1) = f^*(\overline{x}, y) \cdot p_{y+1}^{f(\overline{x},y+1)+1} = f^*(\overline{x}, y) \cdot p_{y+1}^{h(\overline{x},y,f^*(\overline{x},y))+1}$.

Δηλαδή η f^* ορίζεται με την αναδρομή:

$f^*(\overline{x}, 0) = 2^{g(\overline{x})+1}$,

$f^*(\overline{x}, y+1) = f^*(\overline{x}, y) \cdot p_{y+1}^{h(\overline{x},y,f^*(\overline{x},y))+1}$.

Εδώ η συνάρτηση H της αναδρομής είναι η

$H(\overline{x}, y, z) = z \cdot p_{y+1}^{h(\overline{x},y,z)+1}$. QED

Ασκήσεις

2.3.5 Δείξτε με τη βοήθεια της Πρότασης 2.3.5 ότι τα παραδείγματα διπλής και σχεδόν πλήρους αναδρομής που αναφέρθηκαν πιο πάνω ορίζουν β.α. συναρτήσεις.

Θα κλείσουμε αυτή την παράγραφο με μία πρόταση που δείχνει αυτό που είπαμε στο τέλος της παραγράφου 2.1, ότι όχι μόνο το κύριο γνώρισμα της αναδρομής είναι η επανάληψη, αλλά ότι η αναδρομή μπορεί να *αναχθεί* σε επανάληψη.

Πρόταση 2.3.6 *Έστω C_0 η ελάχιστη κλάση συναρτήσεων C με τις ιδιότητες:*

(a) Η C περιέχει τις αρχικές συναρτήσεις.

(β) Η C είναι κλειστή ως προς την επανάληψη, δηλαδή αν $f \in C$, τότε $f^I \in C$ (δες παράδειγμα 15 της § 2.2).

(γ) Η C είναι κλειστή ως προς τη σύνθεση.

(δ) Η C είναι κλειστή ως προς τα γινόμενα, δηλαδή αν $f = (g_1, \ldots, g_l)$ και $g_i \in C$, τότε $f \in C$.

Τότε $C_0 = \mathcal{PR}^*$.

Απόδειξη. Από το παράδειγμα 15 της § 2.2 έπεται ότι $C_0 \subseteq \mathcal{PR}^*$. Για το αντίστροφο, αρκεί να δείξουμε ότι αν $g, h \in C_0$, και η f παράγεται από τις g, h με βασική αναδρομή, τότε $f \in C_0$. Έστω $g, h \in C_0$ και έστω

$f(\overline{x}, 0) = g(\overline{x})$, και

$f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$.

Θεωρούμε τη συνάρτηση $\rho : \mathbb{N}^{k+2} \to \mathbb{N}^{k+2}$ που ορίζεται ως εξής:

$$\rho(\overline{x}, y, z) = (\overline{x}, y+1, h(\overline{x}, y, z)).$$

Έστω ρ^I η επανάληψη της ρ, δηλαδή

$$\rho^I(\overline{x}, y, z, 0) = (\overline{x}, y, z), \quad \rho^I(\overline{x}, y, z, m+1) = \rho(\rho^I(\overline{x}, y, z, m)).$$

Ισχυρίζομαι ότι για κάθε $\overline{x}, y$,

$$\rho^I(\overline{x}, 0, g(\overline{x}), y) = (\overline{x}, y, f(\overline{x}, y)) \tag{7}$$

οπότε $f(\overline{x}, y) = \pi_{33}\rho^I(\overline{x}, 0, g(\overline{x}), y))$. Τώρα, $\rho^I \in C_0$ αφού $h \in C_0$, και $\rho \in C_0$. Συνεπώς $f \in C_0$.

Απόδειξη της (7): Με επαγωγή στο y. Εξ ορισμού

$$\rho^I(\overline{x}, 0, g(\overline{x}), 0) = (\overline{x}, 0, g(\overline{x})) = (\overline{x}, 0, f(\overline{x}, 0)),$$

άρα ισχύει για $y = 0$.

Έστω ισχύει για y, δηλαδή η (7) αληθεύει. Τότε

$$\rho^I(\overline{x}, 0, g(\overline{x}), y+1) = \rho(\rho^I(\overline{x}, 0, g(\overline{x}), y)) = \rho(\overline{x}, y, f(\overline{x}, y)) \text{ (από την υπόθεση της επαγωγής)}$$

$$= (\overline{x}, y+1, h(\overline{x}, y, f(\overline{x}, y)) \text{ (από τον ορισμό της } \rho)$$

$$= (\overline{x}, y+1, f(\overline{x}, y+1)).$$

QED

2.4 Πέρα από τις β.α. συναρτήσεις. Η συνάρτηση Ackermann

Η κλάση $\mathcal{PR}$ των β.α. συναρτήσεων, μολονότι πολύ ευρεία, δεν περιλαμβάνει όλες τις συναρτήσεις που έχουν έναν προφανή αλγόριθμο. Κατ'αρχήν δεν περιλαμβάνει την τετριμμένη συνάρτηση Ω, που είναι μερική, ενώ όλες οι β.α. είναι ολικές (δες Παρατήρηση 2.2.5 (2)). Βέβαια θα μπορούσε κανείς να περιλάβει την Ω στις αρχικές, οπότε χρειαζόμαστε ένα πιο πειστικό παράδειγμα. Ένα κλασσικό παράδειγμα συνάρτησης με προφανή αλγόριθμο που δεν είναι β.α. αποτελεί η συνάρτηση Ackermann που θα ορίσουμε αμέσως.

Ας ξεκινήσουμε από τις συναρτήσεις $x+y$, $x\cdot y$, x^y, που η μία διαδέχεται την άλλη με έναν κανονικό τρόπο:

$$x\cdot y = \underbrace{x+\cdots+x}_{y\ \text{φορές}}, \qquad x^y = \underbrace{x\cdot\cdots\cdot x}_{y\ \text{φορές}}.$$

Αν συμβολίσουμε με f_0, f_1, f_2 αντίστοιχα τις συναρτήσεις αυτές, τότε από τους αναδρομικούς τους ορισμούς έχουμε

$$\begin{cases} f_1(x,0)=0, & f_1(x,y+1)=f_0(x,f_1(x,y)) \\ f_2(x,0)=1, & f_2(x,y+1)=f_1(x,f_2(x,y)). \end{cases} \tag{8}$$

Οι σχέσεις (8) υποβάλλουν την ιδέα να συνεχίσουμε την ακολουθία των f_0, f_1, f_2, θέτοντας

$$f_3(x,0)=1,\ f_3(x,y+1)=f_2(x,f_3(x,y)).$$

Με επαγωγή στο y εύκολα βλέπουμε ότι

$$f_3(x,y+1)=x^{f_3(x,y)}=x^{x^{\cdot^{\cdot^{x}}}}\quad (y+1\ \text{φορές}).$$

Γενικότερα μπορούμε να θέσουμε για κάθε $n>1$,

$$f_{n+1}(x,0)=1,\ f_{n+1}(x,y+1)=f_n(x,f_{n+1}(x,y)).$$

Η ακολουθία $(f_n)_n$ είναι τώρα μια αλγοριθμική ακολουθία β.α. συναρτήσεων, και αν θέσουμε

$$A_1(x,y,z)=f_x(y,z),$$

η A_1 είναι προφανώς αλγοριθμική. Για σταθερό $y>1$, η A ορίζεται από το αναδρομικό σχήμα:

$$\begin{cases} A_1(0,y,z) & = y+z \\ A_1(x+1,y,0) & = 0 \ \text{ αν } x=0,1 \ \text{ αν } x>0 \\ A_1(x+1,y,z+1) & = A_1(x,y,A_1(x+1,y,z)). \end{cases} \tag{9}$$

Η παραπάνω συνάρτηση A_1 είναι η *συνάρτηση Ackermann*(ή ακριβέστερα μια μορφή της). Επειδή γενικεύει την εκθετική συνάρτηση, λέγεται και *γενικευμένη εκθετική* συνάρτηση.

Στον ορισμό (9) το y εμφανίζεται ως παράμετρος, οπότε μπορούμε να θέσουμε $y = 1$, $z = y$ και να θεωρήσουμε την απλούστερη συνάρτηση δύο μεταβλητών $A_2(x, y) = A_1(x, 1, y)$. Η A_2 λόγω της (9), γράφεται:

$$\begin{cases} A_2(0, y) & = y + 1 \\ A_2(x + 1, 0) & = 0 \ \text{ αν } x = 0, 1 \ \text{ αν } x > 0 \\ A_2(x + 1, y + 1) & = A_2(x, A_2(x + 1, y)). \end{cases} \tag{10}$$

Στην πραγματικότητα, αυτό που μας ενδιαφέρει σχετικά με τις παραπάνω συναρτήσεις, δεν είναι τόσο οι συγκεκριμένες τιμές που παίρνουν για τα διάφορα x, y, αλλά η *ταχύτητα* με την οποία αυξάνονται. Έτσι οι A_1, A_2, μολονότι διαφορετικές, αυξάνονται με την ίδια ταχύτητα. Γι' αυτό και τελικά η συνάρτηση Ackermann ορίζεται συνήθως απλούστερα ως εξής:

$$\begin{cases} A(0, y) & = y + 1 \\ A(x + 1, 0) & = A(x, 1) \\ A(x + 1, y + 1) & = A(x, A(x + 1, y)). \end{cases} \tag{11}$$

Με πρώτη ματιά ο παραπάνω ορισμός της A (όπως και οι προηγούμενοι των A_1, A_2) φαίνεται να είναι μια διπλή βασική αναδρομή, π.χ. σαν αυτή του παραδείγματος της §2.3, όπου $f(m + 1, n + 1) = h(m, n, f(m + 1, n), f(m, n + 1))$, η οποία όπως είδαμε ανάγεται σε βασική αναδρομή και άρα οδηγεί σε β.α. συνάρτηση. Η διαφορά είναι ότι στο παράδειγμα, και σ' όλα τα αντίστοιχα παραδείγματα πολλαπλής αναδρομής, η αναδρομή γίνεται μέσω μιας τρίτης συνάρτησης h, ανεξάρτητης από την f, ενώ στον ορισμό (11) η αναδρομή γίνεται μέσω της ίδιας της A. Αυτό είναι ένα είδος *διαγωνιοποίησης* που μας βγάζει όπως θα δούμε από την κλάση των β.α.

Ασκήσεις

2.4.1 Δείξτε τις εξής ιδιότητες της A.
(α) $A(1, n) = n + 2$.
(β) $A(2, n) = 2n + 3$.
(γ) $A(3, n) = 2^{n+3} - 3$.
(δ) $A(4, n) = 2^{2^{\cdot^{\cdot^{2}}}} - 3$ ($n + 3$ εκθέτες).

2.4.2 Δείξτε τις εξής ιδιότητες της A.
(α) $A(x, y) > y$. [Δείξτε πρώτα τις περιπτώσεις $A(0, y) > y$, $A(x, 0) > 0$, και κατόπιν δείξτε την ζητούμενη με επαγωγή στο x.]

(β) $A(x, y+1) > A(x, y)$. [Με επαγωγή στο x και χρήση του (α).]
(γ) $y_1 < y_2 \Rightarrow A(x, y_1) < A(x, y_2)$. [Με χρήση του (β).]
(δ) $A(x+1, y) \geq A(x, y+1)$. [Με επαγωγή στο y.]
(ε) $A(x, y) > x$. [Με χρήση του (δ), απ' όπου προκύπτει ότι $A(x+z, y) \geq A(x, y+z)$ και $x = 0$.]
(ζ) $x_1 < x_2 \Rightarrow A(x_1, y) < A(x_2, y)$. [Αρκεί να δειχτεί ότι $A(x+1, y) > A(x, y)$. Με χρήση των (δ) και (β).]
(η) $A(x+2, y) > A(x, 2y)$. [Με επαγωγή στο y.]

Στή συνάρτηση Ackermann $A(x, y)$, ο x καθορίζει το ''ύψος '' των εκθετών, άρα και την τάξη μεγέθους του $A(x, y)$. Π.χ. έχουμε δει στην άσκηση 2.4.1 ότι $A(2, n) = 2n+3$, $A(3, n) = 2^{n+3}$ και $A(4, n) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} - 3$. Δηλαδή ενώ η $A(2, n)$ είναι πολυωνμική πρώτου βαθμού, η $A(3, n)$ είναι εκθετική και η $A(4, n)$ είναι υπερεκθετική.

Ορισμός 2.4.1 Έστω $f : \mathbb{N} \to \mathbb{N}$. Λέμε ότι η f είναι *το πολύ τάξης* r αν για κάθε $x \in \mathbb{N}$, $f(x) \leq A(r, x)$, όπου A η συνάρτηση Ackermann. Γενικότερα, αν $f : \mathbb{N}^k \to \mathbb{N}$, λέμε ότι η f το πολύ τάξης r αν $f(\overline{x}) \leq A(r, \max(\overline{x}))$.

Δηλαδή η f είναι το πολύ τάξης r, αν η ταχύτητα αύξησής της είναι το πολύ όση και της $A(r, x)$. Η παρακάτω πρόταση δείχνει το γιατί η συνάρτηση Ackermann ξεφεύγει από την κλάση των β.α.

Πρόταση 2.4.2 *Για κάθε β.α. συνάρτηση f, υπάρχει $r \in \mathbb{N}$ τέτοιο ώστε η f είναι το πολύ τάξης r.*

Απόδειξη. Θα δώσουμε μόνο ένα σκαρίφημα της απόδειξης, χωρίς όλες τις τεχνικές λεπτομέρειες. Με επαγωγή στον τρόπο κατασκευής των β.α. συναρτήσεων (ορισμός (2.2.3). Προφανώς οι αρχικές συναρτήσεις είναι το πολύ τάξης 1. Έστω ότι η f παράγεται με σύνθεση από τις h, $g_1, \ldots, g_m$, δηλαδή

$$f(\overline{x}) = h(g_1(\overline{x}), \ldots, g_m(\overline{x})),$$

και έστω η h είναι το πολύ τάξης r και η g_i το πολύ τάξης s_i, $i \leq m$. Ας θέσουμε για συντομία $g_i(\overline{x}) = y_i$, καθώς επίσης και $\max(\overline{x}) = a$, $\max(\overline{y}) = b$. Τότε

$$f(\overline{x}) = h(g_1(\overline{x}), \ldots, g_m(\overline{x})) = h(y_1, \ldots, y_m) = h(\overline{y}).$$

Από την υπόθεση,

$$h(\overline{y}) \leq A(r, b) \quad \text{καί} \quad g_i(\overline{x}) = y_i \leq A(s_i, a).$$

Έστω

$$s = \max\{r, s_1, \ldots, s_m\} + 3.$$

Αρκεί να δείξουμε ότι η f είναι το πολύ τάξης s, δηλαδή ότι για κάθε $\overline{x}$,

$$f(\overline{x}) \leq A(s, \max(\overline{x})) = A(s, a).$$

Κάνουμε χρήση των ιδιοτήτων (α)-(η) της άσκησης 2.4.2. Από την (δ) έχουμε

$$A(s, a) \geq A(s-1, a+1) = A(s-2, A(s-1, a)).$$

Επίσης $s - 1 > s_i$, άρα από την (ζ)

$$A(s-1, a) > A(s_i, a) \geq g_i(\overline{x}) = y_i.$$

Από τις δύο τελευταίες και την (γ) έπεται ότι $A(s, a) > A(s-2, y_i)$ για κάθε i, άρα, από τη (ζ) και την $s - 2 > r$,

$$A(s, a) > A(s-2, b) > A(r, b) \geq h(\overline{y}) = f(\overline{x}),$$

δηλαδή το ζητούμενο.

Παρόμοια δουλεύουμε με το σχήμα βασικής αναδρομής. Εκεί η απόδειξη είναι πιο περίπλοκη και την παραλείπουμε (οι ενδιαφερόμενοι μπορούν να δούν την απόδειξη στην Πρόταση 3.14 του [3]). QED

Πόρισμα 2.4.3 *Η συνάρτηση Ackermann δεν είναι β.α.*

Απόδειξη. Έστω ότι είναι. Τότε και η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, όπου $f(x) = A(x, x) + 1$ είναι β.α. Από την προηγούμενη Πρόταση, η f είναι το πολύ τάξης r για κάποιο r, δηλαδή $f(x) \leq A(r, x)$ για κάθε x. Συνεπώς $f(r) \leq A(r, r)$, ενώ από τον ορισμό της f $f(r) = A(r, r) + 1$. Αντίφαση. QED

Αποδεικνύεται ότι το γράφημα $G(A)$ της συνάρτησης A, δηλαδή το σύνολο $\{(x, y, z) : A(x, y) = z\}$, είναι β.α. σύνολο και ότι

$$A(x, y) = (\mu z)((x, y, z) \in G(A)).$$

Μ' άλλα λόγια η A παράγεται από μια β.α. συνάρτηση με ελαχιστοποίηση. Άρα στην παραπάνω σχέση ο τελεστής *μz δεν μπορεί να φραχτεί* από καμμιά β.α. συνάρτηση.

2.5 Αναδρομικές συναρτήσεις

Στο παράδειγμα 8 της § 1.1 είδαμε την f να ορίζεται από την g ως εξής:

$$f(\overline{x}) = \begin{cases} (\mu y)(g(\overline{x}, y) = 1) & \text{αν} \quad (\exists y)(g(\overline{x}, y) = 1), \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Λέμε τότε ότι η f *παράγεται από την* g *με ελαχιστοποίηση*. Παρατηρήστε ότι η έκφραση $z = (\mu y)(g(\overline{x}, y) = 1)$ είναι μια *συντομογραφία*, και ότι αυτό αναλυτικά γράφεται

$$g(\overline{x}, z) = 1 \text{ και } (\forall u < z)(g(\overline{x}, z) \neq 1).$$

Ορισμός 2.5.1 Το σύνολο $\mathcal{R}$ των *(μερικών) αναδρομικών συναρτήσεων* είναι το ελάχιστο σύνολο C (δηλαδή η τομή όλων των συνόλων C) με τις ιδιότητες:

(i) Το C περιέχει όλες τις αρχικές συναρτήσεις.

(ii) Το C είναι κλειστό ως προς το σχήμα βασικής αναδρομής, δηλαδή αν $g, h \in C$ και η f ορίζεται με βασική αναδρομή από τις g, h, τότε $f \in C$.

(iii) Το C είναι κλειστό ως προς τη σύνθεση, δηλαδή αν $h : \mathbb{N}^m \to \mathbb{N}$ και $g_i : \mathbb{N}^k \to \mathbb{N}$, $i = 1, \ldots, m$, ανήκουν στο C, τότε η $f : \mathbb{N}^k \to \mathbb{N}$, όπου $f(\overline{x}) = h(g_1(\overline{x}), \ldots, g_m(\overline{x}))$, ανήκει στο C.

(iv) Το C είναι κλειστό ως προς την ελαχιστοποίηση, δηλαδή αν $g \in C$ και η f παράγεται από την g με ελαχιστοποίηση, τότε $f \in C$.

Η ελαχιστοποίηση είναι ένα πολύ ισχυρό σχήμα το οποίο μας βγάζει από την κλάση των β.α. Για παράδειγμα αποδεικνύεται ότι

Πρόταση 2.5.2 *Η συνάρτηση Ackermann ανήκει στο* $\mathcal{R}$.

Για την απόδειξη δες [3], Πρόταση 3.13. Συγκεκριμένα αποδεικνύεται ότι η συνάρτηση A παράγεται από β.α. συναρτήσεις με σύνθεση και ελαχιστοποίηση.

Με το σχήμα ελαχιστοποίησης παίρνουμε γενικά *μερικές* συναρτήσεις καθώς το σχήμα δεν εγγυάται ολικότητα. Έτσι λέγοντας ''αναδρομική'' θα εννοούμε εν γένει *μερική* αναδρομική. Οι ολικές αναδρομικές θα είναι μέρος μόνον των αναδρομικών.

Φυσικά και για την κλάση $\mathcal{R}$ θα μπορούσε να τεθεί το ερώτημα αν υπάρχουν αλγοριθμικές συναρτήσεις που δεν ανήκουν σ' αυτή. Όμως υπάρχουν πειστικές ενδείξεις ότι η $\mathcal{R}$ είναι η μέγιστη κλάση, και ότι κάθε συνάρτηση που περιγράφεται με κάποιον εμπειρικό αλγόριθμο ανήκει σ' αυτήν. Αυτή η παραδοχή είναι γνωστή ως Θέση του Church (ή Θέση των Church-Turing-Markov).

Θέση του Church. *Μια συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$ είναι αλγοριθμική (με την εμπειρική έννοια του όρου) αν και μόνον αν είναι αναδρομική.*

Δεν τίθεται θέμα απόδειξης της Θέσης, καθώς δεν είναι μια μαθηματική πρόταση, αλλά μάλλον ένα φιλοσοφικό δόγμα αναφορικά με την έννοια της αλγοριθμικότητας. Μας

λέει: Μην ψάχνετε για κάτι πέρα από αυτό που παράγει η σύνθεση, η αναδρομή και η ελαχιστοποίηση. Βέβαια μπορούν να υπάρξουν διαφορετικές περιγραφές της αλγοριθμικότητας (π.χ. μέσω μηχανών Turing) αλλά αυτές οι περιγραφές τελικά αποδεικνύονται ισοδύναμες με την περιγραφή μέσω αναδρομικών συναρτήσεων, κι αυτό είναι που κάνει την Θέση του Church αρκετά πειστική.

Στην πράξη η Θέση είναι μια βολική γέφυρα ανάμεσα στην διαίσθηση και την αυστηρότητα. Όταν συναντήσουμε μια συνάρτηση με έναν προφανή αλλά όχι αυστηρά διατυπωμένο αλγόριθμο, μπορούμε να την κατατάξουμε στις αναδρομικές, χωρίς να ανατρέχουμε στην λεπτομερή τεχνική απόδειξη του πως παράγεται από τα σχήματα του ορισμού της αναδρομής.

2.6 Αναδρομικά και αναδρομικά απαριθμήσιμα σύνολα

Ορισμός 2.6.1 Ένα σύνολο $X \subseteq N^k$ λέγεται *αναδρομικό* αν η χαρακτ. του συνάρτηση C_X είναι αναδρομική. Το X θα λέγεται *αναδρομικά απαριθμήσιμο* ή α.α. για συντομία (recursively enumerable ή r.e), αν $X = \emptyset$ ή $X = rng(f)$, όπου f ολική αναδρομική[2].

Θα αποδείξουμε τώρα ορισμένες προτάσεις που είναι ''μεταφράσεις '' των αντίστοιχων για τα αλγοριθμικά, και αλγοριθμικά απαριθμήσιμα σύνολα (§ 1.1). Στην § 1.1 οι αλγόριθμοι ήταν εμπειρικά αντικείμενα, ενώ τώρα είναι μαθηματικά αντικείμενα. Εξ αιτίας αυτού, οι αποδείξεις δεν είναι τετριμμένες αναδιατυπώσεις των μεν στις δε.

Πρόταση 2.6.2 *(α) Κάθε αναδρομικό σύνολο είναι α.α.*
(β) Το X είναι αναδρομικό αν και μόνον αν τα X και $-X$ είναι α.α.

Απόδειξη. (α) Έστω X αναδρομικό. Τότε η C_X είναι αναδρομική. Θέλουμε να δείξουμε ότι $X = rng(f)$ για κάποια ολική αναδρομική f. Αν $X = \emptyset$, το X είναι α.α. εξ ορισμού. Έστω $X \neq \emptyset$ και έστω $a \in X$. Ορίζουμε την $f : \mathbb{N} \to \mathbb{N}$ ως εξής:

$$f(n) = n \cdot C_X(n) + cosign(C_X(n)) \cdot a.$$

Προφανώς f ολική αναδρομική και είναι εύκολο να δούμε ότι $rng(f) = X$.

(β) Προφανώς X αναδρομικό συνεπάγεται $-X$ αναδρομικό, άρα η μία κατεύθυνση προκύπτει από το (α). Αντίστροφα, έστω $X = rng(f)$ και $-X = rng(g)$, όπου f, g ολικές αναδρομικές. Θεωρούμε τη συνάρτηση h, με $h(2n) = f(n)$ και $h(2n+1) = g(n)$. Προφανώς h ολική αναδρομική και $rng(h) = \mathbb{N}$. Έστω η συνάρτηση:

[2] Η συντομογραφία ''α.α.'' χρησιμοποιήθηκε ήδη πιο πριν για τα ''αλγοριθμικά απαριθμήσιμα σύνολα'', κι εδώ τον χρησιμοποιούμε ξανά για να σημάνει ''αναδρομικά απαριθμήσιμα''. Όμως δεν υπάρχει κίνδυνος πραγματικής σύγχυσης, διότι λόγω της Θέσης του Church αυτές οι δύο έννοιες αποδεικνύονται ισοδύναμες.

$$e(x) = \begin{cases} 1 & \text{αν} \quad (\mu n)(h(n) = x) = \text{άρτιος}, \\ 0 & \text{αν} \quad (\mu n)(h(n) = x) = \text{περιττός}. \end{cases}$$

Είναι εύκολο να διαπιστώσουμε ότι η e είναι αναδρομική (διότι ορίζεται με περιπτώσεις, δες παραδείγματα της § 2.2). Επίσης η e είναι ολική και είναι η χαρακτ. συνάρτηση του X. QED

Πρόταση 2.6.3 *Έστω f ολική. Η f είναι αναδρομική αν και μόνον αν το σύνολο $G(f)$ είναι αναδρομικό.*

Απόδειξη. Αν f αναδρομική, τότε η συνάρτηση

$$g(m,n) = \begin{cases} 1 & \text{αν} \quad f(m) = n \\ 0 & \text{αν} \quad f(m) \neq n, \end{cases}$$

είναι ολική αναδρομική και $g = C_{G(f)}$. Αντίστροφα. Έστω η $C_{G(f)}$ είναι αναδρομική. Τότε η f γράφεται

$$f(m) = (\mu n)(C_{G(f)}(m,n) = 1).$$

Συνεπώς f αναδρομική. QED

Πρόταση 2.6.4 *Έστω $X \subseteq \mathbb{N}$. Το X είναι α.α αν και μόνον αν υπάρχει αναδρομικό $Y \subseteq \mathbb{N}^2$, τέτοιο ώστε για κάθε $x \in \mathbb{N}$,*

$$x \in X \iff \exists n \ (n,x) \in Y.$$

Απόδειξη. Έστω $X \subseteq \mathbb{N}$ α.α. Από τον ορισμό, $X = rng(f)$ για μια ολική αναδρομική f. Άρα

$$x \in X \iff \exists n \ f(n) = x \iff \exists n \ (n,x) \in G(f).$$

Από την προηγούμενη πρόταση το $G(f)$ είναι αναδρομικό, συνεπώς η ιδιότητα ισχύει. Αντίστροφα, έστω το X έχει την παραπάνω ιδιότητα. Το Y είναι αναδρομικό, άρα α.α. και έστω $g : \mathbb{N} \to \mathbb{N}^2$ ολική αναδρομική τέτοια ώστε $Y = rng(g)$. Ορίζουμε $f : \mathbb{N} \to \mathbb{N}$ ως εξής: $f(n) =$ το δεύτερο μέλος του ζεύγους $g(n)$. Αυτό αυστηρά γράφεται $f(n) = \pi_{22}(g(n))$. Προφανώς η f είναι ολική αλγοριθμική και $rng(f) = \pi_{22}(rng(g)) = X$. Άρα το X είναι α.α. QED

Πρόταση 2.6.5 *(α) Το X είναι α.α. αν καί μόνον αν υπάρχει 1-1 ολική αναδρομική f τέτοια ώστε $X = rng(f)$.*

(β) Έστω X άπειρο. Το X είναι αναδρομικό αν καί μόνον αν υπάρχει αυστηρά αύξουσα ολική αναδρομική f τέτοια ώστε $X = rng(f)$.

Απόδειξη. (α) Η απόδειξη είναι ίδια με την απόδειξη της ισοδυναμίας (α) $\Leftrightarrow$ (δ) στην Πρόταση 1.1.11.

(β) Η κατεύθυνση $\Rightarrow$ είναι ίδια με την απόδειξη της 1.1.12. Για την άλλη κατεύθυνση, έστω $X = rng(f)$, f αυστηρά αύξουσα αλγοριθμική. Όπως και στην 1.1.14, έχουμε ότι

$$m \in X \iff (\exists n \leq m)(f(n) = m).$$

Από την Πρόταση 2.3.3 (κλειστότητα ως προς φραγμένους ποσοδείκτες), το X ορίζεται από μια αναδρομική σχέση, άρα είναι αναδρομικό. QED

Ασκήσεις

2.6.1 Έστω $X \subseteq \mathbb{N}$ τέτοιο ώστε

$$x \in X \iff (\exists n_1) \cdots (\exists n_k)((n_1, \ldots, n_k, x) \in Y),$$

όπου Y αναδρομικό υποσύνολο του $\mathbb{N}^{k+1}$. Δείξτε ότι το X είναι α.α.

Αυτό που δεν μπορούμε προς το παρόν να κάνουμε είναι να μεταφράσουμε προτάσεις που αποδεικνύονται με τη βοήθεια των αλγορίθμων αναμονής, T_A, όπως είναι π.χ. οι υπόλοιποι χαρακτηρισμοί των α.α. συνόλων που περιέχονται στην Πρόταση 1.1.11 (ότι το X είναι α.α. αν και μόνον αν είναι το πεδίο τιμών ή ορισμού μιας αναδρομικής συνάρτησης κλπ). Και τούτο διότι ο T_A ορίζεται με τη βοήθεια του ''χρόνου αναμονής '', ή του *υπολογιστικού βήματος* το οποίο δεν έχουμε πει τι σημαίνει για τις αναδρομικές συναρτήσεις, κι ούτε είναι τόσο εύκολο να το ορίσει κανείς (σε αντίθεση με τις μηχανές Turing όπου αυτό είναι πολύ εύκολο).

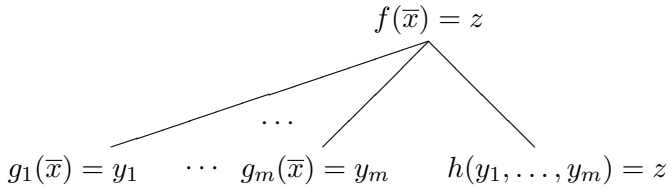
2.7 Αριθμητικοποίηση και κανονική μορφή Kleene (Kleene's normal form) για αναδρομικές συναρτήσεις

Όπως προκύπτει από τον ορισμό 2.5.1 και την παρατήρηση 2.2.5, για κάθε αναδρομική συνάρτηση f υπάρχει μία πεπερασμένη ακολουθία συναρτήσεων $f_1, \ldots, f_n$, τέτοια ώστε: (α) $f_n = f$ και (β) για κάθε $i \leq n$, η f_i είτε είναι αρχική, είτε παράγεται από δύο προηγούμενες f_k, f_j, $(k, j < i)$ με βασική αναδρομή, είτε παράγεται από προηγούμενες με σύνθεση, είτε παράγεται από μία προηγούμενη με ελαχιστοποίηση. Η ακολουθία $f_1, \ldots, f_n$ περιέχει προφανώς τα *βήματα κατασκευής* της f ξεκινώντας από αρχικές συναρτήσεις. Αν τώρα θέλουμε να υπολογίσουμε την τιμή $f(\overline{x})$, ένας κανονικός τρόπος να το κάνουμε είναι να ακολουθήσουμε τα βήματα αυτά, ανάγοντας τον υπολογισμό του $f(\overline{x})$ σε προηγούμενους υπολογισμούς. Τα βήματα αυτά δεν βρίσκονται πάνω σε μία ευθεία, αλλά καλύτερα μπορούμε να τα φαντασθούμε σαν κόμβους ενός (ανεστραμμένου) δέντρου, του *δέντρου υπολογισμού της* f *στο* $\overline{x}$, $T(f, \overline{x})$. Κάθε κόμβος

αντιστοιχεί σε έναν υπολογισμό, και οι προπάτορες (predecessors) ενός κόμβου περιέχουν τους αμέσως προηγούμενους υπολογισμούς. Συγκεκριμένα, το $T(f, \overline{x})$ ορίζεται με τα παρακάτω βήματα 1)- 5):

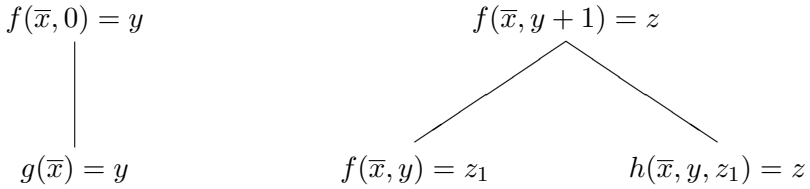
1) Η ρίζα του δέντρου είναι ο τελικός υπολογισμός $f(\overline{x}) = y$.

2) Αν η f παράγεται με σύνθεση από από τις h, $g_1, \ldots, g_m$ και $f(\overline{x}) = h(g_1(\overline{x}), \ldots, g_m(\overline{x}))$, τότε για να υπολογίσουμε το $f(\overline{x})$ πρέπει να έχουμε υπολογίσει πρώτα τα $y_1 = g_1(\overline{x}), \ldots, y_m = g_m(\overline{x})$ και $z = h(y_1, \ldots, y_m)$, για να θέσουμε τελικά $f(\overline{x}) = z$. Έτσι ο κόμβος του $f(\overline{x})$ έχει τους $m + 1$ προπάτορες που δείχνει το σχήμα 1.



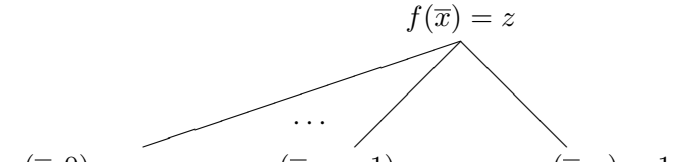
Σχήμα 1

3) Αν η f παράγεται με βασική αναδρομή από τις g και h, δηλαδή $f(\overline{x}, 0) = g(\overline{x})$ και $f(\overline{x}, y + 1) = h(\overline{x}, y, f(\overline{x}, y))$, οι προπάτορες του $f(\overline{x}, y)$ φαίνονται στο σχήμα 2.



Σχήμα 2

4) Αν η f παράγεται από την g με ελαχιστοποίηση, δηλαδή $f(\overline{x}) = (\mu y)(g(\overline{x}, y) = 1)$, οι προπάτορες του $f(\overline{x}, y)$ είναι αυτοί του σχήματος 3.



όπου $a_0 \neq 1, \ldots, a_{z-1} \neq 1$.

Σχήμα 3

5) Τέλος τα ''φύλλα'' του δέντρου, δηλαδή οι κόμβοι χωρίς προπάτορες, είναι οι αρχικές συναρτήσεις $c_0(x) = 0$, $S(x) = x + 1$, $\pi_{ni}(x_1, \ldots, x_n) = x_i$.

Είναι τώρα φανερό ότι σε κάθε συνάρτηση f, σε κάθε αλγόριθμο που την ορίζει, και σε κάθε είσοδο $\overline{x}$, αντιστοιχεί (μονοσήμαντα) ένα *δέντρο υπολογισμού* (computation tree). Φυσικά ο υπολογισμός του $f(\overline{x})$ γίνεται από τα φύλλα προς τη ρίζα. Η μόνη περίπτωση να μην τερματίσει ο υπολογισμός και να έχουμε δέντρο με άπειρους κόμβους και χωρίς ρίζα, είναι όταν σε κάποιο σημείο του υπολογισμού εφαρμόσουμε το σχήμα ελαχιστοποίησης (σχήμα 3) και η ιδιότητα $g(\overline{x}, y) = 1$ δεν είναι κανονική, δηλαδή $(\exists \overline{x})(\forall y)(g(\overline{x}, y) \neq 1)$.

Ώστε λοιπόν, αυτό που στην παράγραφο 1.1 ονομάζαμε εμπειρικά ''βήμα υπολογισμού'', ή ''μονάδα χρόνου αναμονής '', εδώ γίνεται σαφές ως ''κόμβος στο δέντρο υπολογισμού'' και το να ''περιμένουμε k μονάδες χρόνου'' εδώ μεταφράζεται στο να ''περάσουμε από k κόμβους του δέντρου''.

Χρησιμοποιώντας την παραπάνω ιδέα ο S. Kleene (1936) μπόρεσε να δώσει μια κανονική περιγραφή των αναδρομικών συναρτήσεων. Συγεκριμένα έδειξε το ακόλουθο:

Θεώρημα 2.7.1 (Θεώρημα Κανονικής Μορφής του Kleene) *Υπάρχουν μια β.α. συνάρτηση $U : \mathbb{N} \to \mathbb{N}$ και, για κάθε $n \geq 1$, ένα β.α. σύνολο/ιδιότητα $T_n(e, x_1, \ldots, x_n, y) \subseteq \mathbb{N}^{n+2}$ τέτοια ώστε: Γιά κάθε αναδρομική συνάρτηση $f : \mathbb{N}^n \to \mathbb{N}$, υπάρχει αριθμός e (ο δείκτης της f) έτσι ώστε να ισχύουν τα ακόλουθα:*

(α) $(x_1, \ldots, x_n) \in dom(f) \iff \exists y\, T_n(e, x_1, \ldots, x_n, y)$,

(β) $f(x_1, \ldots, x_n) = U(\mu y\, T_n(e, x_1, \ldots, x_n, y))$.

Η ιδιότητα $T_n(e, x_1, \ldots, x_n, y)$ σημαίνει το εξής: Ο y είναι κώδικας ενός (δέντρου) υπολογισμού της τιμής που δίνει η συνάρτηση με κώδικα e όταν τροφοδοτηθεί με εισόδους τα $x_1, \ldots, x_n$. Αν f είναι η συνάρτηση με κώδικα e, παίρνοντας τον ελάχιστο κώδικα $y_0 = \mu y T_n\ (e, x_1, \ldots, x_n, y)$, το $U(y_0)$ είναι η τιμή της f στο $(x_1, \ldots, x_n)$.

Στο υπόλοιπο αυτής της παραγράφου θα προσπαθήσουμε να δώσουμε ένα σκαρίφημα της απόδειξης. Κατ' αρχήν χρειάζεται να κωδικοποιήσουμε τις αναδρομικές συναρτήσεις με αριθμούς. Θυμηθείτε την κωδικοποίηση της n-άδας $(x_1, \ldots, x_n)$ με τον αριθμό $y = \langle x_1, \ldots, x_n \rangle = \Pi_{i \leq n} p_i^{x_i + 1}$, με αντίστροφες συναρτήσεις $(y)_i = x_i$.

Αριθμητικοποίηση των αναδρομικών συναρτήσεων. Αντιστοιχούμε σε κάθε αναδρομική συνάρτηση f, που ορίζεται με έναν συγκεκριμένο αλγόριθμο, έναν αριθμητικό κώδικα $\lceil f \rceil$ (που εξαρτάται από τον συγκεκριμένο αλγόριθμο) ως εξής:

(1) Για τη σταθερή συνάρτηση c_0, $\lceil c_0 \rceil = 0$.

(2) Για τη συνάρτηση διαδοχής S, $\lceil S \rceil = 1$.

(3) Για την προβολή π_{ni}, $i \leq n$, $\lceil \pi_{ni} \rceil = \langle 2, n, i \rangle$.

(4) Αν $f = h \circ (g_1, \ldots, g_m)$, $\lceil f \rceil = \langle 3, \lceil h \rceil, \lceil g_1 \rceil, \ldots, \lceil g_m \rceil \rangle$.

(5) Αν η f παράγεται με βασική αναδρομή από τις g και h, $\lceil f \rceil = \langle 4, \lceil h \rceil, \lceil g \rceil \rangle$.

(6) Αν η f παράγεται με ελαχιστοποίηση από την g, $\lceil f \rceil = \langle 5, \lceil g \rceil \rangle$.

Με τα παραπάνω βήματα προφανώς κάθε αναδρομική συνάρτηση f αποκτά έναν αριθμητικό κώδικα $\lceil f \rceil$. Ο $\lceil f \rceil$ λέγεται *δείκτης* (index) της f.

Παρατήρηση 2.7.2 1) Είναι σημαντικό να παρατηρήσουμε ότι ο δείκτης e μιας συνάρτησης *δεν είναι μοναδικός*, και ότι ο συμβολισμός $\lceil f \rceil \rangle$ είναι μάλλον καταχρηστικός. Μια συνάρτηση μπορεί να οριστεί με πολλούς διαφορετικούς τρόπους (αλγορίθμους), άρα αυτό που κωδικοποιεί ένας δείκτης e είναι ένας (από τους πολλούς) συγκεκριμένος αλγόριθμος που ορίζει την f. Πιο πρακτικά μπορούμε να θεωρούμε εναν δείκτη της f σαν ένα *πρόγραμμα* που υπολογίζει την f.

2) Προφανώς δεν είναι κάθε $x \in \mathbb{N}$ δείκτης μιας αναδρομικής συνάρτησης. Όμως το σύνολο των δεικτών, δηλαδή το σύνολο

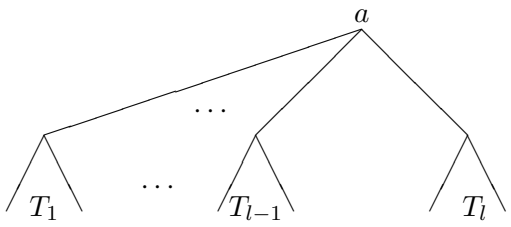
$$Ind = \{x : \exists \text{ αναδρομική } f \text{ τέτοια ώστε } \lceil f \rceil = x\}$$

είναι αναδρομικό. Από την άλλη μεριά θα δούμε ότι το σύνολο των δεικτών των ολικών αναδρομικών συναρτήσεων δεν είναι αλγοριθμικό.

3) Ας θυμηθούμε ότι υπάρχει και η τετριμμένη συνάρτηση Ω, με $dom(\Omega) = \emptyset$. Η Ω δεν είναι β.α., άρα μόνο από το σχήμα ελαχιστοποίησης μπορεί να προέλθει. Π.χ. ένας ορισμός της είναι: $\Omega(x) = (\mu y)(s(x) + s(y) = 1)$. Άρα οι δείκτες της Ω είναι της μορφής $\langle 5, x \rangle$.

Αριθμητικοποίηση των κόμβων του δέντρου υπολογισμού. Κάθε κόμβος a σ' ένα δέντρο υπολογισμού αντιστοιχεί σε μια ισότητα της μορφής $f(x_1, \ldots, x_n) = y$, δηλαδή μια συνάρτηση, μια είσοδο και μια εξοδο. Άρα μπορεί να κωδικοποιηθεί με τον αριθμό $\lceil a \rceil = \langle \lceil f \rceil, \langle x_1, \ldots, x_n \rangle, y \rangle$.

Αριθμητικοποίηση των δέντρων υπολογισμού. Κάθε δέντρο T αποτελείται από έναν κόμβο-ρίζα a και πεπερασμένο αριθμό υποδέντρων $T_1, \ldots, T_l$ με ρίζες τους προπάτορες του a (σχήμα 4).



Σχήμα 4

Άρα με επαγωγή μπορούμε να ορίσουμε τον κώδικα $\lceil T \rceil$ του T ως εξής: $\lceil T \rceil = \langle \lceil a \rceil, \lceil T_1 \rceil, \ldots, \lceil T_l \rceil \rangle$.

Έστω $C(y)$ η ιδιότητα ''το y είναι κώδικας ενός δέντρου υπολογισμού''. Πρόκειται για αναδρομική ιδιότητα; Η απάντηση είναι ότι πρόκειται για *βασική αναδρομική* ιδιότητα. Βέβαια η λεπτομερής απόδειξη αυτού του ισχυρισμού είναι αρκετά μακρά και κοπιώδης, αλλά όχι δύσκολη με την έννοια της επινόησης κάποιου δύσκολου συλλογισμού. Ο έλεγχος της παραπάνω ιδιότητας συνίσταται αποκλειστικά στην *αποκωδικοποίηση* του y και την εξέταση αν πράγματι είναι κώδικας δέντρου υπολογισμού. Η βασική ιδιότητα που εμπλέκεται στην απόκωδικοποίηση είναι η $(y)_z = x$ η οποία είναι β.α. όπως είδαμε στην άσκηση 2.3.3.

Αν το y είναι πράγματι κώδικας ενός δέντρου υπολογισμού, τότε είναι αποτέλεσμα όχι μιας αλλά πολλαπλών κωδικοποιήσεων, και άρα χρειάζονται πολλαπλές αποκωδικοποιήσεις για να βρούμε τον υπολογισμό στον οποίο αντιστοιχεί. Έτσι, αν $y = \langle \lceil a \rceil, \lceil T_1 \rceil, \ldots, \lceil T_l \rceil \rangle$, όπου a είναι η ισότητα $f(x_1, \ldots, x_n) = z$, πρέπει

$(y)_1 = \lceil a \rceil = \langle \lceil f \rceil, \langle x_1, \ldots, x_n \rangle, z \rangle$,

$(y)_2 = \lceil T_1 \rceil$,

$(y)_{i+1} = \lceil T_i \rceil$, για $i \leq l$,

και εν συνεχεία

$((y)_1)_1 = \lceil f \rceil$,

$((y)_1)_2 = \langle x_1, \ldots, x_n \rangle$,

$((y)_1)_3 = z$

και εν συνεχεία,

$(((y)_1)_2)_1 = x_1$,

$(((y)_1)_2)_j = x_j$, για $j \leq n$, κλπ.

Ο έλεγχος για το αν αληθεύει η $C(y)$, συνίσταται στο να ξεδιπλώνουμε τα στοιχεία $(y)_i$, $((y)_i)_j$, $(((y)_i)_j)_k$ κλπ και να ελέγχουμε αν αυτά αντιστοιχούν είτε σε αρχικές συναρτήσεις, είτε σε κάποιο από τα σχήματα σύνθεσης, βασικής αναδρομής και ελαχιστοποίησης, με αντίστοιχες εισόδους, εξόδους κλπ. Όλη αυτή η διαδικασία είναι προφανώς β.α.

Έχοντας στα χέρια μας την ιδιότητα $C(y)$ ο ορισμός των ιδιοτήτων T_n και της συνάρτησης U είναι εύκολος. Αρκεί να θέσουμε

$$T_n(e, x_1, \ldots, x_n, y) \iff C(y) \;\&\; ((y)_1)_1 = e \;\&\; ((y)_1)_2 = \langle x_1, \ldots, x_n \rangle,$$

$$U(y) = ((y)_1)_3, \text{ αν το } y \text{ είναι κώδικας υπολογισμού, αλλιώς } U(y) = 0.$$

Τα T_n και U είναι προφανώς β.α.

Τώρα αν f είναι μια αναδρομική συνάρτηση με δείκτη e και $dom(f) \subseteq N^n$, $(x_1, \ldots, x_n) \in dom(f)$ αν και μόνον αν υπάρχει ένα δέντρο υπολογισμού με κώδικα y, δηλαδή αν $\exists y \; T_n(e, x_1, \ldots, x_n, y)$. Για να πάρουμε δε την τιμή $f(x_1, \ldots, x_n)$, αρκεί να θέσουμε $f(x_1, \ldots, x_n) = U(\mu y \; T_n(e, x_1, \ldots, x_n, y))$. QED

Παραδειγματα Αριθμητικοποιησης

Ας δώσουμε μερικά απλά παραδείγματα κωδικοποίησης αναδρομικών συναρτήσεων και δέντρων υπολογισμού.

1) Να βρεθεί ένας κώδικας $\lceil + \rceil$ για τη συνάρτηση $+$.

Έστω $f(x,y) = x + y$. Έχουμε δει ότι η f ορίζεται με την αναδρομή

$f(x,0) = x = \pi_{11}(x)$,

$f(x,y+1) = f(x,y) + 1 = S\pi_{33}(x,y,f(x,y))$,

δηλαδή $g = \pi_{11}$ και $h = S \circ \pi_{33}$. Άρα, σύμφωνα με τους παραπάνω ορισμούς,

$$\lceil + \rceil = \langle 4, \lceil h \rceil, \lceil g \rceil \rangle = \langle 4, \lceil S \circ \pi_{33} \rceil, \lceil \pi_{11} \rceil \rangle.$$

Τώρα η $S \circ \pi_{33}$ παράγεται με σύνθεση από τις S και π_{33}, άρα

$$\lceil S \circ \pi_{33} \rceil = \langle 3, \lceil S \rceil, \lceil \pi_{33} \rceil \rangle$$

και τέλος

$$\lceil S \rceil = 1, \ \lceil \pi_{33} \rceil = \langle 2,3,3 \rangle, \lceil \pi_{11} \rceil = \langle 2,1,1 \rangle.$$

Άρα τελικά,

$$\lceil + \rceil = \langle 4, \langle 3,1, \langle 2,3,3 \rangle \rangle, \langle 2,1,1 \rangle \rangle.$$

2) Να βρεθεί $\lceil \cdot \rceil$.

Θέτοντας $f(x,y) = x \cdot y$, έχουμε

$f(x,0) = 0 = c_0(x)$,

$f(x,y+1) = f(x,y) + x = (\pi_{33} + \pi_{31})(x,y,f(x,y))$,

δηλαδή $g = c_0$ και $h = \pi_{33} + \pi_{31}$. Άρα

$$\lceil \cdot \rceil = \langle 4, \lceil \pi_{33} + \pi_{31} \rceil, \lceil c_0 \rceil \rangle = \langle 4, \langle 3, \lceil + \rceil, \lceil \pi_{33} \rceil, \lceil \pi_{31} \rceil \rangle, \lceil c_0 \rceil \rangle =$$

$$\langle 4, \langle 3, \lceil + \rceil, \langle 2,3,3 \rangle, \langle 2,3,1 \rangle \rangle, 0 \rangle,$$

όπου το $\lceil + \rceil$ υπολογίστηκε πιο πάνω.

3) Έστω η συνάρτηση $f(x) = x^2$.

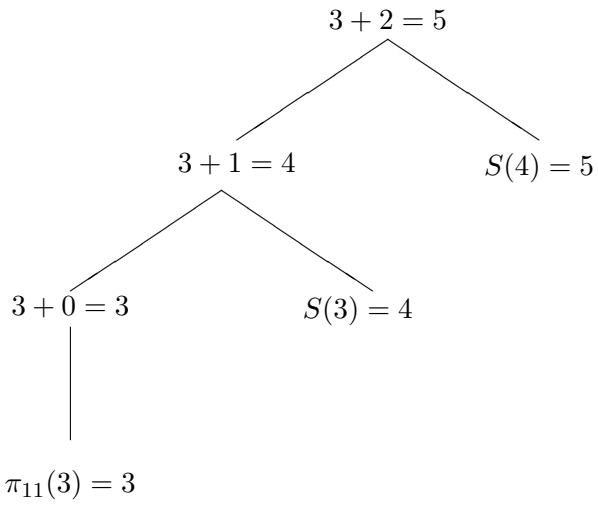
Η f μπορεί να θεωρηθεί είτε ότι παράγεται με σύνθεση από τις $\cdot$ και $id = \pi_{11}$, δηλαδή $f = \cdot \circ (\pi_{11}, \pi_{11})$, είτε ότι παράγεται με βασική αναδρομή από τις σχέσεις

$f(0) = 0 = c_0(x)$,

$f(x+1) = f(x) + 2x + 1 = f(x) + S(2x)$.

Οι παραπάνω είναι δύο διαφορετικοί αλγόριθμοι που θα δώσουν διαφορετικούς κώδικες e, e' για την f.

4) Σύμφωνα με τον αναδρομικό ορισμό της $+$, για να υπολογίσουμε π.χ. το $3+2$ πρέπει πρώτα να υπολογίσουμε το $3+0$, κατόπιν το $3+1$ και τέλος το $3+2$. Αυτό γράφεται υπό μορφή δέντρου υπολογισμού ως εξής:



Σχήμα 5

Ο κώδικας του παραπάνω δέντρου υπολογισμού T είναι

$$\ulcorner T\urcorner = \langle \ulcorner 3+2=5\urcorner, \ulcorner T_1\urcorner, \ulcorner T_2\urcorner\rangle = \langle\langle \ulcorner +\urcorner, \langle 3,2\rangle, 5\rangle, \ulcorner T_1\urcorner, \ulcorner T_2\urcorner\rangle,$$

όπου T_1, T_2 είναι τα υποδέντρα με ρίζες τους κόμβους $3+1=4$ και $S(4)=5$. Άρα

$$\ulcorner T_1\urcorner = \langle\langle \ulcorner +\urcorner, \langle 3,1\rangle, 4\rangle, \ulcorner T_3\urcorner, \ulcorner T_4\urcorner\rangle,$$

όπου T_3, T_4 τα υποδέντρα με ρίζες $3+0=3$ και $S(3)=4$, και

$$\ulcorner T_2\urcorner = \ulcorner S(4)=5\urcorner = \langle \ulcorner S\urcorner, 4, 5\rangle = \langle 1,4,5\rangle.$$

Όμοια

$$\ulcorner T_3\urcorner = \langle\langle \ulcorner +\urcorner, \langle 3,0\rangle, 3\rangle, \ulcorner T_4\urcorner, \ulcorner T_5\urcorner\rangle,$$

όπου

$$\ulcorner T_4\urcorner = \ulcorner \pi_{11}(3)=3\urcorner = \langle\langle 2,1,1\rangle, 3, 3\rangle$$

και

$$\ulcorner T_5\urcorner = \ulcorner S(3)=4\urcorner = \langle 1,3,4\rangle.$$

Άρα

$$\ulcorner T_3\urcorner = \langle\langle \ulcorner +\urcorner, \langle 3,0\rangle, 3\rangle, \langle\langle 2,1,1\rangle, 3, 3\rangle, \langle 1,3,4\rangle\rangle.$$

Επίσης

$$\ulcorner T_1\urcorner = \langle\langle \ulcorner +\urcorner, \langle 3,1\rangle, 4\rangle, \langle\langle \ulcorner +\urcorner, \langle 3,0\rangle, 3\rangle, \langle\langle 2,1,1\rangle, 3, 3\rangle, \langle 1,3,4\rangle\rangle, \langle\langle 2,1,1\rangle, 3, 3\rangle\rangle,$$

και τελικά

$$\ulcorner T \urcorner = \langle\langle\ulcorner+\urcorner, \langle 3,2\rangle, 5\rangle, \langle\langle\ulcorner+\urcorner, \langle 3,1\rangle, 4\rangle, \langle\langle\ulcorner+\urcorner, \langle 3,0\rangle, 3\rangle,$$
$$\langle\langle 2,1,1\rangle, 3, 3\rangle, \langle 1,3,4\rangle\rangle, \langle\langle 2,1,1\rangle, 3, 3\rangle\rangle, \langle 1,4,5\rangle\rangle,$$

όπου ο $\ulcorner+\urcorner$ υπολογίστηκε πιο πάνω.

Η αξία του θεωρήματος 2.7.1 είναι μεγάλη. Λέει ότι *όλες* οι n-μελείς αναδρομικές συναρτήσεις ορίζονται ομοιόμορφα από *μία* β.α. σχέση T_n $n+2$ θέσεων, όπου τη μία θέση κατέχει ο κώδικας της συνάρτησης, και *μία* β.α. αναδομική συνάρτηση U. Πέρα από την αισθητική του αξία, το θεώρημα αυτό είναι η βάση για την τη διαδικασία *απαρίθμησης* των αναδρομικών συναρτήσεων (δες § 4.1) και των γεγονότων που απορρέουν από αυτήν, δηλαδή το διπλό *παιγνίδι* των αριθμών, ως ορίσματα από τη μια και ως κώδικες συναρτήσεων από την άλλη.

Πέρα από αυτό μια άλλη εφαρμογή μας δίνει τους χαρακτηρισμούς των α.α. συνόλων ως πεδία τιμών και ορισμού αναδρομικών συναρτήσεων. Στη σχέση $T_n(e, \overline{x}, y)$, το y παριστά το ''μήκος του υπολογισμού'', δηλαδή είναι το ανάλογο του χρόνου αναμονής, το δε κατηγόρημα $T_n(e, \overline{x}, y))$ είναι το ανάλογο του αλγορίθμου αναμονής (dovetailing). Αν η f είναι μια (μερική εν γένει) συνάρτηση με δείκτη e, τότε προφανώς

$$f(\overline{x}) = u \iff (\exists y)[T_n(e, \overline{x}, y) \ \& \ U(y) = u], \tag{12}$$

και η σχέση $T_n(e, \overline{x}, y) \ \& \ U(y) = u$ είναι β.α.

Πρόταση 2.7.3 *Έστω $X \subseteq \mathbb{N}$. Τα παρακάτω είναι ισοδύναμα:*

(α) Το X είναι α.α.

(β) Το X είναι πεδίο τιμών μια αναδρομικής συνάρτησης (όχι κατ' ανάγκη ολικής).

(γ) Το X είναι είναι πεδίο ορισμού μιας αναδρομικής συνάρτησης.

Απόδειξη. Χωρίς περιορισμό της γενικότητας ας πάρουμε το X άπειρο.

(α)⇒(β): Τετριμμένο αφού κάθε ολική αναδρομική είναι αναδρομική συνάρτηση.

(β)⇒(α): Έστω $X = rng(f)$ και έστω $\ulcorner f \urcorner = e$ ένας δείκτης της f. Τότε $u \in X \iff (\exists n)(f(n) = u)$, και από την (12) έχουμε

$$u \in X \iff (\exists n)(\exists y)[T_1(e, n, y) \ \& \ U(y) = u].$$

Αφού η σχέση

$$T_1(e, n, y) \ \& \ U(y) = u$$

είναι αναδρομική, από την πρόταση 2.6.4 και την άσκηση 2.6.1, το X είναι α.α.

(α)⇒(γ): Έστω X α.α., δηλαδή $X = rng(f)$, f ολική αναδρομική. Ορίζουμε $h : \mathbb{N} \to \mathbb{N}$, ως εξής:

$h(n) = (\mu m)(f(m) = n)$.
Προφανώς η h είναι (μερική) αναδρομική και $dom(h) = rng(f) = X$.

(γ)⇒(β): Έστω $X = dom(f)$, όπου f αναδρομική, με κώδικα e. Από το Θεώρημα του Kleene, $x \in dom(f) \iff \exists y\ T_1(e, x, y)$, και το συμπέρασμα προκύπτει από την 2.6.4. Αλλιώς: Ορίζουμε την συνάρτηση g ως εξής: $g(x) = x + 0 \cdot f(x)$. Προφανώς η g είναι αναδρομική και $dom(g) = dom(f)$. Και για κάθε $x \in \mathbb{N}$,

$$x \in X \iff x \in dom(f) \iff x \in dom(g) \iff g(x) = x \iff x \in rng(g),$$

δηλαδή $X = rng(g)$. QED

3 Δεύτερη τυποποίηση των αναδρομικών συναρτήσεων: Μηχανές Turing

Στην § 2 είδαμε την πρώτη κύρια τυποποίηση των αλγοριθμικών συναρτήσεων, μέσω των αναδρομικών συναρτήσεων. Στο κεφάλαιο αυτό θα δούμε την δεύτερη κύρια τυποποίηση, και ίσως πιο δημοφιλή, μέσω των μηχανών Turing.

Ο Alan Turing το 1936 περιέγραψε μια θεωρητική υπολογιστική μηχανή που πήρε το όνομά του και υπήρξε ο πρόδρομος των πραγματικών υπολογιστών που εμφανίστηκαν 20 χρόνια αργότερα.

Η μηχανή Turing είναι το πιο διαισθητικό και συγχρόνως ακριβές μοντέλο υπολογιστικής διαδικασίας. Ενώ πρόκειται για *μαθηματικό* αντικείμενο (που θα το ορίσουμε αμέσως παρακάτω) και όχι, βέβαια, για μηχάνημα, μπορεί κανείς να έχει στο μυαλό του μια εικόνα της, σαν να πρόκειται για φυσικό αντικείμενο, πράγμα που βοηθάει τη διαίσθηση.

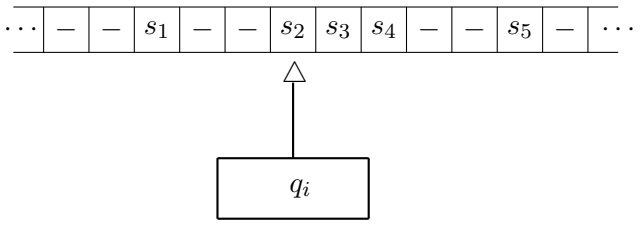
3.1 Γενική περιγραφή

Η εικόνα είναι η εξής (δίνουμε μία από τις πολλές παραλλαγές που υπάρχουν στη βιβλιογραφία): Η μηχανή αποτελείται από μία (σταθερή) ταινία απείρου μήκους[3], χωρισμένη σε τετράγωνα διαμερίσματα (cells) και μια κινούμενη κεφαλή, ή κέρσορα, (read/write head). Η κεφαλή κινείται δεξιά-αριστερά και ανά πάσα στιγμή εξετάζει (διαβάζει) ένα τετράγωνο (δες σχήμα 6)[4]. Κάθε τετράγωνο, περιέχει ανά πάσα στιγμή ένα σύμβολο ενός πεπερασμένου αλφαβήτου S (ή είναι κενό, το οποίο σημειώνεται με ένα ειδικό

[3] Η ταινία μπορεί να είναι άπειρη είτε μόνο προς τα δεξιά, οπότε τα τετράγωνα αριθμούνται με τους φυσικούς $0, 1, 2, \ldots$, είτε και προς τις δύο κατευθύνσεις, οπότε τα τετράγωνα αριθμούνται με τους ακεραίους $\ldots, -2, -1, 0, 1, 2, \ldots$.

[4] Αυτό είναι το μοντέλο ΜΤ με *κινούμενη κεφαλή* (Moving Head Turing Machine). Υπάρχει και το μοντέλο ΜΤ με *κινούμενη ταινία* (Moving Tape Turing Machine). Εδώ η κεφαλή είναι σταθερή και διαβάζει πάντα το τετράγωνο υπ' αριθμ. 0. Σάν υπολογιστικά συστήματα οι δύο τύποι είναι ισοδύναμοι. Όμως σαν *δυναμικά συστήματα* έχουν κάποιες διαφορές (δες [6]).

σύμβολο $-$ του S). Μόνο πεπερασμένου πλήθους τετράγωνα της ταινίας περιέχουν σύμβολο διαφορετικό του $-$.



Σχήμα 6

Η μηχανή μπορεί να εκτελέσει μία από τις παρακάτω στοιχειώδεις πράξεις (ανά χρονική στιγμή):

(α) Να γράψει ένα σύμβολο στο εξεταζόμενο τη στιγμή εκείνη τετράγωνο (αντικαθιστώντας το ήδη υπάρχον σύμβολο μ' ένα καινούργιο).

(β) Να μετακινηθεί μια θέση (τετράγωνο) αριστερά.

(γ) Να μετακινηθεί μια θέση δεξιά.

Κάθε τέτοια στοιχειώδης πράξη είναι ένα *βήμα* της μηχανής. Σε επίπεδο λογισμικού, υπάρχει ένας πεπερασμένος αριθμός *καταστάσεων* (states), $q_0, \ldots, q_k$, και σε κάθε στιγμή της λειτουργίας της η μηχανή βρίσκεται σε μια κατάσταση.

Η μηχανή λειτουργεί με βάση ένα ''πρόγραμμα'', δηλαδή ένα πεπερασμένο σύνολο εντολών. Κάθε εντολή είναι μια τετράδα της μορφής $q_i x y q_j$, όπου q_i, q_j καταστάσεις, $x \in S$ και $y \in S \cup \{L, R\}$ (τα L, R είναι από τις λέξεις left και right αντίστοιχα). Δηλαδή οι εντολές έχουν μία από τις εξής μορφές:

$$q_i s_k s_l q_j, \quad q_i s_k L q_j, \quad q_i s_k R q_j.$$

Η σημασία τους είναι η εξής:

• $q_i s_k s_l q_j$: Όταν η μηχανή είναι σε κατάσταση q_i και διαβάζει ένα τετράγωνο που περιέχει το σύμβολο s_k, τότε γράφει σ' αυτό το σύμβολο s_l και μεταβαίνει σε κατάσταση q_j.

• $q_i s_k L q_j$: Όταν η μηχανή είναι σε κατάσταση q_i και διαβάζει ένα τετράγωνο που περιέχει το σύμβολο s_k, τότε μετακινείται μια θέση αριστερά και μεταβαίνει σε κατάσταση q_j.

• $q_i s_k R q_j$: Όταν η μηχανή είναι σε κατάσταση q_i και διαβάζει ένα τετράγωνο που περιέχει το σύμβολο s_k, τότε μετακινείται μια θέση δεξιά και μεταβαίνει σε κατάσταση q_j.

Ο αυστηρός ορισμός είναι ο εξής:

Ορισμός 3.1.1 (Turing, 1936) Μια *(ντετερμινιστική) μηχανή Turing* (ΜΤ για συντομία) είναι μία τριάδα $M = (S, Q, F)$, όπου:

(α) S είναι ένα πεπερασμένο σύνολο συμβόλων, το *αλφάβητο* της μηχανής. Ένα από τα σύμβολα του S είναι το $-$, που σημαίνει ''κενό'' (blank).

(β) $Q = \{q_0, \ldots, q_f\}$ είναι ένα πεπερασμένο σύνολο *καταστάσεων* για την M, $Q \cap S = \emptyset$, όπου q_0 η *αρχική κατάσταση* και q_f η *τελική κατάσταση*,

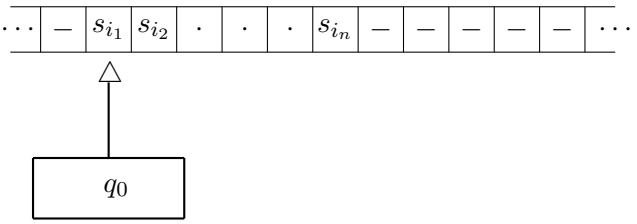
(γ) F είναι η *συνάρτηση μετάβασης* (transition function)

$$F : (Q - \{q_f\}) \times S \to Q \times (S \cup \{R, L\}),$$

όπου τα R, L είναι ειδικά σύμβολα που δεν ανήκουν στο S και στο Q.

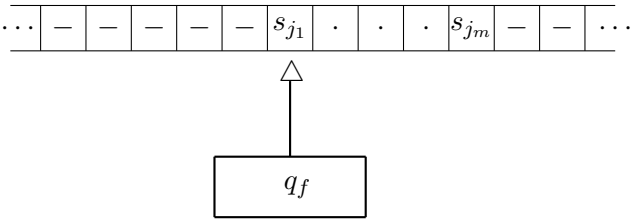
Η συνάρτηση F προσδιορίζει τις εντολές του προγράμματος. Για ευκολία αντί για $F(q_i, x) = (q_j, y)$, συμφωνούμε να γράφουμε $q_i x y q_j$, όπως κάναμε νωρίτερα. Η μηχανή ξεκινά πάντα σε κατάσταση q_0, και σταματά όταν περιέλθει στην τελική κατάσταση q_f (γι' αυτό και δεν ορίζεται το $F(q_f, x)$).

Οι είσοδοι και οι έξοδοι της μηχανής είναι λέξεις του αλφαβήτου S. Λόγω της παρουσίας του συμβόλου $-$ που αντιστοιχεί στο κενό, οι είσοδοι και οι έξοδοι είναι λέξεις που δεν αρχίζουν ούτε τελειώνουν με $-$. Τέτοιες λέξεις ας τις πούμε *γνήσιες*. Δοθείσης μιας γνήσιας λέξης $s_{i_1} \cdots s_{i_n}$, θέτουμε την μηχανή σε κατάσταση q_0, και την κεφαλή της να διαβάζει το ακρο-αριστερό γράμμα της λέξης s_{i_1} (ενώ παντού αλλού υπάρχει μόνο το σύμβολο $-$) (σχήμα 7).



Σχήμα 7

Η μηχανή ξεκινά ακολουθώντας το πρόγραμμα F. Αν και όταν σταματήσει, ως έξοδο θεωρούμε τη γνήσια λέξη $s_{j_1} \cdots s_{j_m}$ που είναι γραμμένη στην ταινία και στης οποίας το αριστερό άκρο είναι σταματημένη η κεφαλή σε κατάσταση q_f (σχήμα 8).



Σχήμα 8

Σε κάθε στιγμή η μηχανή βρίσκεται σε μια *υπολογιστική φάση* ή απλώς *φάση* (configuration). Μια φάση περιγράφεται πλήρως (1) από το περιεχόμενο της ταινίας (τη δεδομένη στιγμή), (2) την εσωτερική κατάσταση q της μηχανής, και (3) από τη θέση του κέρσορα, δηλαδή το ποιό τετράγωνο της ταινίας διαβάζει η κεφαλή. Το περιεχόμενο της ταινίας (αν τη θεωρήσουμε άπειρη και προς τις δύο κατευθύνσεις) είναι μια απεικόνιση $\sigma : \mathbf{Z} \to S$. Άρα, για να είμαστε ακριβείς, η φάση είναι μια τριάδα της μορφής (q, σ, n), όπου q η κατάσταση, σ το περιεχόμενο της ταινίας και $n \in \mathbf{Z}$ ο ακέραιος που δείχνει τη θέση του κέρσορα. Όμως, επειδή ο κέρσορας, σχεδόν πάντα, δείχνει κάποιο γράμμα της πεπερασμένης γνήσιας λέξης που υπάρχει στη ταινία, ή κάποιο από τα διπλανά $-$, πιο απλά και διαισθητικά η φάση γράφεται

$$(q, s_{i_1} \cdots \underline{s_{i_k}} \cdots s_{i_n}),$$

όπου $s_{i_1} \cdots s_{i_n}$ η γνήσια λέξη της ταινίας και το υπογραμμισμένο σύμβολο δείχνει τη θέση του κέρσορα. Ακόμη πρακτικότερα η φάση μπορεί να παρασταθεί ως εξής:

$$s_{i_1} \cdots q s_{i_k} \cdots s_{i_n},$$

δηλαδή το σύμβολο της κατάστασης μπαίνει αμέσως αριστερά του εξεταζόμενου συμβόλου.

Επειδή για κάθε κατάσταση q_i (πλήν της τελικής) και κάθε $x \in S$, η F προσδιορίζει ντετερμινιστικά την επόμενη κατάσταση q_j και το βήμα της μηχανής, δηλαδή το $F(q_i, x) = (q_j, y)$, είναι φανερό ότι από κάθε φάση a που δεν περιέχει την τελική κατάσταση q_f, πηγαίνουμε στην *αμέσως επόμενη ή διάδοχη φάση* a', μέσω μιας εντολής της μορφής $q_i x y q_j$. Αν συμβολίσουμε με γ την εντολή αυτή, αυτή τη μετάβαση τη συμβολίζουμε $a \xrightarrow{\gamma} a'$, ή απλώς $a \to a'$. Μία *αρχική φάση* είναι της μορφής $q_0 s_{i_1} \cdots s_{i_n}$, ενώ μια *τελική φάση* είναι της μορφής $q_f s_{i_1} \cdots s_{i_n}$. Ένας *υπολογισμός* (computation) είναι μια ακολουθία φάσεων, πεπερασμένη ή άπειρη,

$$a_0 \to a_1 \to \cdots \to a_f,$$

ή

$$a_0 \to a_1 \to \cdots \to a_i \to a_{i+1} \to \cdots,$$

όπου η a_0 είναι αρχική φάση, a_f τελική, και κάθε a_{i+1} είναι διάδοχη της a_i. Ο πρώτος είναι ένας *τερματιζόμενος υπολογισμός* (terminated computation), ενώ ο δεύτερος είναι μη τερματιζόμενος.

Κάθε ΜΤ M ορίζει με φυσικό τρόπο μία (μερική) συνάρτηση $\widehat{M} : S^* \to S^*$ από το σύνολο των (γνήσιων) λέξεων του S στον εαυτό του, που ορίζεται ως εξής: Έστω $x = s_{i_1} \cdots s_{i_n}$ μία γνήσια λέξη του S. Αν ο υπολογισμός που αρχίζει με τη φάση $a_0 = q_0 s_{i_1} \cdots s_{i_n}$ είναι τερματιζόμενος, και $a_f = q_f s_{j_1} \cdots s_{j_n}$ είναι η τελική του φάση, τότε

$$\widehat{M}(s_{i_1} \cdots s_{i_n}) = s_{j_1} \cdots s_{j_m}.$$

Αν ο υπολογισμός δεν είναι τερματιζόμενος, το $\widehat{M}(s_{i_1} \cdots s_{i_n})$ δεν ορίζεται.

3.2 Turing υπολογίσιμες συναρτήσεις

Τα παραπάνω περιγράφουν τη γενική μορφή και λειτουργία των ΜΤ. Όταν τώρα θέλουμε η μηχανή να επεξεργάζεται μόνο φυσικούς αριθμούς, είναι αρκετό να πάρουμε ως αλφάβητο απλώς το σύνολο $S = \{-, |\}$, όπου $-$ είναι όπως πριν το σύμβολο του κενού. Οι αριθμοί εδώ γράφονται στο ενικό (unary) σύστημα του μοναδικού ψηφίου $|$: Ο 0 γράφεται $|$, ο 1 γράφεται $||$, ο n γράφεται $\underbrace{|\cdots|}_{n+1}$ (δηλαδή το $|$ δεν είναι ο αριθμός ''ένα'', αλλά μια ''χαρακιά''(tally)). Γενικότερα η n-άδα $(n_1, \ldots, n_k) \in \mathbb{N}^k$ παρίσταται από τη λέξη

$$\underbrace{|\cdots|}_{n_1+1} - \underbrace{|\cdots|}_{n_2+1} - \cdots - \underbrace{|\cdots|}_{n_k+1}$$

Ορισμός 3.2.1 Έστω $f : \mathbb{N}^k \to \mathbb{N}$ μια συνάρτηση. Η f λέγεται *Turing-υπολογίσιμη* (Turing-computable), αν υπάρχει ΜΤ M με αλφάβητο $S = \{-, |\}$, τέτοια ώστε για κάθε $n_1, \ldots, n_k, m \in \mathbb{N}$, $f(n_1, \ldots, n_k) = m$ αν και μόνον αν

$$\widehat{M}(\underbrace{|\cdots|}_{n_1+1} - \underbrace{|\cdots|}_{n_2+1} - \cdots - \underbrace{|\cdots|}_{n_k+1}) = \underbrace{|\cdots|}_{m+1},$$

δηλαδή ο υπολογισμός που αρχίζει με τη φάση $q_0 \underbrace{|\cdots|}_{n_1+1} - \underbrace{|\cdots|}_{n_2+1} - \cdots - \underbrace{|\cdots|}_{n_k+1}$, τερματίζει με τη φάση $q_f \underbrace{|\cdots|}_{m+1}$.

Είναι προφανές ότι κάθε Turing-υπολογίσιμη συνάρτηση είναι αλγοριθμική, με αλγόριθμο το ''πρόγραμμα'' της μηχανής. Άρα οι Turing-υπολογίσιμες συναρτήσεις συνιστούν μία εναλλακτική αυστηρή προσέγγιση της αλγοριθμικότητας. Οι συναρτήσεις αυτές

ορίστηκαν την ίδια περίπου εποχή με τις αναδρομικές, οπότε φυσικά τέθηκε το ερώτημα για τη σχέση τους με τις τελευταίες. Δηλαδή ποιά είναι η σχέση της κλάσης των αναδρομικών και της κλάσης των Turing-υπολογίσιμων; Αποδεικνύεται ότι αυτές οι κλάσεις ταυτίζονται (χωρίς βέβαια την επίκληση της Θέσης του Church. Η Θέση του Church ήρθε ακριβώς ως συμπέρασμα αυτής της ταύτισης). Θα σκιαγραφήσουμε τις αποδείξεις των θεωρημάτων που αποδεικνύουν αυτή την ισότητα. Ένα συνηθισμένο πρόβλημα ''πρωτόγονου προγραμματισμού'' σ' αυτό το χώρο είναι: Δοθείσης (αλγοριθμικής) συνάρτησης f, βρείτε ΜΤ που να την υπολογίζει. Αφού το αλφάβητο σ' όλες αυτές τις μηχανές είναι το ίδιο, $S = \{-, |\}$, το να βρούμε ΜΤ σημαίνει να γράψουμε ένα κατάλληλο σύνολο εντολών της μορφής $q_i x y q_j$ για έναν ικανό αριθμό καταστάσεων $Q = \{q_0, \ldots, q_f\}$, που θα τον προσδιορίσουμε εμείς ανάλογα με τις ανάγκες μας. (Άρα, σταθεροποιώντας το αλφάβητο, η ΜΤ δεν είναι παρά ένα πρόγραμμα.) Εδώ, ανάλογα με την όρεξη και το ταλέντο του, μπορεί κανείς να ασκηθεί κατά βούληση. Εμείς θα δώσουμε μόνο κάποια αναγκαία παραδείγματα. Λόγου χάρη έχουμε το εξής:

Πρόταση 3.2.2 *Οι αρχικές συναρτήσεις είναι Turing-υπολογίσιμες.*

Απόδειξη. Θα κατασκευάσουμε ΜΤ για τον υπολογισμό της S, της σταθεράς c_0 και των προβολών.

(α) ΜΤ για την $S(x) = x + 1$. Πρέπει να φτιάξουμε ένα πρόγραμμα έτσι ώστε ξεκινώντας με τη φάση $q_0 \underbrace{|\cdots|}_{n+1}$ να τερματίζουμε στη φάση $q_f \underbrace{|\cdots|}_{n+2}$. Θεωρούμε το πρόγραμμα με τρείς καταστάσεις $Q = \{q_0, q_1, q_f\}$ και εντολές:

$$\gamma_1 = q_0|Rq_0,\ \gamma_2 = q_0 - |q_1,\ \gamma_3 = q_1|Lq_1,\ \gamma_4 = q_1 - Rq_f.$$

Τότε π.χ. για είσοδο ''2'', που παρίσταται με τη λέξη $|||$, έχουμε τον υπολογισμό:

$$q_0||| \xrightarrow{\gamma_1} |q_0|| \xrightarrow{\gamma_1} ||q_0| \xrightarrow{\gamma_1} |||q_0- \xrightarrow{\gamma_2} |||q_1|$$
$$\xrightarrow{\gamma_3} ||q_1|| \xrightarrow{\gamma_3} |q_1||| \xrightarrow{\gamma_3} q_1|||| \xrightarrow{\gamma_3} q_1 - |||| \xrightarrow{\gamma_4} q_f||||.$$

Άρα έχουμε έξοδο $||||$ που παριστά τον ''3''. Το ίδιο γίνεται με κάθε είσοδο $\underbrace{|\cdots|}_{n+1}$. Η ιδέα είναι η εξής: Ο κέρσορας σε κατάσταση q_0, όταν διαβάζει $|$ προχωρεί συνεχώς δεξιά. Μόλις συναντήσει $-$ το κάνει $|$ και αλλάζει την κατάστασή του σε q_1. Τώρα, διαβάζοντας $|$ προχωρεί αριστερά, δηλαδή γυρίζει πίσω, μέχρι να συναντήσει το πρώτο $-$. Τότε γυρίζει πάλι δεξιά, και πάει σε τελική κατάσταση, άρα σταματά. Το αποτέλεσμα είναι να έχει προστεθεί ένα $|$ στο τέλος της προηγούμενης λέξης και ο κέρσορας να είναι ξανά στην παλιά του θέση.

(β) Ερχόμαστε στη σταθερή συνάρτηση, $c_0(x) = 0$. Εδώ πρέπει ξεκινώντας με τη φάση $q_0\underbrace{|\cdots|}_{n+1}$ να τερματίζουμε στη φάση $q_f|$. Εδώ πάλι θεωρούμε ένα σύνολο τριών καταστάσεων $Q = \{q_0, q_1, q_f\}$. Η ιδέα είναι για είσοδο $\underbrace{|\cdots|}_{n+1}$, η μηχανή να σβήνει όλες τις μονάδες, αφήνοντας στο τέλος μία και να σταματάει. Αρκεί να πάρουμε το πρόγραμμα:

$$\gamma_1 = q_0| - q_1,\ \gamma_2 = q_1 - Rq_0,\ \gamma_3 = q_0 - |q_f.$$

Έτσι, π.χ. για είσοδο $|||$ θα έχουμε:

$$q_0||| \xrightarrow{\gamma_1} q_1 - || \xrightarrow{\gamma_2} q_0|| \xrightarrow{\gamma_1} q_1 - | \xrightarrow{\gamma_2} q_0| \xrightarrow{\gamma_1}$$
$$q_1 - \xrightarrow{\gamma_2} q_0 - \xrightarrow{\gamma_3} q_f|.$$

(γ) Έστω η προβολή $\pi_{nm} : \mathbb{N}^n \to \mathbb{N}$, όπου $\pi(x_1, \ldots, x_n) = x_m$. Εδώ πρέπει να φτιάξουμε ένα πρόγραμμα το οποίο για είσοδο

$$\underbrace{|\cdots|}_{x_1+1} - \underbrace{|\cdots|}_{x_2+1} - \cdots - \underbrace{|\cdots|}_{x_n+1},$$

να σβήνει όλες τις μονάδες εκτός εκείνες του m-block, δηλαδή να δίνει έξοδο $\underbrace{|\cdots|}_{x_m+1}$. Αυτό μπορεί να γίνει χρησιμοποιώντας για παράδειγμα $2n + 5$ καταστάσεις $q_0, q_0', q_1, q_1', \ldots q_n, q_n', q_{n+1}, q_{n+1}', q_f$. Κάθε ζεύγος q_i, q_i', $i \leq n$, $i \neq m$, θα χρησιμεύσει για να σβηστούν τα i-blocks, για $i \neq m$, όπως έγινε στο (β). Το ζεύγος q_m, q_m', θα χρησιμεύσει για τη διατήρηση του m-block, ενώ οι υπόλοιπες θα χρειαστούν για να επιστρέψει ο κέρσορας στην αρχή του m-block και να σταματήσει. Η ακριβής γραφή του συγκεκριμένου προγράμματος να γίνει σαν άσκηση. QED

Η ΜΤ δεν έχει χωριστή ''μνήμη'', δηλαδή έναν χώρο όπου να αποθηκεύει πληροφορίες και να τις ανακαλεί όποτε χρειάζεται. Ο μόνος τρόπος να ''θυμάται'' είναι μέσω των κατάλληλων καταστάσεων. Αυτό κάνει ώστε διαδικασίες που φαίνονται πολύ απλές για έναν συνηθισμένο υπολογιστή, να απαιτούν αρκετά πολύπλοκο πρόγραμμα σε μια ΜΤ, και μεγάλο αριθμό καταστάσεων.

Παραδειγμα-Ασκηση 1. Να κατασκευασθεί ΜΤ που να εκτελεί την εντολή ''φτιάξε αντίγραφο της λέξης s προς τα δεξιά της αφήνοντας δύο κενά ανάμεσα''. Για απλότητα ας αντιγράφει απλώς λέξεις της μορφής $\underbrace{|\cdots|}_{n+1}$, δηλαδή για είσοδο $\underbrace{|\cdots|}_{n+1}$ να δίνει έξοδο $\underbrace{|\cdots|}_{n+1} - - \underbrace{|\cdots|}_{n+1}$.

Απάντηση. Περιγράφουμε πρώτα με λόγια τον αλγόριθμο. Έστω $s = \underbrace{|\cdots|}_{n+1}$ η είσοδος.

Βήμα 1. Πήγαινε στο δεξιό άκρο της s, άφησε δύο κενά και γράψε ένα |.

Βήμα 2. Γύρισε πίσω, αναζήτησε το δεξιό | της s και σβήστο.

Βήμα 3. Έλεγξε αν το | που σβήστηκε προηγουμένως ήταν το τελευταίο (δηλαδή αν αριστερά του υπάρχει άλλο | ή όχι). Αν όχι τότε:

Βήμα 3.1. Πήγαινε γράψε αμέσως μετά το | που έγραψες προηγουμένως ένα ακόμη |. Εν συνεχεία επανέλαβε το Βήμα 2. Αν ναι τότε:

Βήμα 3.2. Ξαναγράψε την είσοδο s (γράφοντας διαδοχικά | προς τα δεξιά μέχρι να συναντήσεις το επόμενο | και τότε σβήνοντας δύο για να μείνουν δύο κενά ανάμεσα στο s και το αντίγραφό του).

Θα υλοποιήσουμε παρακάτω αυτόν τον αλγόριθμο με μια MT με 17 καταστάσεις (πιθανόν ο αριθμός αυτός να μπορεί να μειωθεί). Ας δούμε με τι εντολές υλοποιείται το κάθε ένα από τα παραπάνω βήματα. Ξεκινάμε με αρχική κατάσταση q_0, και στην πορεία εισάγουμε νέες καταστάσεις και ανάλογες εντολές καθοδηγούμενοι απ' τον αλγόριθμο. Ας πάρουμε για οδηγό την είσοδο $s = |||$. Το πρόγραμμα που θα ορίσουμε όμως δουλεύει για κάθε $s = \underbrace{|\cdots|}_{n+1}$

Βήμα 1. Ορίζουμε:

$$q_0||| \overset{q_0|Rq_0}{\longrightarrow} |q_0|| \overset{q_0|Rq_0}{\longrightarrow} ||q_0| \overset{q_0|Rq_0}{\longrightarrow} |||q_0- \overset{q_0-Rq_1}{\longrightarrow} ||| - q_1- \overset{q_1-Rq_2}{\longrightarrow}$$

$$||| - -q_2- \overset{q_2-|q_3}{\longrightarrow} ||| - -q_3|$$

Βήμα 2. Ορίζουμε:

$$||| - -q_3| \overset{q_3|Lq_4}{\longrightarrow} ||| - q_4 - | \overset{q_4-Lq_4}{\longrightarrow} |||q_4 - -| \overset{q_4-Lq_4}{\longrightarrow}$$

$$||q_4| - -| \overset{q_4|-q_5}{\longrightarrow} ||q_5 - - - |.$$

Βήμα 3. Ορίζουμε:

$$||q_5 - - - | \overset{q_5-Lq_6}{\longrightarrow} |q_6| - - - |.$$

Στο σημείο αυτό αν ο κέρσορας διαβάζει |, είμαστε στο Βήμα 3.1, ενώ αν διαβάζει −, είμαστε στο Βήμα 3.2. Στην προκειμένη περίπτωση είμαστε στο

Βήμα 3.1. Ορίζουμε:

$$|q_6| - - - | \overset{q_6|Rq_7}{\longrightarrow} ||q_7 - - - | \overset{q_7-Rq_7}{\longrightarrow} || - q_7 - -| \overset{q_7-Rq_7}{\longrightarrow} || - -q_7 - |$$

$$\overset{q_7-Rq_7}{\longrightarrow} ||---q_7| \overset{q_7|Rq_8}{\longrightarrow} ||---|q_8- \overset{q_8-|q_8}{\longrightarrow} ||---|q_8| \overset{q_8|Lq_9}{\longrightarrow}$$

$$||---q_9|| \overset{q_9|Lq_9}{\longrightarrow} ||--q_9-|| \overset{q_9--q_4}{\longrightarrow} ||-q_4-||.$$

Βλέπουμε ότι με την τελευταία φάση έχουμε επανέλθει στο Βήμα 2 (βρόχος). Αφού εκτελέσουμε δύο φορές αυτόν τον βρόχο, θα σβηστούν όλα τα | της αρχικής λέξης και θα έρθουμε στη φάση $q_6 -----|||$. Τώρα είμαστε στο

Βήμα 3.2. Ορίζουμε:

$$q_6 -----|||\overset{q_6-|q_{10}}{\longrightarrow} q_{10}|----|||\overset{q_{10}|Rq_{11}}{\longrightarrow} |q_{11}---|||\overset{q_{11}-|q_{10}}{\longrightarrow}$$

$$|q_{10}|---|||\overset{q_{10}|Rq_{11}}{\longrightarrow} ||q_{11}---|||\overset{q_{11}-|q_{10}}{\longrightarrow} ||q_{10}|--|||$$

$$\overset{q_{10}|Rq_{11}}{\longrightarrow} |||q_{11}--|||\overset{q_{11}-|q_{10}}{\longrightarrow} |||q_{10}|-|||\overset{q_{10}|Rq_{11}}{\longrightarrow} ||||q_{11}-|||$$

$$\overset{q_{11}-|q_{10}}{\longrightarrow} ||||q_{10}||||\overset{q_{10}|Rq_{11}}{\longrightarrow} |||||q_{11}|||\overset{q_{11}|Lq_{12}}{\longrightarrow} ||||q_{12}||||$$

$$\overset{q_{12}|-q_{13}}{\longrightarrow} ||||q_{13}-|||\overset{q_{13}-Lq_{12}}{\longrightarrow} |||q_{12}|-|||\overset{q_{12}|-q_{13}}{\longrightarrow} |||q_{13}--|||$$

$$\overset{q_{13}-Lq_{14}}{\longrightarrow} ||q_{14}|--|||\overset{q_{14}|Lq_{14}}{\longrightarrow} |q_{14}||--|||\overset{q_{14}|Lq_{14}}{\longrightarrow} q_{14}|||--|||$$

$$\overset{q_{14}|Lq_{15}}{\longrightarrow} q_{15}-|||--|||\overset{q_{15}-Rq_f}{\longrightarrow} q_f|||--|||.$$

Παραδειγμα-Ασκηση 2. Μια σημαντική κατηγορία μηχανών Turing είναι οι ‘‘ναι-όχι’’ μηχανές, δηλαδή εκείνες όπου η έξοδος δεν είναι μια λέξη αλλά ένα ‘‘ναί’’ ή ένα ‘‘όχι’’. (Π.χ. όλα τα ‘‘αυτόματα’’ είναι αυτού του είδους.) Στις μηχανές αυτές το σύνολο των καταστάσεων Q περιέχει μεταξύ άλλων και τις ειδικές καταστάσεις ‘‘yes’’ και ‘‘no’’. Δηλαδή $Q = \{yes, no, q_0, q_1, \ldots\}$. Οι καταστάσεις yes και no είναι *τελικές* καταστάσεις, δηλαδή όταν η μηχανή βρεθεί σε φάση που περιέχει το yes ή το no, σταματά. Έστω M μια ναι-όχι μηχανή με αλφάβητο S. Μία λέξη $x \in S^*$ λέγεται *αποδεκτή* από την M, αν ο υπολογισμός που ξεκινά με τη φάση q_0x τερματίζει σε μία φάση της μορφής $y“yes”z$. Το σύνολο

$$L(M) = \{x \in S^* : \ x \text{ αποδεκτή από την } M\}$$

λέγεται η *γλώσσα* της M.

Έστω ένα αλφάβητο $S = \{-, 0, 1, \times, \ldots\}$. Μία δυαδική λέξη, δηλαδή $\{0,1\}$-λέξη, του S λέγεται *παλίνδρομο* αν διαβάζεται το ίδιο από αριστερά προς τα δεξιά και αντίστροφα. Π.χ. η λέξη 1100011 είναι παλίνδρομο ενώ η 0100011 δεν είναι. Ζητείται να κατασκευαστεί μηχανή M (δηλαδή πρόγραμμα) που να δέχεται ακριβώς τα παλίνδρομα, δηλαδή $L(M) = \{x \in \{0,1\}^* : x \text{ παλίνδρομο}\}$.

Η ιδέα είναι ελέγχουμε ένα-ένα τα ζεύγη των συμμετρικών ψηφίων της λέξης. Αν σε κάποιο τέτοιο ζεύγος τα ψηφία διαφέρουν, η απάντηση είναι no. Αλλιώς η απάντηση είναι ναι. Θα χρησιμοποιήσουμε για το σκοπό αυτό το βοηθητικό σύμβολο $\times$. Θα χρειαστούμε επίσης καταστάσεις l_0, l_1 με τις οποίες η μηχανή ''θυμάται'' αν ένα σύμβολο που έλεγξε από αριστερά ήταν 0 ή 1 αντίστοιχα, καθώς και καταστάσεις r_0, r_1 για να ''θυμάται'' το ίδιο για τα σύμβολα που ελέγχει από δεξιά. Τα βήματα είναι τα εξής:

1) Η μηχανή ξεκινά με αρχική φάση q_0x. Βλέπει το πρώτο σύμβολο της x. Αν είναι 0 το αντικαθιστά με $\times$ και πηγαίνει σε κατάσταση l_0 (δηλαδή ''θυμάται'' ότι συνάντησε 0). Αν είναι 1 το αντικαθιστά με $\times$ και πηγαίνει σε κατάσταση l_1.

2) Οντας τώρα σε κατάσταση l_0 ή l_1, κινείται σταθερά δεξιά (προσπερνώντας τα σύμβολα $\times$, 0,1) μέχρι να συναντήσει το πρώτο $-$. Τότε κινείται μια θέση αριστερά και πάει σε κατάσταση r_0 ή r_1 αντίστοιχα.

3) Αν είναι σε r_0 και συναντήσει 1, η είναι σε r_1 και συναντήσει 0, γράφει no και σταματά. Αλλιώς αντικαθιστά το 0 ή το 1 με $-$, πηγαίνει σε κατάσταση q, και κινείται αριστερά μέχρι να συναντήσει το $\times$.

4) Αν συναντήσει $\times$, τότε κινείται μια θέση δεξιά, και πάει σε κατάσταση q_0. Τώρα συνεχίζει όπως στο βήμα 1). Αν σβηστούν όλα τα ψηφία 0,1 και μείνουν μόνο $\times$ και $-$, η μηχανή δίνει yes και σταματά.

Τα παραπάνω δίνουν το ακόλουθο σύνολο εντολών με σύνολο καταστάσεων $Q = \{yes, no, q_0, q, l_0, l_1, r_0, r_1\}$:

(11) $q_0 0 \times l_0$, (12) $q_0 1 \times l_1$, (13) $q_0 - yes$,
(21) $l_0 \times R l_0$, (22) $l_0 0 R l_0$, (23) $l_0 1 R l_0$, (24) $l_0 - L r_0$
(31) $l_1 \times R l_1$, (32) $l_1 0 R l_1$, (33) $l_1 1 R l_1$, (34) $l_1 - L r_1$
(41) $r_1 0 no$, (42) $r_1 1 - q$, (43) $r_1 \times yes$,
(51) $r_0 1 no$, (52) $r_0 0 - q$, (53) $r_0 \times yes$,
(61) $q 0 L q$, (62) $q 1 L q$, (63) $q \times R q_0$.

Ας εφαρμόσουμε τα παραπάνω στη λέξη 101:

$$q_0 101 \xrightarrow{12} l_1 \times 01 \longrightarrow^* \times 01 l_1 - \xrightarrow{34} \times 0 r_1 1$$
$$\times 0 r_1 1 \xrightarrow{42} \times 0 q - \longrightarrow^* q \times 0 - \xrightarrow{63} \times q_0 0$$
$$\times q_0 0 \xrightarrow{11} l_0 \times \xrightarrow{21} \times l_0 - \xrightarrow{24} r_0 \times - \xrightarrow{53} yes$$

Ασκήσεις

3.2.1 Κατασκευάστε μηχανές Turing για τις συναρτήσεις: (α) $x+y$, (β) $f(x)=3$, (γ) $f(x)=2x$.

Προκειμένου να δείξουμε ότι κάθε αναδρομική συνάρτηση είναι Turing- υπολογίσιμη, πρέπει να παρατηρήσουμε ότι αν έχουμε n μηχανές Turing $M_1,\ldots,M_n$, τότε μπορούμε να βρούμε μία M που θα προσομοιώνει τη λειτουργία κάθε μιας από τις M_i. Αυτό είναι σαν να έχετε n ανεξάρτητα προγράμματα, και να τα ''συγκολλάτε'' σε ένα που τα περιέχει ως υποπρογράμματα. Π.χ. αν $Q_i=\{q_{i0},\ldots,q_{if}\}$ είναι το σύνολο των καταστάσεων και Γ_i το σύνολο των εντολών της M_i, μπορούμε να θεωρήσουμε ότι τα Q_i είναι ξένα σύνολα (αλλιώς θεωρούμε ξένα αντίγραφα), και να πάρουμε ως σύνολο καταστάσεων της M ένα Q τέτοιο ώστε $\bigcup_i Q_i\subseteq Q$. Επίσης τροποποιώντας κατάλληλα τις εντολές των Γ_i (ειδικά εκείνες που αφορούν τις τελικές καταστάσεις q_{if}, ώστε να μην είναι τώρα τελικές), μπορούμε να διαμορφώσουμε το πρόγραμμα Γ της M, ώστε να καλεί ανάλογα με τον σκοπό που επιδιώκουμε τα υποπρογράμματα Γ_i.

Μιά διευκόλυνση που μπορούμε να εισάγουμε είναι ότι όταν ξεκινά ένας υπολογισμός $-q_0s_{i_1}\cdots s_{i_m}-$, δηλαδή με είσοδο $s_{i_1}\cdots s_{i_m}$, ο κέρσορας δεν κινείται ποτέ αριστερότερα του $-$ που κείται αριστερά του s_{i_1}. Μ' άλλα λόγια οι υπολογισμοί διεξάγονται στο δεξιό τμήμα της ταινίας που ορίζει η αρχή της λέξης.

Θεώρημα 3.2.3 (Turing 1936) *Κάθε αναδρομική συνάρτηση είναι Turing- υπολογίσιμη.*

Απόδειξη. Με επαγωγή στα βήματα κατασκευής μιας αναδρομικής συνάρτησης.
(α) Για τις αρχικές το δείξαμε στην πρόταση 3.2.2.
(β) Έστω ότι η f παράγεται με σύνθεση από τις h, $g_1,\ldots,g_m$, δηλαδή

$$f(x_1,\ldots,x_k)=h(g_1(x_1,\ldots,x_k),\ldots,g_m(x_1,\ldots,x_k)),$$

και ότι οι h, $g_1,\ldots,g_m$ είναι Turing- υπολογίσιμες με τις μηχανές M_0, $M_1,\ldots,M_m$ αντίστοιχα. Θεωρούμε μία μηχανή M που προσομοιώνει τις M_0, $M_1,\ldots,M_m$, με τον τρόπο που περιγράψαμε πιο πριν και όταν δοθεί μια είσοδος

$$s=\underbrace{|\cdots|}_{x_1+1}-\underbrace{|\cdots|}_{x_2+1}-\cdots-\underbrace{|\cdots|}_{x_k+1},$$

κάνει τα εξής:

1) Ξεκινά με την αρχική φάση q_0s, αντιγράφει την είσοδο μια φορά προς τα δεξιά αφήνοντας δύο κενά ανάμεσά τους, και πηγαίνει στην αρχή του αντιγράφου σε κατάσταση q_{m0} (αρχική της M_m), δηλαδή στη φάση

$$s--q_{m0}s.$$

2) Τώρα αρχίζει να δουλεύει το υποπρόγραμμα M_m με είσοδο s, και θα δώσει μία έξοδο t_m (που παριστά την τιμή $g_m(x_1, \ldots, x_k)$). (Επειδή οι υπολογισμοί γίνονται προς τα δεξιά, όπως συμφωνήσαμε παραπάνω, η ύπαρξη του αντιγράφου της s προς τα αριστερά του κέρσορα δεν επηρεάζει τον υπολογισμό.) Τώρα η M είναι σε φάση

$$s - -q_{mf}t_m.$$

3) Κατόπιν μεταφέρει τη λέξη t_m αριστερά της s, αφήνοντας δύο κενά ανάμεσά τους, αντιγράφει ξανά την s προς τα δεξιά της, και τίθεται στην αρχή του αντιγράφου σε κατάσταση $q_{m-1,0}$ (αρχική της M_{m-1}), δηλαδή σε φάση

$$t_m - -s - -q_{m-1,0}s.$$

4) Τώρα δουλεύει το υποπρόγραμμα M_{m-1} με είσοδο s και δίνει έξοδο t_{m-1} (=η τιμή $g_{m-1}(x_1, \ldots, x_k)$), την οποία μεταφέρει αριστερά της t_m, με ένα κενό ανάμεσά τους, αντιγράφει την είσοδο, και έρχεται στη φάση

$$t_{m-1} - t_m - -s - -q_{m-2,0}s.$$

5) Συνεχίζοντας με τον ίδιο τρόπο φτάνει στη φάση

$$t_1 - t_2 - \cdots - t_m - -q_p s,$$

όπου q_p κάποια κατάσταση.

6) Τώρα σβήνει τη λέξη s και έρχεται στο αριστερό άκρο της λέξης $t_1 - t_2 - \cdots - t_m$, σε κατάσταση q_{00} (αρχική της μηχανής M_0), δηλαδή σε φάση

$$q_{00}t_1 - t_2 - \cdots - t_m.$$

7) Όμως η λέξη $t_1 - t_2 - \cdots - t_m$ παριστά την m-άδα

$$(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k)),$$

η δέ M_0 υπολογίζει τη συνάρτηση h, άρα όταν τερματίσει ο υπολογισμός που ξεκινά με τη φάση $q_{00}t_1 - t_2 - \cdots - t_m$ και δώσει τελική φάση

$$q_{0f}r,$$

η λέξη r παριστά την τιμή $h(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k))$, δηλαδή $f(x_1, \ldots, x_k)$. Συνεπώς η M είναι μηχανή Turing για την f.

(γ) Έστω ότι η f παράγεται με βασική αναδρομή από τις g και h, δηλαδή

$f(\overline{x}, 0) = g(\overline{x})$,

$f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$,

και ότι οι g, h είναι Turing-υπολογίσιμες με τις μηχανές M_0, M_1 αντίστοιχα. Έστω

M μια μηχανή που προσομοιώνει τις M_0, M_1. Έστω s παριστά το διάνυσμα $\overline{x}$ και t_y παριστά τον αριθμό y. Τότε μια είσοδος έχει τη μορφή $s - t_y$. Ξεκινάμε τη μηχανή με την φάση

$$q_0 s - t_y.$$

Η M ελέγχει πρώτα τη μορφή του t_y. Αν $y = 0$, δηλαδή $t_y = |$, τότε ο κέρσορας σβήνει το t_0, επιστρέφει στην αφετηρία του σε κατάσταση q_{00} (αρχική της M_0), δηλαδή σε φάση $q_{00}s$, και εκτελεί τον υπολογισμό που αντιστοιχεί στο $g(\overline{x})$. Αν $y > 0$, τότε η μηχανή γράφει δεξιά της εισόδου, διαδοχικά τις λέξεις $s - t_{y-1}$, $s - t_{y-2}, \ldots s - t_0$, s, αφήνοντας δύο κενά ανάμεσά τους, σβήνει την αρχική είσοδο $s - t_y$, και έρχεται στην αρχή της λέξης s σε κατάσταση q_{00}, δηλαδή στη φάση:

$$s - t_{y-1} - -s - t_{y-2} - - \cdots - -s - t_0 - -q_{00}s.$$

Τώρα μιμείται την M_0, εκτελεί τον υπολογισμό, δίνει έξοδο r_0, μετατοπίζει την r_0 μια θέση αριστερά, και κινούμενος αριστερά, έρχεται στην αρχή της προηγούμενης λέξης σε κατάσταση q_{10} (αρχική της M_1). Δηλαδή είμαστε στη φάση:

$$s - t_{y-1} - -s - t_{y-2} - - \cdots - -q_{10}s - t_0 - r_0.$$

Η λέξη $s - t_0 - r_0$ παριστά το διάνυσμα $(\overline{x}, 0, f(\overline{x}, 0))$, συνεπώς είναι η είσοδος για τη μηχανή M_1 που αντιπροσωπεύει την h. Αν r_1 είναι η έξοδος αυτού του υπολογισμού, ξανά ο κέρσορας μετατοπίζει το r_1 μια θέση αριστερά, και έρχεται στην αρχή της προηγούμενης λέξης (αν υπάρχει) σε κατάσταση πάλι q_{10}, δηλαδή στη φάση:

$$s - t_{y-1} - -s - t_{y-2} - - \cdots - -q_{10}s - t_1 - r_1.$$

Συνεχίζοντας με τον ίδιο τρόπο θα έρθει η μηχανή στη φάση

$$q_{10}s - t_{y-1} - r_{y-1}.$$

Εκτελεί τον υπολογισμό, δίνει έξοδο r_y, ψάχνει να δει αν υπάρχει άλλη λέξη αριστερά, δεν βρίσκει και σταματά. Η τελική έξοδος του υπολογισμού είναι το r_y, που παριστά το $h(\overline{x}, y-1, f(\overline{x}, y-1)) = f(\overline{x}, y)$.

(δ) Έστω ότι η f παράγεται από την g με ελαχιστοποίηση, δηλαδή

$$f(\overline{x}) = \begin{cases} (\mu y)(g(\overline{x}, y) = 1) & \text{αν} \quad (\exists y)(g(\overline{x}, y) = 1), \\ \text{δεν ορίζεται αλλιώς,} \end{cases}$$

και ότι η g είναι Turing-υπολογίσιμη με τη μηχανή M_0. Έστω M πάλι μια μηχανή που εξομοιώνει την M_0. Έστω η λέξη s παριστά την είσοδο $\overline{x}$ της M. Η M ξεκινά με τη φάση $q_0 s$ και αφήνοντας δύο κενά δεξιά γράφει τη λέξη $s - |$ και έρχεται στο αριστερό της άκρο σε κατάσταση q_{00}, δηλαδή στη φάση:

$$s - -q_{00}s - |.$$

Εκτελεί τον υπολογισμό μιμούμενη τη μηχανή M_0. Αν η έξοδος είναι η λέξη $||$ (δηλαδή ο αριθμός 1), ο κέρσορας αφήνει μόνο τη λέξη $|$ και σταματά. Αν η έξοδος είναι $\neq ||$, σβήνει την έξοδο, γράφει δεξιά της s τη λέξη $s-||$, έρχεται στη φάση

$$s--q_{00}s-||,$$

και εκτελεί τον υπολογισμό. Αν η έξοδος είναι $||$, αφήνει μόνο τη λέξη $||$ και σταματά. Αλλιώς συνεχίζει με τον ίδιο τρόπο (πιθανόν επ΄ άπειρον). Γενικά, όταν από τη φάση

$$s--q_{00}s-\underbrace{|\cdots|}_{n+1},$$

εκτελέσει τον υπολογισμό και η έξοδος είναι $||$, γράφει τη λέξη $\underbrace{|\cdots|}_{n+1}$ και σταματά. Αλλιώς συνεχίζει με τον ίδιο τρόπο.

Η μηχανή M που συμπεριφέρεται όπως περιγράψαμε είναι η ζητούμενη. Αυτό ολοκληρώνει την σκιαγράφηση της απόδειξης. QED

Ισχύει και το αντίστροφο του προηγουμένου.

Θεώρημα 3.2.4 (Turing 1936) *Κάθε Turing- υπολογίσιμη συνάρτηση είναι αναδρομική.*

Απόδειξη. Στην παράγραφο 2.7 δείξαμε πως μπορούμε να αριθμητικοποιήσουμε τις αναδρομικές συναρτήσεις και τους υπολογισμούς που αντιστοιχούν σ' αυτές. Με ακριβώς ανάλογο τρόπο μπορούμε να αριθμητικοποιήσουμε τις ΜΤ και τους αντίστοιχους υπολογισμούς, παρ΄ όλο που οι ΜΤ δεν ορίζονται επαγωγικά όπως οι αναδρομικές συναρτήσεις. Ας θυμηθούμε ότι μια ΜΤ M είναι ένα πεπερασμένο σύνολο τετράδων q_ixyq_j, όπου τα q_i, q_j ανήκουν σ' ένα σύνολο Q_M ''καταστάσεων'', τα x, y σ' ένα σύνολο S_M ''συμβόλων'' και $Q_M \cap S_M = \emptyset$. Μπορούμε έτσι να πάρουμε δύο άπειρα (αριθμήσιμα) ξένα σύνολα Q, S και να υποθέσουμε ότι το μεν Q περιέχει τις καταστάσεις *όλων* των ΜΤ, το δε S περιέχει τα σύμβολα *όλων* των ΜΤ. Πιο συγκεκριμένα έστω $S = \{s_0, s_1, \ldots\}$, $Q = \{q_0, q_1, \ldots\}$, όπου ειδικά, $s_0 = -$, $s_1 = L$, $s_2 = R$, και $s_k = 2k$, ενώ $q_i = 2i+1$. Μια ΜΤ M κωδικοποιείται με έναν αριθμό e τέτοιον ώστε για κάποιο k, τα $(e)_1, \ldots, (e)_k$ είναι οι εντολές του προγράμματος της M, δηλαδή για κάθε κάθε $i \leq k$,η τετράδα

$$((e)_i)_1((e)_i)_2((e)_i)_3((e)_i)_4$$

είναι μια εντολή, δηλαδή $((e)_i)_1, ((e)_i)_4 \in Q$, $((e)_i)_2, ((e)_i)_3 \in S$, και τα $((e)_i)_j$ πληρούν τις συνθήκες συμβιβαστότητας που απαιτούνται για τις εντολές.

Ανάλογα μπορούμε να ορίσουμε τον κώδικα ενός (τερματισμένου) υπολογισμού, δηλαδή μιας πεπερασμένης ακολουθίας φάσεων $a_0 \to a_1 \to \ldots \to a_n$, όπου η a_0 είναι αρχική φάση, η a_{i+1} είναι διάδοχη φάση της a_i, και η a_n είναι τελική φάση. Όπως και στο θεώρημα 2.7.1, για κάθε $n \geq 1$, ορίζεται μια β.α. αναδρομική ιδιότητα $K_n(e, x_1, \ldots, x_n, y)$ που σημαίνει:

''Το y είναι κώδικας ενός υπολογισμού που πραγματοποιεί η ΜΤ με κώδικα e και είσοδο $x_1, \ldots, x_n$.''

Ορίζεται τότε η εξής β.α. αναδρομική συνάρτηση $W : \mathbb{N} \to \mathbb{N}$:

''Αν y είναι ο κώδικας ενός υπολογισμού, $W(y)$ είναι ο αριθμός που παριστά η έξοδος του υπολογισμού. Αλλιώς $W(y) = 0$.''

Έστω τώρα f μια n-μελής Turing-υπολογίσιμη συνάρτηση. Έστω M μια ΜΤ που την υπολογίζει, και έστω e ο κώδικας της M. Τότε προφανώς για κάθε $x_1, \ldots, x_n \in \mathbb{N}$,

$$f(x_1, \ldots, x_n) = W(\mu y K_n(e, x_1, \ldots, x_n, y)).$$

Συνεπώς η f είναι αναδρομική. QED.

Για περισσότερα για τις μηχανές Turing δείτε π.χ. το [8].

4 Συνέπειες της αριθμητικοποίησης: Αρίθμηση, διαγωνιοποίηση, σταθερά σημεία κλπ.

4.1 Θεωρήματα s-m-n και Rice

Μερικές από τις συνέπειες της αριθμητικοποίησης, δηλαδή της κωδικοποίησης των αναδρομικών συναρτήσεων με αριθμούς, φάνηκαν ήδη: Έχουμε τήν κομψή κανονική μορφή Kleene (§ 2.7, θεώρημα 2.7.1), που λέει ότι όλες οι n-μελείς αναδρομικές συναρτήσεις ορίζονται ομοιόμορφα με μια β.α. σχέση T_n $n+2$ θέσεων και μια β.α. αναδομική συνάρτηση U, δηλαδή για κάθε n-μελή αναδρομική f, υπάρχει $e \in \mathbb{N}$ τέτοιο ώστε, για κάθε $x_1, \ldots, x_n \in \mathbb{N}$

$$f(x_1, \ldots, x_n) = U(\mu y \; T_n(e, x_1, \ldots, x_n, y)). \tag{13}$$

Με την ίδια ιδέα αποδείξαμε πιο πριν ότι κάθε Turing -υπολογίσιμη συνάρτηση είναι αναδρομική. Στο κεφάλαιο αυτό θα δούμε μερικά από τα αποτελέσματα της διαπλοκής των δύο ρόλων των αριθμών, ως ορισμάτων από τη μια και ως κωδίκων από την άλλη. Συγκεριμένα η (13) μας δίνει τη δυνατότητα να αναφερόμαστε στην f μέσω κάποιου από τους κώδικές της e (δες παρατήρηση 2.7.2). Θυμίζουμε ότι ο e λέγεται *δείκτης* της f.

Ορισμός 4.1.1 Συμβολίζουμε με φ_e^n τη n-μελή αναδρομική συνάρτηση που έχει δείκτη e, δηλαδή

$$\varphi_e^n(x_1, \ldots, x_n) = U(\mu y\ T_n(e, x_1, \ldots, x_n, y)).$$

(Σε ορισμένα παλιότερα βιβλία χρησιμοποιείται ο συμβολισμός $\{e\}^n$ αντί για φ_e^n.)

Επίσης συμβολίζουμε με W_e^n το πεδίο ορισμού της φ_e^n.

Για $n = 1$, γράφουμε απλώς φ_e, W_e. Αλλά και όταν ο αριθμός των ορισμάτων είναι ένας δεδομένος n, συχνά γράφουμε φ_e αντί για φ_e^n.

Πρόταση 4.1.2 *Ένα σύνολο $X \subseteq \mathbb{N}^n$ είναι α.α. αν και μόνον αν υπάρχει $e \in \mathbb{N}$ τέτοιο ώστε $X = W_e^n$.*

Απόδειξη. Άμεση από την πρόταση 2.7.3. QED

Πρόταση 4.1.3 (Θεώρημα απαρίθμησης) *Για κάθε n υπάρχει (μερική) αναδρομική συνάρτηση $\Phi : \mathbb{N}^{n+1} \to \mathbb{N}$ που απαριθμεί όλες τις αναδρομικές n-μελείς συναρτήσεις, δηλαδή $\Phi(e, \overline{x}) = \varphi_e(\overline{x})$, για κάθε $\overline{x} \in \mathbb{N}^n$.*

Απόδειξη. Αρκεί να θέσουμε $\Phi(e, \overline{x}) = U(\mu y\ T_n(e, \overline{x}, y))$. Από την (13) προκύπτει ότι $\Phi(e, \overline{x}) = \varphi_e(\overline{x})$, και η Φ είναι προφανώς αναδρομική. QED

Πρόταση 4.1.4 (Θεώρημα Καθολικής Συνάρτησης) *Υπάρχει (μερική) αναδρομική συνάρτηση $\Psi : \mathbb{N}^2 \to \mathbb{N}$ που παράγει όλες τις φ_e^n (άρα όλες τις n-μελείς αναδρομικές, για κάθε n), με την εξής έννοια: Για κάθε $e, n, x_1, \ldots, x_n \in \mathbb{N}$,*

$$\Psi(e, \langle x_1, \ldots, x_n \rangle) = \varphi_e^n(x_1, \ldots, x_n).$$

Η Ψ λέγεται καθολική αναδρομική.

Απόδειξη. Αρκεί να θέσουμε

$$\Psi(x, y) = \begin{cases} z, & \text{αν ο } x \text{ είναι δείκτης μιας } n\text{-μελούς συνάρτησης } \varphi_x^n \text{ για} \\ & \text{κάποιο } n, \text{ και αν για κάποια } x_1, \ldots, x_n\ y = \langle x_1, \ldots, x_n \rangle \\ & \text{και} \quad \varphi_x^n(x_1, \ldots, x_n) = z, \\ \text{δεν ορίζεται αλλιώς.} & \end{cases}$$

Προφανώς η Ψ είναι αλγοριθμική και έχει τη ζητούμενη ιδιότητα. QED

Καθώς η παραπάνω καθολική συνάρτηση Ψ είναι αναδρομική, είναι Turing-υπολογίσιμη, και μία μηχανή M που την υπολογίζει λέγεται *καθολική μηχανή Turing*) (universal Turing machine). Η ύπαρξη τέτοιων μηχανών είχε αποδειχθεί ήδη από τον Turing. Μιά τέτοια μηχανή είναι πιο κοντά στην σημερινή έννοια του υπολογιστού, καθώς δεν εκτελεί ένα και μοναδικό πρόγραμμα, όπως οι κοινές MT, αλλά μπορεί να

τροφοδοτηθεί με οποιοδήποτε πρόγραμμα και να το εκετελέσει, δηλαδή μπορουμε να την προγραμματίσουμε.

Σε αντίθεση με την 4.1.4 έχουμε το ακόλουθο:

Πρόταση 4.1.5 *Δεν υπάρχει αναδρομική απαρίθμηση των μονομελών, ολικών αναδρομικών συναρτήσεων, δηλαδή το σύνολο* $\{x : \varphi_x$ *είναι ολική*$\}$ *δεν είναι α.α.*

Απόδειξη. Έστω ότι το $X = \{x : \varphi_x$ είναι ολική$\}$ είναι α.α. Τότε υπάρχει ολική αναδρομική σ τέτοια ώστε $X = rng(\sigma)$, δηλαδή μια f είναι ολική αν και μόνον αν $f = \varphi_{\sigma(x)}$ για κάποιο x. Θέτουμε

$$g(x) = \varphi_{\sigma(x)}(x) + 1.$$

Προφανώς η g είναι ολική αναδρομική, άρα για κάποιο e, $g = \varphi_{\sigma(e)}$. Τότε για κάθε x,

$$\varphi_{\sigma(e)}(x) = g(x) = \varphi_{\sigma(x)}(x) + 1.$$

Η τελευταία για $x = e$ δίνει $\varphi_{\sigma(e)}(e) = \varphi_{\sigma(e)}(e) + 1$, αντίφαση. QED

Ασκήσεις

4.1.1 Δείξτε ότι το σύνολο $Y = \{x : \varphi_x$ ολική και $rng(\varphi_x) \subseteq \{0, 1\}\}$ δεν είναι α.α.

[Υπόδειξη. Υποθέστε ότι $Y = rng(\sigma)$ και θέστε $g(x) = cosign(\varphi_{\sigma(x)}(x))$.]

4.1.2 Μιμούμενοι την απόδειξη της 4.1.5, θέτουμε $f(x) = \varphi_x(x) + 1$. Οδηγεί αυτό σε αντίφαση όπως προηγουμένως;

Όπως είπαμε στην παρατήρηση 2.7.2 (2), το σύνολο Ind των δεικτών αναδρομικών συναρτήσεων είναι αναδρομικό, άρα τίθεται το ερώτημα: Είναι το σύνολο

$$\mathcal{H} = \{(x, y) : y \in W_x\},$$

δηλαδή των (x, y) έτσι ώστε $\varphi_x(y) \downarrow$, καθώς επίσης και το σύνολο

$$\mathcal{K} = \{x : x \in W_x\},$$

αναδρομικά; Το ερώτημα αυτό είναι γνωστό σαν *Πρόβλημα Τερματισμού* (Halting Problem), καθώς στην ορολογία των MT, $\varphi_x(y) \downarrow$ σημαίνει ότι η μηχανή που υπολογίζει την φ_x, τερματίζει όταν λάβει είσοδο y.

Πρόταση 4.1.6 (Το Πρόβλημα Τερματισμού) *Το πρόβλημα τερματισμού έχει αρνητική απάντηση, δηλαδή τα* $\mathcal{H}$ *και* $\mathcal{K}$ *είναι α.α. αλλά όχι αναδρομικά.*

Απόδειξη. Αν φ είναι η αναδρομική συνάρτηση που απαριθμεί τις συναρτήσεις φ_x^1 σύμφωνα με την 4.1.4, τότε $\varphi(x,y) = \varphi_x(y)$ και συνεπώς $\mathcal{H} = dom(\varphi)$, άρα το $\mathcal{H}$ είναι α.α. ως πεδίο ορισμού αναδρομικής συνάρτησης. Όμοια το $\mathcal{K}$ είναι α.α ως πεδίο ορισμού της συνάρτησης $f(x) = \varphi_x(x)$. Έστω ότι το $\mathcal{H}$ είναι αναδρομικό. Τότε προφανώς και το $\mathcal{K}$ είναι αναδρομικό, άρα το συμπληρωμά του $-\mathcal{K}$ είναι α.α., συνεπώς $-\mathcal{K} = W_s$ για κάποιο δείκτη s. Τότε για κάθε x έχουμε

$$x \in W_s \iff x \in -\mathcal{K} \iff x \notin \mathcal{K} \iff x \notin W_x.$$

Για $x = s$ η προηγούμενη δίνει την αντίφαση

$$s \in W_s \iff s \notin W_s.$$

Άρα τα $\mathcal{H}$, $\mathcal{K}$ δεν είναι αναδρομικά. QED

Ένα άλλο κλασσικό αποτέλεσμα που αναφέρεται στους δείκτες είναι το λεγόμενο "Θεώρημα s-m-n" (το περίεργο όνομα προέρχεται από τη συνάρτηση s_n^m που θα δούμε παρακάτω). Η ιδέα που πραγματεύεται είναι απλή. Έστω π.χ. η διμελής συνάρτηση $\varphi_e(x,y)$ με δείκτη e. Αν σταθεροποιήσουμε το x, έστω $x = c$, θα προκύψει μια μονομελής αναδρομική συνάρτηση $\varphi_e(c,y)$, άρα για κάποιο δείκτη d, $\varphi_e(c,y) = \varphi_d(y)$. Το θεώρημα λέει ότι ο δείκτης d είναι *βασική αναδρομική συνάρτηση* των e και c, δηλαδή υπάρχει β.α. $s : \mathbb{N}^2 \to \mathbb{N}$ τέτοια ώστε για κάθε e, x, y, $\varphi_e(x,y) = \varphi_{s(e,x)}(y)$. Στη γενική του μορφή το θεώρημα έχει ως εξής:

Θεώρημα 4.1.7 (Θεώρημα s-m-n, Kleene 1938) *1) Για κάθε $m, n \in \mathbb{N}$, υπάρχει β.α. (άρα ολική) συνάρτηση $s_n^m : \mathbb{N}^{m+1} \to \mathbb{N}$, τέτοια ώστε για κάθε $e, x_1, \ldots, x_m$, $y_1, \ldots, y_n \in \mathbb{N}$,*

$$\varphi_e^{m+n}(x_1, \ldots, x_m, y_1, \ldots, y_n) = \varphi_d^n(y_1, \ldots, y_n),$$

όπου $d = s_n^m(e, x_1, \ldots, x_m)$.

2) Ειδικότερα, για κάθε $f : \mathbb{N}^{m+n} \to \mathbb{N}$, υπάρχει β.α. αναδρομική $s : \mathbb{N}^m \to \mathbb{N}$, τέτοια ώστε,

$$f(\overline{x}, y_1, \ldots, y_n) = \varphi_{s(\overline{x})}(y_1, \ldots, y_n).$$

Απόδειξη. 1) Έστω f η συνάρτηση που παράγεται από την φ_e για κάποια σταθερή τιμή των $x_1, \ldots, x_m$, δηλαδή

$$f(y_1, \ldots, y_n) = \varphi_e^{m+n}(x_1, \ldots, x_m, y_1, \ldots, y_n).$$

Γράφοντας $\overline{y} = (y_1, \ldots, y_n)$ και χρησιμοποιώντας τις σταθερές συναρτήσεις c_{x_i}, η παραπάνω γράφεται

$$f(\overline{y}) = \varphi_e^{m+n}(c_{x_1}(\overline{y}), \ldots, c_{x_m}(\overline{y}), \overline{y}).$$

Αλλά τώρα, ανατρέχοντας στην απόδειξη του 2.7.1, και συγκεκριμένα στον ορισμό του δείκτη $\lceil f \rceil$ της f, βλέπουμε ότι ο $\lceil f \rceil$ θα είναι β.α. συνάρτηση του δείκτη e της φ_e και των $x_1, \ldots, x_m$. Δηλαδή $\lceil f \rceil = s(e, x_1, \ldots, x_m)$. Η s είναι η ζητούμενη.

2) Έστω e ένας δείκτης της f, δηλαδή $f = \varphi_e$. Από το 1) πιο πάνω υπάρχει $t : \mathbb{N}^{m+1} \to \mathbb{N}$, έτσι ώστε

$$\varphi_{t(e,\overline{x})}(\overline{y}) = \varphi_e(\overline{x}, \overline{y}) = f(\overline{x}, \overline{y}).$$

Αφού ο δείκτης e είναι σταθερός αρκεί να θέσουμε $s(\overline{x}) = t(e, \overline{x})$ και έχουμε το ζητούμενο. QED

Με αφορμή την πρόταση 4.1.5 και την άσκηση 4.1.1, μπορούμε σε κάθε σύνολο αναδρομικών συναρτήσεων F να αντιστοιχίσουμε το *σύνολο δεικτών* του F, $Ind(F)$, δηλαδή το σύνολο

$$Ind(F) = \{x : \varphi_x \in F\}.$$

(Είναι εύκολο να δούμε ότι ένα σύνολο $I \subseteq \mathbb{N}$ είναι σύνολο δεικτών αν και μόνον αν για κάθε x, y, $x \in I$ καί $\varphi_x = \varphi_y \ \Rightarrow \ y \in I$.) Τί ιδιότητες έχουν τα σύνολα δεικτών; Π.χ. η 4.1.5 και η άσκηση 6.1 λένε ότι αν F είναι το σύνολο των ολικών ή τών ολικών με τιμές στο $\{0, 1\}$ συναρτήσεων, τότε το $Ind(F)$ δεν είναι α.α. Φυσικά η πιο επιθυμητή κατάσταση θα ήταν το $Ind(F)$ να είναι αναδρομικό. Όμως το παρακάτω Θεώρημα του Rice λέει ότι αυτό συμβαίνει μόνο όταν $F = \emptyset$ ή όταν $F = \mathcal{R}$.

Θεώρημα 4.1.8 (Θεώρημα του Rice, 1953) *Έστω $F \subseteq \mathcal{R}$. Το $Ind(F)$ είναι αναδρομικό αν και μόνον αν $F = \emptyset$ ή $F = \mathcal{R}$. (Ισοδύναμα: Αν $X \subseteq \mathbb{N}$, X αναδρομικό και X διάφορο των $\emptyset$ και Ind, τότε υπάρχουν x, y τέτοια ώστε $x \in X$, $y \notin X$ και $\varphi_x = \varphi_y$.)*

Απόδειξη. Αν $F = \emptyset$ ή $F = \mathcal{R}$, τότε $Ind(F) = \emptyset$ ή το $Ind(F)$ είναι το σύνολο όλων των δεικτών, το οποίο, όπως παρατηρήσαμε στην Παρατήρηση 2.7.2 (2), είναι αναδρομικό. Αντίστροφα, έστω ότι $F \neq \emptyset$ και $F \neq \mathcal{R}$. Τότε υπάρχει $f \in F$ και $g \notin F$. Ξωρίς περιορισμό της γενικότητας ας υποθέσουμε ότι οι f, g είναι μονομελείς. Ας θυμηθούμε ότι Ω είναι η συνάρτηση με πεδίο ορισμού $\emptyset$. Ας υποθέσουμε ότι $\Omega \notin F$. Ορίζουμε την συνάρτηση $h : \mathbb{N}^2 \to \mathbb{N}$ ως εξής:

$$h(x, y) = \begin{cases} f(y), & \text{αν } x \in \mathcal{K}, \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Η h είναι αλγοριθμική (άρα αναδρομική) διότι δοθέντος του ζεύγους (x, y), εφαρμόζουμε στο x τον αλγόριθμο A του $\mathcal{K}$. Αν αυτός δώσει ''ναι'', εφαρμόζουμε στο y τον αλγόριθμο B της f. Αν ο A δεν απαντήσει, η h δεν ορίζεται στο (x, y). (Το ίδιο και εάν ο A απαντήσει αλλά δεν απαντήσει ο B.) Από το θεώρημα s-m-n (2), υπάρχει ολική s τέτοια ώστε $h(x, y) = \varphi_{s(x)}(y)$. Άρα

$$\varphi_{s(x)}(y) = \begin{cases} f(y), & \text{αν } x \in \mathcal{K}, \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Αυτό σημαίνει ότι αν $x \in \mathcal{K}$, τότε $\varphi_{s(x)} = f$, και άρα $s(x) \in Ind(F)$, αφού $f \in F$. Αντίστροφα, αν $x \notin \mathcal{K}$, τότε η $\varphi_{s(x)}$ δεν ορίζεται για κανένα y, δηλαδή $\varphi_{s(x)} = \Omega$, και επειδή $\Omega \notin F$, $s(x) \notin Ind(F)$. Μ' άλλα λόγια έχουμε την ισοδυναμία:

$$x \in \mathcal{K} \iff \varphi_{s(x)} \in F \iff s(x) \in Ind(F).$$

Αυτό σημαίνει ότι $\mathcal{K} = s^{-1}(Ind(F))$, οπότε αν το $Ind(F)$ ήταν αναδρομικό, και το $\mathcal{K}$ θα ήταν αναδρομικό, πράγμα που δεν συμβαίνει.

Υποθέσαμε πιο πριν ότι $\Omega \notin F$. Αν $\Omega \in F$, τότε δουλεύουμε όπως πριν με το σύνολο $-F$ και την g στη θέση της f, και δείχνουμε ότι το σύνολο $Ind(-F)$ δεν είναι αναδρομικό. Επειδή $Ind(-F) = -Ind(F)$, έπεται ότι το $-Ind(F)$ και άρα το $Ind(F)$ δεν είναι αναδρομικό. QED

Δεδομένου ότι ο δείκτης μιας συνάρτησης παριστά ένα ''πρόγραμμα'' για τον υπολογισμό της, το θεώρημα του Rice μπορεί να ερμηνευθεί ως εξής: Δεν μπορούμε να συμπεράνουμε τις ιδιότητες της συνάρτησης από το πρόγραμμα που την υπολογίζει, ή, αντίστροφα, το σύνολο των προγραμμάτων της από τη συνάρτηση. Π.χ. αν δοθεί μία f, το σύνολο $\{x : \varphi_x = f\}$, είναι το $Ind(F)$ για $F = \{\varphi_x : \varphi_x = f\}$. Το τελευταίο είναι διάφορο του $\emptyset$ και του $\mathcal{R}$, άρα το $\{x : \varphi_x = f\}$ δεν είναι αναδρομικό. Αυτό σημαίνει ότι, δοθείσης μιας f, δεν έχουμε τρόπο (αλγόριθμο) να ελέγξουμε αν ένα τυχόν πρόγραμμα, είναι πρόγραμμα για την f. Κατά μείζονα λόγο δεν έχουμε αλγόριθμο που να αποφασίζει αν δύο προγράμματα κάνουν την ίδια ακριβώς δουλειά (δηλαδή το $\{(x, y) : \varphi_x = \varphi_y\}$ δεν είναι αναδρομικό).

4.2 Θεωρήματα Σταθερού Σημείου

Οι προτάσεις 4.1.6 και 4.1.5 είναι τυπικά αποτελέσματα της αλληλεπίδρασης δεικτών και ορισμάτων μέσω της διαγωνιοποίησης (όπου δείκτης και όρισμα συμπίπτουν. Συγκρίνετε την απόδειξη της 4.1.6 μ' εκείνην του θεωρήματος 6.4.6). Το πιο εντυπωσιακό όμως αποτέλεσμα της διαγωνιοποίησης είναι τα *Θεωρήματα Σταθερού Σημείου*[5] του Kleene (Fixed-point theorem). Πρόκειται για βαθιά θεωρήματα που η απόδειξή τους δεν είναι μια απλή διαγωνιοποίηση όπως π.χ στο πρόβλημα τερματισμού, αλλά ένα ξεχωριστό δείγμα ευρηματικότητας. Με μια λέξη, είναι μια απόδειξη που δεν θα μπορούσε να

[5]Θεωρήματα Σταθερού Σημείου υπάρχουν πολλά, σε ποικίλες περιοχές των μαθηματικών, και όλα ισχυρίζονται την ύπαρξη, κάτω από ορισμένες συνθήκες, για μια συνάρτηση f ενός σημείου x τέτοιου ώστε $f(x) = x$. Η αρχή έγινε με το κλασσικό θεώρημα του Brouwer, ότι κάθε συνεχής συνάρτηση f από το $[0, 1]$ στο $[0, 1]$ έχει ένα σταθερό σημείο. Στην προκειμένη περίπτωση δεν έχουμε ακριβώς σταθερό σημείο, αλλά την ύπαρξη για κάθε f ενός e τέτοιου ώστε $\varphi_e = \varphi_{f(e)}$, και όχι $f(e) = e$. Γι' αυτό ορισμένοι τα ονομάζουν θεωρήματα ψευδο-σταθερού σημείου.

σκεφτεί ο καθένας. Σε ορισμένα βιβλία τα ΘΣΣ λέγονται *Θεωρήματα Αναδρομής* (Recursion Theorems). Και όχι άδικα διότι εκφράζουν ίσως την σημαντικότερη πτυχή της αναδρομής: Ότι καθε αναδρομική (επαναληπτική) διαδικασία αργά ή γρήγορα οδηγείται σε μια κατάσταση ισορροπίας, δηλαδή ένα σταθερό σημείο. Αρχίζουμε με το απλό ΘΣΣ.

Θεώρημα 4.2.1 (Θεώρημα Σταθερού Σημείου, Kleene 1938) *Για κάθε $n \in \mathbb{N}$ και κάθε ολική αναδρομική $f : \mathbb{N} \to \mathbb{N}$, υπάρχει e τέτοιο ώστε τα e και $f(e)$ να είναι δείκτες της ίδιας συνάρτησης, δηλαδή $\varphi^n_e = \varphi^n_{f(e)}$, άρα και $W^n_e = W^n_{f(e)}$.*

Απόδειξη. Το βασικό τέχνασμα είναι να ''παίξει'' κανείς με δείκτες της μορφής $\varphi_i(j)$. Τέτοιοι δείκτες υπόκεινται στη διαγωνιοποίηση $\varphi_i(i)$ (πρώτη διαγωνιοποίηση). Έστω μία $f : \mathbb{N} \to \mathbb{N}$. Αν θεωρήσουμε τη σύνθεση $g(i) = f(\varphi_i(i))$, η g είναι προφανώς αναδρομική, άρα $g = \varphi_a$ για κάποιο a. Συνεπώς $g(i) = \varphi_a(i) = f(\varphi_i(i))$ για κάθε i. Ειδικά για $i = a$ παίρνουμε $\varphi_a(a) = f(\varphi_a(a))$. Θέτοντας $\varphi_a(a) = e$, παίρνουμε $f(e) = e$ (δηλαδή πραγματικά σταθερό σημείο) και κατά μείζονα λόγο $\varphi^n_e = \varphi^n_{f(e)}$. Τελειώσαμε; Όχι ακριβώς. Δεν είμαστε σίγουροι ότι η φ_a ορίζεται στο a, δηλαδή ότι το $e = \varphi_a(a)$ υπάρχει. Γι' αυτό επιστρέφουμε στους δείκτες $\varphi_i(i)$.

Για κάθε n, i ορίζεται μια αναδρομική συνάρτηση $h_i : \mathbb{N}^n \to \mathbb{N}$ ως εξής:

$$h_i(\overline{x}) = \begin{cases} \varphi^n_{\varphi_i(i)}(\overline{x}), & \text{αν το } \varphi_i(i) \text{ ορίζεται και είναι δείκτης,} \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Επειδή η $h_i(\overline{x})$ γράφεται και $h(i, \overline{x})$, από το θεώρημα s-m-n υπάρχει ολική συνάρτηση $s : \mathbb{N} \to \mathbb{N}$ τέτοια ώστε $h_i = \varphi^n_{s(i)}$. Τότε η σύνθεση fs είναι ολική και για κάποιο m, $fs = \varphi_m$. Η φ_m είναι ολική, άρα το $fs(m) = \varphi_m(m)$ ορίζεται (δεύτερη διαγωνιοποίηση). Έστω $s(m) = e$. Το e είναι σταθερό σημείο. Πράγματι από τον ορισμό της s έχουμε:

$$\varphi^n_e = \varphi^n_{s(m)} = h_m = \varphi^n_{\varphi_m(m)} = \varphi^n_{f(s(m))} = \varphi^n_{f(e)}.$$

QED

Το παραπάνω είναι το *απλό ΘΣΣ*. Συνέπειές του είναι διάφορες κατασκευές παράξενων (παθολογικών) συναρτήσεων και συνόλων.

Παραδειγματα. 1) Πάρτε τη συνάρτηση $f(x) = x + 1$. Έπεται από το ΘΣΣ ότι για κάποιο e, $\varphi_e = \varphi_{e+1}$. Όμοια υπάρχουν e τέτοια ώστε $\varphi_e = \varphi_{e^2}$, $\varphi_e = \varphi_{2^e}$, κλπ.

2) Υπάρχει e τέτοιο ώστε η συνάρτηση φ_e είναι η σταθερή συνάρτηση $f(x) = e$ για κάθε e, δηλαδή $\varphi_e = c_e$. Πράγματι, έστω η συνάρτηση $f(x, y) = x$ για κάθε x, y. Από το θεώρημα s-m-n υπάρχει ολική s τέτοια ώστε $\varphi_{s(x)}(y) = f(x, y) = x$. Αν e είναι σταθερό σημείο της s, τότε $\varphi_e = \varphi_{s(e)}$ και για κάθε x,

$$\varphi_e(x) = \varphi_{s(e)}(x) = f(e, x) = e.$$

3) Υπάρχει e, τέτοιο ώστε $W_e = \{e\}$. Πράγματι, η συνάρτηση

$$f(x,y) = \begin{cases} 0, & \text{αν } x = y, \\ \text{δεν ορίζεται αλλιώς,} \end{cases}$$

είναι αναδρομική και από το θεώρημα s-m-n υπάρχει ολική s τέτοια ώστε $\varphi_{s(x)}(y) = f(x,y)$. Έστω e σταθερό σημείο της s. Είναι εύκολο να δούμε ότι $W_e = \{e\}$. Πράγματι, $\varphi_e(e) = \varphi_{s(e)}(e) = f(e,e) = 0$, συνεπώς $e \in W_e$. Αν τώρα $x \neq e$, έχουμε $\varphi_e(x) = \varphi_{s(e)}(x) = f(e,x)$, το οποίο δεν ορίζεται, άρα $x \notin W_e$. Συνεπώς $W_e = \{e\}$.

Όμως πολύ πιο ισχυρό είναι το *ΘΣΣ με παραμέτρους*, όπου το σταθερό σημείο δεν είναι ένας αριθμός αλλά μια συνάρτηση:

Θεώρημα 4.2.2 (Θεώρημα Σταθερού Σημείου με Παραμέτρους) *Για κάθε ολική αναδρομική $f : \mathbb{N}^{n+1} \to \mathbb{N}$, υπάρχει ολική αναδρομική $h : \mathbb{N}^n \to \mathbb{N}$, τέτοια ώστε για κάθε $\overline{x} = (x_1, \ldots, x_n)$,*

$$\varphi_{h(\overline{x})} = \varphi_{f(\overline{x},h(\overline{x}))}.$$

Απόδειξη. Όπως και στο απλό ΘΣΣ, υπάρχει ολική $s : \mathbb{N}^{n+1} \to \mathbb{N}$ τέτοια ώστε

$$\varphi_{s(i,\overline{x})}(y) = \begin{cases} \varphi_{\varphi_i(i,\overline{x})}(y), & \text{αν το } \varphi_i(i,\overline{x}) \text{ ορίζεται και είναι δείκτης,} \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Δοθείσης της f, έστω m δείκτης της συνάρτησης $f(\overline{x}, s(i,\overline{x}))$, δηλαδή

$$\varphi_m(i,\overline{x}) = f(\overline{x}, s(i,\overline{x})).$$

Η φ_m είναι ολική. Ενώ πριν το σταθερό σημείο ήταν ο αριθμός $s(m) = e$, τώρα το σταθερό σημείο είναι η συνάρτηση $s(m,\overline{x})$. Πράγματι, από τον πιο πάνω ορισμό έχουμε

$$\varphi_{s(m,\overline{x})} = \varphi_{\varphi_{m(m,\overline{x})}} = \varphi_{f(\overline{x},s(m,\overline{x}))}.$$

Θέτοντας $h(\overline{x}) = s(m,\overline{x})$, η h είναι ολική αναδρομική και έχουμε

$$\varphi_{h(\overline{x})} = \varphi_{s(m,\overline{x})} = \varphi_{f(\overline{x},s(m,\overline{x}))} = \varphi_{f(\overline{x},h(\overline{x}))}.$$

QED

Τώρα μπορούμε να δούμε ότι οι συναρτήσεις που ορίζονται από τα σχήματα βασικής αναδρομής και ελαχιστοποίησης, είναι στην ουσία σταθερά σημεία κάποιας αναδρομικής συνάρτησης.

Πρόταση 4.2.3 *Αν η f ορίζεται με το σχήμα βασικής αναδρομής ή με ελαχιστοποίηση, τότε είναι σταθερό σημείο μιας αναδρομής. Συγκεκριμένα:*

1) Αν η $f : \mathbb{N}^{k+1} \to \mathbb{N}$ παράγεται με βασική αναδρομή, υπάρχει $\rho : \mathbb{N}^k \to \mathbb{N}$ τέτοια ώστε $f(\overline{x}, y) = \varphi_{\rho(\overline{x})}(y)$ και $\phi_{\rho(\overline{x})} = \phi_{s(\overline{x},\rho(\overline{x}))}$ για κάποια s.

2) Αν η $f : \mathbb{N}^k \to \mathbb{N}$ παράγεται με ελαχιστοποίηση, τότε $f(\overline{x}) = \varphi_e(0,\overline{x})$, και το e είναι σταθερό σημείο μιας συνάρτησης s.

Απόδειξη. 1) Έστω ότι η $f : \mathbb{N}^{k+1} \to \mathbb{N}$ ορίζεται από τις g, h με βασική αναδρομή, δηλαδή:

$f(\overline{x}, 0) = g(\overline{x})$,

$f(\overline{x}, y+1) = h(\overline{x}, y, f(\overline{x}, y))$.

Θεωρούμε τη συνάρτηση $F : \mathbb{N}^{k+2} \to \mathbb{N}$ που ορίζεται ως εξής:

$$F(\overline{x}, i, y) = \begin{cases} g(\overline{x}), & \text{αν } y = 0, \\ h(\overline{x}, y-1, F(\overline{x}, i, y-1)), & \text{αλλιώς.} \end{cases}$$

Από το θεώρημα s-m-n, υπάρχει ολική συνάρτηση $s : \mathbb{N}^{k+1} \to \mathbb{N}$ τέτοια ώστε

$$F(\overline{x}, i, y) = \varphi_{s(\overline{x},i)}(y).$$

Από το ΘΣΣ με παραμέτρους, υπάρχει συνάρτηση $\rho : \mathbb{N}^k \to \mathbb{N}$, που είναι σταθερό σημείο της s, δηλαδή

$$\varphi_{\rho(\overline{x})} = \varphi_{s(\overline{x},\rho(\overline{x}))}.$$

Ισχυρίζομαι ότι για κάθε $\overline{x}$, y,

$$\varphi_{\rho(\overline{x})}(y) = f(\overline{x}, y). \tag{14}$$

Δείχνουμε την (14) με επαγωγή στο y.

(α) Για $y = 0$, έχουμε:

$$\varphi_{\rho(\overline{x})}(0) = \varphi_{s(\overline{x},\rho(\overline{x}))}(0) = F(\overline{x}, \rho(\overline{x}), 0) = g(\overline{x}) = f(\overline{x}, 0).$$

(β) Έστω ισχύει για y, δηλαδή η (14) ισχύει. Αρκεί να δείξουμε ότι

$$\varphi_{\rho(\overline{x})}(y+1) = f(\overline{x}, y+1).$$

Έχουμε:

$$\varphi_{\rho(\overline{x})}(y+1) = \varphi_{s(\overline{x},\rho(\overline{x}))}(y+1) = F(\overline{x}, \rho(\overline{x}), y+1) = h(\overline{x}, y, F(\overline{x}, \rho(\overline{x}), y)) =$$

$$h(\overline{x}, y, \varphi_{s(\overline{x},\rho(\overline{x}))}(y)) = h(\overline{x}, y, \varphi_{\rho(\overline{x})}(y)).$$

Από την υπόθεση της επαγωγής όμως $\varphi_{\rho(\overline{x})}(y) = f(\overline{x}, y)$, άρα το τελευταίο μέλος των παραπάνω ισοτήτων ισούται με $h(\overline{x}, y, f(\overline{x}, y)) = f(\overline{x}, y+1)$, δηλαδή το ζητούμενο.

2) Έστω τώρα ότι η $f : \mathbb{N}^k \to \mathbb{N}$ παράγεται με ελαχιστοποίηση από την g, δηλαδή

$f(\overline{x}) = (\mu y)(g(\overline{x}, y) = 1)$.

Θεωρούμε τη συνάρτηση $F : \mathbb{N}^{k+1} \to \mathbb{N}$ που ορίζεται ως εξής:

$$F(i, y, \overline{x}) = \begin{cases} y, & \text{αν } g(\overline{x}, y) = 1, \\ F(i, y+1, \overline{x}), & \text{αλλιώς.} \end{cases}$$

Είναι εύκολο να επαληθεύσει κανείς ότι για κάθε i, $F(i, 0, \overline{x}) = f(\overline{x})$. Πράγματι, η F, για δοθέν $\overline{x}$, για κάθε i, και ξεκινώντας με $y = 0$, πυροδοτεί μια αναζήτηση ενός

y τέτοιου ώστε $g(\overline{x}, y) = 1$. Αν δεν υπάρχει τέτοιο y για το δοθέν $\overline{x}$, το $F(i, 0, \overline{x})$ δεν ορίζεται, όπως συμβαίνει και με το $f(\overline{x})$. Αν υπάρχει, τότε το $F(i, 0, \overline{x})$ θα είναι προφανώς το ελάχιστο μ' αυτή την ιδιότητα, άρα και πάλι ισούται με $f(\overline{x})$. Τώρα το όρισμα i στην F, μπήκε μόνο για να μας βοηθήσει να πάρουμε την F σαν σταθερό σημείο. Πράγματι από το s-m-n, υπάρχει s τέτοια ώστε

$$\varphi_{s(i)}(y, \overline{x}) = F(i, y, \overline{x}).$$

Αν e είναι σταθερό σημείο για την s (εδώ χρησιμοποιούμε το απλό ΘΣΣ), θα έχουμε $\varphi_e(y, \overline{x}) = F(e, y, \overline{x})$, άρα $f(\overline{x}) = \varphi_e(0, \overline{x})$. QED

Πρίν κλείσουμε αυτή την παράγραφο θα δώσουμε μια εφαρμογή του s-m-n στο πρόβλημα της *σχετικής αναδρομικότητας* και των *Turing βαθμών* (Turing degrees). Πέρα από τις (απολύτως) αναδρομικές συναρτήσεις και σύνολα, έχουμε τις αντίστοιχες σχετικοποιημένες έννοιες. Π.χ. αν g είναι μια οποιαδήποτε συνάρτηση και $f(x) = g(x) + x^2$, η f δεν είναι κατ' ανάγκη αναδρομική, αλλά είναι *αναδρομική ως προς την* g, δηλαδή παράγεται από την g, και τις αναδρομικές συναρτήσεις $+$ και $\cdot$, με σύνθεση. Γενικότερα έχουμε τον εξής

Ορισμός 4.2.4 Έστω g μια ολική συνάρτηση. Η κλάση των *αναδρομικών ως προς* g *συναρτήσεων,* $\mathcal{R}(g)$, είναι η ελάχιστη κλάση C τέτοια ώστε:

(i) Η C περιέχει την g και τις αρχικές συναρτήσεις.

(ii) Η C είναι κλειστή ως προς βασική αναδρομή, σύνθεση και ελαχιστοποίηση.

Λέμε ότι η f είναι *Turing αναγώγιμη στην* g (Turing reducible in g), και συμβολίζουμε $f \leq_T g$, αν $f \in \mathcal{R}(g)$.

Όμοια, για δύο σύνολα X, Y γράφουμε $X \leq_T Y$ αν $C_X \leq_T C_Y$.

Μιά είδική περίπτωση Turing αναγωγιμότητας είναι η εξής:

Ορισμός 4.2.5 Έστω X, Y δύο σύνολα. Το X λέγεται *m-αναγώγιμο στο* Y, και γράφουμε $X \leq_m Y$, αν υπάρχει ολική αναδρομική f τέτοια ώστε

$$\forall x(x \in X \iff f(x) \in Y).$$

Είναι εύκολο να δούμε ότι

$$X \leq_m Y \Rightarrow X \leq_T Y. \tag{15}$$

Πράγματι, $X \leq_m Y$ συνεπάγεται ότι $C_X(x) = 1 \iff C_Y(f(x)) = 1$, άρα $C_X = C_Y \circ f$, και συνεπώς $C_X \in \mathcal{R}(C_Y)$ (αφού η f είναι αναδρομική), δηλαδή $X \leq_T Y$.

Επίσης, αν $X \leq_T Y$ και το Y είναι α.α., και το X θα είναι α.α.

Ορισμός 4.2.6 Ένα σύνολο X λέγεται *α.α.-πλήρες* (r.e.-complete ή Turing complete), αν είναι α.α. και για κάθε α.α. σύνολο Y, $Y \leq_T X$.

Θεώρημα 4.2.7 (Post 1944) *Το σύνολο* $\mathcal{K} = \{x : x \in W_x\}$ *είναι α.α.-πλήρες.*

Απόδειξη. Λόγω της (15), αρκεί να δείξουμε ότι για κάθε α.α. σύνολο X, $X \leq_m \mathcal{K}$, δηλαδή ότι υπάρχει f τέτοια ώστε για κάθε x,

$$x \in X \iff f(x) \in \mathcal{K} \iff f(x) \in W_{f(x)}.$$

Έστω X ένα α.α. σύνολο. Θεωρούμε τη συνάρτηση

$$h(x,y) = \begin{cases} y, & \text{αν } x \in X, \\ \text{δεν ορίζεται αλλιώς.} \end{cases}$$

Από το θεώρημα s-m-n υπάρχει ολική f τέτοια ώστε $\varphi_{f(x)}(y) = h(x,y)$. Από τόν ορισμό, για $x \in X$, $\varphi_{f(x)}(y) = y$ για κάθε y, δηλαδή $\varphi_{f(x)} = id$, άρα $W_{f(x)} = \mathbb{N}$. Επίσης για $x \notin X$, $\varphi_{f(x)}(y) \uparrow$ για κάθε y, δηλαδή $\varphi_{f(x)} = \Omega$, άρα $W_{f(x)} = \emptyset$. Άρα αφ' ενός

$$x \in X \;\Rightarrow\; W_{f(x)} = \mathbb{N} \;\Rightarrow\; f(x) \in W_{f(x)} \Rightarrow\; f(x) \in \mathcal{K},$$

και αφ' ετέρου,

$$x \notin X \;\Rightarrow\; \forall y\; \varphi_{f(x)}(y) \uparrow \Rightarrow W_{f(x)} = \emptyset \Rightarrow f(x) \notin W_{f(x)} \;\Rightarrow f(x) \notin \mathcal{K}.$$

Άρα $x \in X \iff f(x) \in \mathcal{K}$, και συνεπώς η f είναι η ζητούμενη. QED

5 Στοιχεία από τη Μαθηματική Λογική. Λογικός χαρακτηρισμός των αναδρομικών και α.α. συνόλων

Όπως είναι γνωστό ''Αριθμητική'' είναι η θεωρία των φυσικών αριθμών (ή μηαρνητικών ακεραίων), δηλαδή το σύνολο των προτάσεων που αληθεύουν στο $\mathbb{N} = \{0, 1, 2, \ldots\}$ και αφορούν τις πράξεις $+$, $\cdot$, και τις σχέσεις $<$ και $=$. Υπάρχει και μία ακόμη πράξη, που συνήθως την παραβλέπουμε γιατί τη θεωρούμε μέρος της πρόσθεσης, η πράξη της διαδοχής $S(x) = x + 1$, με την οποία παράγονται από το 0 οι υπόλοιποι φυσικοί, καθώς $1 = S(0)$, $2 = S(1) = SS(0)$, κλπ. Έτσι όλες οι ιδιότητες που αφορούν τα στοιχεία του $\mathbb{N}$, εκφράζονται μέσω των συμβόλων $+$, $\cdot$, S, $<$, $=$, συν κάποια άλλα standard λογικά σύμβολα που θα εισάγουμε παρακάτω. Στην καθημερινή πρακτική δεν νοιαζόμαστε και πολύ για τη μορφή που έχουν οι προτάσεις μας όταν γραφούν με αυστηρό τρόπο στην παραπάνω γλώσσα. Όμως θα δούμε ότι η *λογική μορφή* μιας ιδιότητας έχει άμεσο αντίχτυπο στην πολυπλοκότητα του συνόλου που ορίζεται από την ιδιότητα αυτή, δηλαδή στην αναδρομικότητα ή μη του συνόλου. Σκοπός μας στα επόμενα είναι να δώσουμε μια *λογική*, δηλαδή *συντακτική*, περιγραφή των αναδρομικών και α.α. υποσυνόλων του $\mathbb{N}$.

5.1 Γλώσσα της Αριθμητικής, λογισμός και ερμηνεία των προτάσεων και τύπων

Η γλώσσα (αλφάβητο) της Αριθμητικής είναι το σύνολο των συμβόλων

$$L_A = \{+, \cdot, \underline{0}, <, =\} \cup \{\wedge, \vee, \rightarrow, \leftrightarrow, \neg, \exists, \forall, (,), x_1, x_2, \ldots\}.$$

Το πρώτο σύνολο στην παραπάνω ένωση περιέχει τα *μαθηματικά σύμβολα*. Τα αντικείμενα αυτά, ως σύμβολα, είναι διαφορετικά από τα αντικείμενα που πρόκειται να συμβολίσουν, γι' αυτό και παριστάνουμε με $\underline{0}$ το *σύμβολο του μηδενός*, ώστε να το διακρίνουμε από το ίδιο το 0 που είναι ένα στοιχείο του $\mathbb{N}$. Το ίδιο θα έπρεπε να κάνουμε και με τα υπόλοιπα σύμβολα $+, \cdot$ κλπ, αλλά αυτό θα δημιουργούσε τυπογραφικό πρόβλημα, γι' αυτό περιοριζόμαστε να επισημάνουμε αυτή τη διάκριση. Έτσι άλλες φορές το $+$ θα παριστάνει το σύμβολο της πρόσθεσης και άλλοτε την συγκεκριμένη πράξη στο $\mathbb{N}$.

Το δεύτερο σύνολο περιέχει τα *λογικά σύμβολα*. Τα τελευταία είναι κοινά σ' όλες τις μαθηματικές γλώσσες και το όνομα και η σημασία τους είναι λίγο πολύ γνωστή. Συγκεκριμένα:

1) $\wedge$: Λέγεται *σύξευξη* και σημαίνει ''καί''.
2) $\vee$: Λέγεται *διάζευξη* και σημαίνει ''ή''.
3) $\rightarrow$: Λέγεται *συνεπαγωγή* και σημαίνει ''αν τότε''.
4) $\leftrightarrow$: Λέγεται *ισοδυναμία* και σημαίνει ''άν και μόνον αν''.
5) $\neg$: Λέγεται *άρνηση* και σημαίνει ''όχι''.
6) $(,)$: Παρενθέσεις (βοηθητικά αλλά απαραίτητα σύμβολα).
7) $x_1, x_2, \ldots$: Λέγονται *μεταβλητές* και το πλήθος τους είναι άπειρο. (Στην πράξη χρησιμοποιούμε για απλότητα και ''άτυπες '' μεταβλητές x, y, z κλπ.)

Με το παραπάνω αλφάβητο φτιάχνουμε *όρους* (terms) και *τύπους* (formulas). Μέρος των τύπων είναι οι *προτάσεις*.

Ορισμός 5.1.1 Το σύνολο $T(L_A)$ των *όρων* (terms) της L_A είναι το μικρότερο σύνολο X με τις ιδιότητες:
(α) $\underline{0} \in X$,
(β) $x_i \in X$ για κάθε μεταβλητή x_i,
(γ) Αν $t, s \in X$ τότε $t + s \in X$, $t \cdot s \in X$ και $S(t) \in X$.

Π.χ. τα

$$S(x) + S(y \cdot S(\underline{0})),$$
$$x^2 + y^3,$$

(όπου $x^2 = x \cdot x$, $x^3 = (x \cdot x) \cdot x$, κλπ),

$$s^{k_n}(\underline{0}) \cdot x^n + s^{k_{n-1}}(\underline{0}) \cdot x^{n-1} + \cdots s^{k_1}(\underline{0}) \cdot x + s^{k_0}(\underline{0}),$$

(όπου $S^n(x) = \underbrace{S\cdots S}_{n\ \varphi o\rho\acute{\varepsilon}\varsigma}(x)$), είναι όροι. Όροι χωρίς μεταβλητές λέγονται *κλειστοί*.

Αφού το $\underline{0}$ συμβολίζει το 0, οι όροι $S(\underline{0})$, $S^2(\underline{0}), \ldots S^n(\underline{0})$, θα συμβολίζουν τους ακεραίους $1, 2, \ldots, n, \ldots$ αντίστοιχα, γι' αυτό, για λόγους ομοιομορφίας με ότι αρχίσαμε με το μηδέν, θέτουμε για κάθε $n \in \mathbb{N}$,

$$S^n(\underline{0}) := \underline{n}.$$

Ορισμός 5.1.2 Το σύνολο $F(L_A)$ των *τύπων* (formulas) της L_A είναι το μικρότερο σύνολο X με τις ιδιότητες:

(α) Για όλους τους όρους t, s, οι $t = s$ και $t < s$ ανήκουν στο X.

(β) Αν $\phi, \psi \in X$, τότε οι $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \to \psi$, $\phi \leftrightarrow \psi$, και $\neg\phi$ ανήκουν στο X.

(γ) Αν $\phi \in X$ και x μεταβλητή, τότε οι $(\exists x)\phi$, $(\forall x)\phi$ ανήκουν στο X.

Κάθε ιδιότητα και ισχυρισμός που αφορά τους φυσικούς αριθμούς εκφράζετται με έναν τύπο της γλώσσας.

Παραδειγματα.

(1) ''Ο x διαιρεί τον y'' γράφεται:

$$(\exists z)(y = x \cdot z).$$

[Φυσικά θα συνεχίσουμε να χρησιμοποιούμε τις γνωστές συντομογραφίες, π.χ. $x|y$ για τη διαιρετότητα, αλλά ξέροντας ότι είναι μόνο *συντομογραφίες* και όχι η πραγματική γλώσσα των αριθμών.]

(2) ''Ο x είναι άρτιος '' γράφεται:

$$(\exists y)(x = \underline{2} \cdot y).$$

(3) ''Ο x είναι πρώτος '' γράφεται:

$$(\forall y)(y|x \ \to \ y = x \vee y = \underline{1}).$$

(4) ''Υπάρχουν άπειροι πρώτοι'' γράφεται:

$$(\forall x)(\exists y)(x < y \ \wedge \ P(y)),$$

όπου $P(x)$ είναι ο τύπος ''ο x είναι πρώτος '' που είδαμε προηγουμένως.

(5) ''$x \equiv y (\mathrm{mod} z)$'' γράφεται:

$$(\exists u)(x = y + u \cdot z \ \vee \ y = x + u \cdot z)$$

(επειδή $x \equiv y(\mathrm{mod} z)$ σημαίνει ότι ο z διαιρεί τον $|x-y|$, και $|x-y| = x-y$ ή $y-x$).

(6) Ακόμα και η σχέση διάταξης $<$ μπορεί να εκφρασθεί μέσω των υπολοίπων συμβόλων της γλώσσας καθώς η $x < y$ ισοδυναμεί με

$$(\exists z)(y = x + S(z)).$$

Ορισμός 5.1.3 Έστω ϕ ένας τύπος και x μια μεταβλητή του ϕ. Η x μπορεί να εμφανίζεται σε διάφορες θέσεις μέσα στον ϕ, γι' αυτό μιλάμε για *εμφανίσεις της x στον ϕ*. Μία εμφάνιση της x λέγεται *δεσμευμένη* αν είναι της μορφής $(\forall x)(\cdots x \cdots)$ ή $(\exists x)(\cdots x \cdots)$. Κάθε άλλη εμφάνιση λέγεται *ελεύθερη*. Η x λέγεται *ελεύθερη μεταβλητή του ϕ* αν έχει μία τουλάχιστον ελεύθερη εμφάνιση στον ϕ. Αλλιώς λέγεται *δεσμευμένη μεταβλητή του ϕ*. Ο ϕ λέγεται *πρόταση* (sentence) αν δεν έχει ελεύθερες μεταβλητές.

Το σύνολο των προτάσεων της L_A το συμβολίζουμε $S(L_A)$. Ο συμβολισμός $\phi(x_1, \ldots, x_n)$, ή $\phi(\overline{x})$, σημαίνει ότι οι ελεύθερες μεταβλητές του ϕ είναι μεταξύ των $x_1, \ldots, x_n$. Ο $\phi(x_1, \ldots, x_n)$, για $n > 1$, εκφράζει μια *n-μελή σχέση* μεταξύ αριθμών. Για $n = 1$, εκφράζει μια *ιδιότητα*. Π.χ. στα πιο πάνω παραδείγματα, στο (1) ο τύπος $\phi(x, y) := (\exists z)(y = x \cdot z)$ (με ελεύθερες μεταβλητές τις x, y) εκφράζει τη διμελή σχέση $x|y$, στο (2) και (3) έχουμε τις ιδιότητες $A(x)$:="x άρτιος" και $P(x)$:="x πρώτος" αντίστοιχα, στο (4) έχουμε μια πρόταση, στο (5) έχουμε μια τριμελή σχέση $\psi(x, y, z) := x \equiv y(\mathrm{mod} z)$, και στο (6) έχουμε επίσης τη διμελή σχέση $x < y := (\exists z)(y = x + S(z))$.

Συχνά οι τύποι $(\forall x_1) \ldots (\forall x_n)\phi(x_1, \ldots, x_n)$ και $(\exists x_1) \ldots (\exists x_n)\phi(x_1, \ldots, x_n)$ συντομογραφούνται ως $(\forall \overline{x})\phi(\overline{x})$ και $(\exists \overline{x})\phi(\overline{x})$ αντίστοιχα.

Αν $\phi(x_1, \ldots, x_n)$ είναι ένας τύπος και οι $t_1, \ldots, t_n$ είναι όροι της L_A, τότε με $\phi(t_1, \ldots, t_n)$ παριστάνουμε τον τύπο που προκύπτει από την αντικατάσταση κάθε ελεύθερης μεταβλητής x_i (όπου αυτή εμφανίζεται) από τον όρο t_i.

Τα παραπάνω αφορούν την σύνταξη της γλώσσας L_A. Ερχόμαστε στην *ερμηνεία* των προτάσεων μέσα στη δομή

$$\mathbb{N} = (\mathbb{N}, +^{\mathbb{N}}, .^{\mathbb{N}}, S^{\mathbb{N}}, <^{\mathbb{N}}, 0).$$

Τα $+^{\mathbb{N}}, .^{\mathbb{N}}, S^{\mathbb{N}}, <^{\mathbb{N}}$ είναι η πρόσθεση, ο πολ/σμός, η διαδοχή και η διάταξη του $\mathbb{N}$, τα οποία πρέπει να τα διακρίνουμε από τα απλά σύμβολα $+, \cdot, S, <$ της γλώσσας. Όμως όπως είδη ειπώθηκε, για απλοποίηση του συμβολισμού δεν θα χρησιμοποιούμε τους άνω δείκτες και θα γράφουμε απλώς

$$\mathbb{N} = (\mathbb{N}, +, \cdot, S, <, 0).$$

Το ότι ακόμη συμβολίζουμε με το ίδιο σύμβολο $\mathbb{N}$, τόσο το απλό σύνολο των φυσικών όσο και την δομή επ' αυτού, γίνεται επίσης για λόγους απλότητας.

Ορισμός 5.1.4 Για κάθε κλειστό όρο $t \in T(L_A)$, η *ερμηνεία του* μέσα στο $\mathbb{N}$ είναι ένα στοιχείο $t^{\mathbb{N}}$ του $\mathbb{N}$ που ορίζεται επαγωγικά ως εξής:

(α) $\underline{0}^{\mathbb{N}} = 0$.

(β) $(t+s)^{\mathbb{N}} = t^{\mathbb{N}} + s^{\mathbb{N}}$, $(t \cdot s)^{\mathbb{N}} = t^{\mathbb{N}} \cdot s^{\mathbb{N}}$, $(S(t))^{\mathbb{N}} = S(t^{\mathbb{N}}) = t^{\mathbb{N}} + 1$.

Εύκολα βλέπουμε ότι για κάθε $n \in \mathbb{N}$, $\underline{n}^{\mathbb{N}} = n$. Εν συνεχεία ορίζουμε τι σημαίνει *μία πρόταση ϕ της L_A να είναι αληθής στο* $\mathbb{N}$ (συμβολισμός $\mathbb{N} \models \phi$).

Ορισμός 5.1.5 Για κάθε $\phi \in S(L_A)$ η σχέση $\mathbb{N} \models \phi$ ορίζεται επαγωγικά ως εξής (στα (α), (β) παρακάτω οι όροι t, s είναι κατ' ανάγκη κλειστοί):

(α) $\mathbb{N} \models t = s$ αν $t^{\mathbb{N}} = s^{\mathbb{N}}$.

(β) $\mathbb{N} \models t < s$ αν $t^{\mathbb{N}} < s^{\mathbb{N}}$.

(γ) $\mathbb{N} \models \phi \wedge \psi$ αν $\mathbb{N} \models \phi$ και $\mathbb{N} \models \psi$.

(δ) $\mathbb{N} \models \phi \vee \psi$ αν $\mathbb{N} \models \phi$ ή $\mathbb{N} \models \psi$.

(ε) $\mathbb{N} \models \phi \to \psi$ αν $\mathbb{N} \models \phi \ \Rightarrow \ \mathbb{N} \models \psi$.

(ζ) $\mathbb{N} \models \phi \leftrightarrow \psi$ αν $\mathbb{N} \models \phi \ \Leftrightarrow \ \mathbb{N} \models \psi$.

(η) $\mathbb{N} \models \neg\phi$ αν $\mathbb{N} \not\models \phi$.

(ϑ) $\mathbb{N} \models (\forall x)\phi(x)$ αν $\mathbb{N} \models \phi(\underline{n})$ για κάθε $n \in \mathbb{N}$.

(ι) $\mathbb{N} \models (\exists x)\phi(x)$ αν $\mathbb{N} \models \phi(\underline{n})$ για κάποιο $n \in \mathbb{N}$.

Αν $\phi(x_1, \ldots, x_n)$ είναι τύπος με ελεύθερες μεταβλητές x_i, εξ ορισμού

$$\mathbb{N} \models \phi(x_1, \ldots, x_n) \iff \mathbb{N} \models (\forall x_1) \ldots (\forall x_n)\phi(x_1, \ldots, x_n).$$

Έπεται από τον πιο πάνω ορισμό ότι για κάθε $\phi \in S(L_A)$, ακριβώς μια από τις ϕ και $\neg\phi$ αληθεύει στη $\mathbb{N}$. (Ενώ δεν ισχύει αυτό για ϕ με ελεύθυερες μεταβλητές.) Το σύνολο

$$Th(\mathbb{N}) = \{\phi \in S(L_A) : \mathbb{N} \models \phi\}$$

δηλαδή το σύνολο των αληθειών του $\mathbb{N}$, λέγεται *Πλήρης Αριθμητική* (Complete Arithmetic) και στην πράξη είναι το αντικείμενο του κλάδου που λέγεται Θεωρία Αριθμών. Θα δούμε λίγο αργότερα ότι υπάρχει και η Τυπική Αριθμητική (Formal Arithmetic), που είναι ασθενέστερη θεωρία. Για την ώρα θα ασχοληθούμε με την $Th(\mathbb{N})$.

Όπως ειπώθηκε, κάθε τύπος $\phi(x_1, \ldots, x_k)$, με ελεύθερες μεταβλητές x_i, $i \leq k$, εκφράζει μία k-μελή σχέση στη γλώσσα. Αυτόματα ορίζει μία k-μελή σχέση στο $\mathbb{N}$, R_ϕ, ως εξής:

$$R_\phi = \{(n_1, \ldots, n_k) \in \mathbb{N}^k : \mathbb{N} \models \phi(\underline{n_1}, \ldots, \underline{n_k})\}.$$

Λέμε τότε ότι το R_ϕ *ορίζεται* με τον τύπο ϕ. Ακριβέστερα:

Ορισμός 5.1.6 Ένα σύνολο $X \subseteq \mathbb{N}^k$ λέγεται *ορίσιμο* (definable) αν $X = R_\phi$ για κάποιο ϕ, δηλαδή αν για κάθε $n_1, \ldots, n_k \in \mathbb{N}$,

$$(n_1, \ldots, n_k) \in X \iff \mathbb{N} \models \phi(\underline{n_1}, \ldots, \underline{n_k}).$$

Για κάθε $k > 0$, έστω

$$Def_k(\mathbb{N}) = \{X \subseteq N^k : \text{ υπάρχει } \phi(\overline{x}) : X = R_\phi\}.$$

Η κλάση των ορίσιμων συνόλων του $\mathbb{N}$ είναι το σύνολο

$$Def(\mathbb{N}) = \bigcup_{k>0} Def_k(\mathbb{N}).$$

Η παρακάτω είναι μια απλή άσκηση:

Πρόταση 5.1.7 *Το $Def(\mathbb{N})$ είναι αριθμήσιμο σύνολο. Για κάθε $k > 0$, το $Def_k(\mathbb{N})$ είναι μια άλγεβρα Boole.*

Τα ορίσιμα σύνολα αποτελούν τη σημαντικότερη κλάση συνόλων στο $\mathbb{N}^{<\omega}$. Το $Def(\mathbb{N})$ είναι το σύμπαν των συνόλων για τα οποία μπορούμε να ''μιλήσουμε'' στη γλώσσα L_A. Τα υπόλοιπα, αν και πολύ περισσότερα, είναι πέραν του βελησκούς της γλώσσας μας άρα και της γνωστικής μας δυνατότητας. Αλλά και τα σύνολα του $Def(\mathbb{N})$, μόνον ''κατ' αρχήν'' (in principle) είναι οικεία, αφού οι ορισμοί τους στη γλώσσα L_A μπορεί να είναι εξαιρετικά πολύπλοκοι. Γι' αυτό καλό είναι να τα ιεραρχήσουμε ανάλογα με την λογική πολυπλοκότητα του τύπου που τα ορίζει. Για λόγους που θα γίνουν κατανοητοί παρακάτω, η λογική πολυπλοκότητα ενός τύπου είναι συνάρτηση αποκλειστικά του *αριθμού* και των *εναλλαγών* των ποσοδεικτών που περιέχει, δηλαδή του πόσο μεγάλες ακολουθίες της μορφής $\exists\forall\exists\forall\cdots$ ή $\forall\exists\forall\exists\cdots$ εμφανίζονται στον τύπο. Οι σύνδεσμοι δεν θεωρούμε ότι επηρεάζουν την πολυπλοκότητα, και έναν τύπο χωρίς ποσοδείκτες, όσο μεγάλο αριθμό συνδέσμων και να περιέχει, τον κατατάσσουμε στο κατώτερο σκαλοπάτι της πολυπλοκότητας. Αλλά και για τους ποσοδείκτες, μόνον οι *μη φραγμένοι* θεωρούμε ότι συμβάλλουν στην πολυπλοκότητα. (Θυμηθείτε την φραγμένη αναζήτηση που οδηγεί από (βασικά) αναδρομικά σε (βασικά) αναδρομικά σύνολα, ενώ η μηφραγμένη αναζήτηση οδηγεί από αναδρομικά σε α.α. σύνολα. Δές πρόταση 2.6.4 και § 2.2 παράδειγμα (14).) Τα παραπάνω οδηγούν στην παρακάτω ιεράρχηση.

Ορισμός 5.1.8 Οι ποσοδείκτες $(\forall x)(\cdots)$, $(\exists x)(\cdots)$ λέγονται *φραγμένοι* αν είναι της μορφής $(\forall x)(x < y \ \rightarrow \psi)$ και $(\exists x)(x < y \ \wedge \psi)$, αντίστοιχα. Για συντομία οι παραπάνω τύποι συντομογραφούνται ως $(\forall x < y)\psi$ και $(\exists x < y)\psi$ αντίστοιχα. Ένας τύπος ϕ λέγεται *φραγμένος* αν όλοι οι ποσοδείκτες του (αν έχει) είναι φραγμένοι. Ορίζουμε τα σύνολα τύπων Σ_n, Π_n για $n \geq 0$ ως εξής:

$\Sigma_0 = \Pi_0 = \{\phi : \phi$ φραγμένος$\}$.
$\Sigma_{n+1} = \{(\exists \overline{x})\phi : \phi \in \Pi_n\}$.
$\Pi_{n+1} = \{(\forall \overline{x})\phi : \phi \in \Sigma_n\}$.
Αν $\phi \in \Sigma_n$ ο ϕ λέγεται Σ_n *τύπος* και όμοια για το Π_n.

Ένα σύνολο $X \in Def(\mathbb{N})$ λέγεται Σ_n- *(αντίστοιχα* Π_n*-) ορίσιμο* ή απλώς Σ_n (αντίστοιχα Π_n), αν ορίζεται από έναν Σ_n (αντίστοιχα Π_n) τύπο. Τέλος το X λέγεται Δ_n αν είναι συγχρόνως Σ_n και Π_n.

Προφανώς, ένας Σ_n τύπος είναι της μορφής $(\exists \overline{x}_1)(\forall \overline{x}_2)\cdots(Q\overline{x}_n)\psi$, όπου ο ψ είναι φραγμένος, και έχουμε n εναλλαγές ποσοδεικτών ($Q = \forall$ αν n άρτιος και $\exists$ αλλιώς). Όμοια ένας Π_n τύπος είναι της μορφής $(\forall \overline{x}_1)(\exists \overline{x}_2)\cdots(Q\overline{x}_n)\psi$ (με $Q = \exists$ αν n άρτιος και $\forall$ αλλιώς).

Ο παραπάνω χαρακτηρισμός των τύπων είναι καθαρά συντακτικός και προφανώς δεν εξαντλεί το σύνολο των τύπων. Π.χ. αν ο ϕ είναι Σ_2 και ψ είναι Π_3 ο τύπος $\phi \wedge \psi, \phi \vee \psi$ είναι φανερό ότι δεν ανήκει σε καμμιά από τις παραπάνω κλάσεις $Sigma_n$ και Π_n. Όμως θα δούμε ότι ο τελευταίος, όπως και κάθε τύπος, είναι λογικά ισοδύναμος με κάποιον που ανήκει.

Στη Λογική οι τύποι είναι αντικείμενα ενός λογισμού (calculus) που τους μετασχηματίζει διατηρώντας την ''αλήθεια'' τους, όπως ακριβώς στήν άλγεβρα ο λογισμός μετασχηματίζει τους τύπους διατηρώντας την ποσότητα. Και όπως στην άλγεβρα η βασική σχέση των μετασχηματιζόμενων τύπων είναι η ισότητα, στη λογική η αντίστοιχη σχέση είναι η *λογική ισοδυναμία*. Γι' αυτό θα χρειαστεί να μιλήσουμε για τη θεμελιώδη αυτή λογική έννοια.

5.2 Ταυτολογία, λογικό συμπέρασμα, λογική ισοδυναμία

Παρ΄ όλο που στην προηγούμενη παράγραφο αρκεστήκαμε να ορίσουμε την αλήθεια των προτάσεων της L_A μόνο στη δομή $\mathbb{N}$, δεν είναι μόνο αυτή για την οποία έχει νόημα ο συμβολισμός $\mathbb{N} \models \phi$. Υπάρχουν πολλές άλλες ανάλογες δομές

$$M = (M, +^M, \cdot^M, S^M, <^M, 0^M)$$

που ερμηνεύουν τα σύμβολα της L_A, και στις οποίες συνεπώς μπορούμε να ορίσουμε τη σχέση $M \models \phi$, ακριβώς όπως και την $\mathbb{N} \models \phi$. Τις δομές αυτές, ακριβώς επειδή ερμηνεύουν τη γλώσσα L_A, θα τις λέμε L_A-*δομές*. Αν M είναι μία L_A-δομή και T είναι ένα σύνολο προτάσεων της L_A, ο συμβολισμός $M \models T$ σημαίνει $M \models \phi$ για κάθε $\phi \in T$.

Ορισμός 5.2.1 Μία πρόταση ϕ της L_A λέγεται *ταυτολογία ή λογικά αληθής* (logically true), αν $M \models \phi$ για κάθε L_A-δομή M, και *αντίφαση ή λογικά ψευδής* (logically false), αν $M \not\models \phi$ για κάθε M. Γενικότερα, ένας τύπος με ελεύθερες μεταβλητές $\phi(\overline{x})$

λέγεται *ταυτολογία* αν η πρόταση $(\forall\overline{x})\phi(\overline{x})$ είναι ταυτολογία. Ο τύπος $\phi(\overline{x})$ λέγεται *ικανοποιήσιμος* αν υπάρχει δομή M τέτοια ώστε $M \models (\exists\overline{x})\phi(\overline{x})$. Αν T είναι σύνολο προτάσεων και ϕ μία πρόταση, η ϕ λέγεται *λογικό συμπέρασμα* του T, συμβολικά $T \models \phi$, αν για κάθε δομή M τέτοια ώστε $M \models T$, $M \models \phi$. Γενικότερα, δοθέντων τύπων ϕ, ψ, ο ψ λέγεται *λογικό συμπέρασμα* του ϕ, με σύμβολα $\phi \models \psi$, αν ο τύπος $\phi \to \psi$ είναι ταυτολογία. Δύο τύποι ϕ και ψ, λέγονται *λογικά ισοδύναμοι* (logically equivalent), συμβολικά $\phi \models\mid \psi$, αν $\phi \models \psi$ και $\psi \models \phi$.

Παρατήρηση 5.2.2 1) Για κάθε πρόταση ϕ η ϕ είναι ταυτολογία αν και μόνον αν η $\neg\phi$ είναι αντίφαση.

2) Αν η $\phi(\overline{x})$ είναι τύπος με ελεύθερες μεταβλητές, η $\phi(\overline{x})$ είναι ταυτολογία αν και μόνον αν η $\neg\phi(\overline{x})$ δεν είναι ικανοποιήσιμη.

3) Όλες οι ταυτολογίες είναι μεταξύ τους λογικά ισοσύναμες, το ίδιο και οι αντιφάσεις, γι' αυτό θα συμβολίζουμε με $\top$ και $\bot$ την τυχαία ταυτολογία και αντίφαση αντίστοιχα.

4) Για κάθε ϕ, $\bot \models \phi$ και $\phi \models \top$.

5) $\phi \models\mid \psi$ αν και μόνον αν ο $\phi \leftrightarrow \psi$ είναι ταυτολογία.

Δυό λογικά ισοδύναμοι τύποι είναι σημασιολογικά ταυτόσημοι (χονδρικά είναι δύο φράσεις με το ίδιο ακριβώς νόημα), γι' αυτό είναι σημαντικό να αναγνωρίζουμε μετασχηματισμούς που διατηρούν την ισοδυναμία. Βασικούς τέτοιους μετασχηματισμούς περιέχει ο παρακάτω κατάλογος.

Βασικές λογικές ισοδυναμίες.

(1) $\phi \to \psi \models\mid \neg\phi \vee \psi$.
(2) $\phi \leftrightarrow \psi \models\mid (\phi \to \psi) \wedge (\psi \to \phi)$.
(3) $\neg(\phi \wedge \psi) \models\mid \neg\phi \vee \neg\psi$.
(4) $\neg(\phi \vee \psi) \models\mid \neg\phi \wedge \neg\psi$.
(5) $\neg\neg\phi \models\mid \phi$.
(6) $\phi \wedge \psi \models\mid \psi \wedge \phi$.
(7) $\phi \vee \psi \models\mid \psi \vee \phi$.
(8) $\phi \wedge (\psi \wedge \sigma) \models\mid (\phi \wedge \psi) \wedge \sigma$.
(9) $\phi \vee (\psi \vee \sigma) \models\mid (\phi \vee \psi) \vee \sigma$.
(10) $\phi \wedge (\psi \vee \sigma) \models\mid (\phi \wedge \psi) \vee (\phi \wedge \sigma)$.
(11) $\phi \vee (\psi \wedge \sigma) \models\mid (\phi \vee \psi) \wedge (\phi \vee \sigma)$.
(12) $\phi \wedge \psi \models\mid \phi$ αν και μόνον αν $\phi \models \psi$.
(13) $\phi \vee \psi \models\mid \phi$ αν και μόνον αν $\psi \models \phi$.
(14) $\neg(\forall x)\phi \models\mid (\exists x)\neg\phi$.
(15) $\neg(\exists x)\phi \models\mid (\forall x)\neg\phi$.
(16) $(\forall x)(\forall y)\phi \models\mid (\forall y)(\forall x)\phi$.

(17) $(\exists x)(\exists y)\phi \models\mid (\exists y)(\exists x)\phi$.
(18) $(\forall x)(\phi \wedge \psi) \models\mid (\forall x)\phi \ \wedge \ (\forall x)\psi$.
(19) $(\exists x)(\phi \vee \psi) \models\mid (\exists x)\phi \ \vee \ (\exists x)\psi$.
(20) $(Qx)\phi(x) \models\mid (Qy)\phi(y)$, $(Q = \exists$ ή $\forall)$ αν η y είναι μία νέα μεταβλητή που δεν υπάρχει στον $\phi(x)$. (Αλλαγή δεσμευμένης μεταβλητής.)
(21) $(Qx)\phi \models\mid \phi$, $(Q = \exists$ ή $\forall)$ αν η x δεν είναι ελεύθερη μεταβλητή στον ϕ. (Εικονική μεταβλητή.)
(22) $(Qx)\phi \ \wedge \ \psi \models\mid (Qx)(\phi \wedge \psi)$, άν η x δεν είναι ελεύθερη μεταβλητή στην ψ (και όμοια με $\vee$ στη θέση του $\wedge$).

Με τη βοήθεια των παραπάνω ισοδυναμιών εύκολα μπορεί κανείς να δείξει το παρακάτω:

Λήμμα 5.2.3 *Κάθε τύπος ϕ, μπορεί να πάρει την εξής λογικά ισοδύναμη κανονική μορφή:*

$$\phi \models\mid (Q_1x_1)\cdots(Q_kx_k)\psi, \tag{16}$$

όπου Q_i ποσοδείκτες και η ψ είναι τύπος χωρίς ποσοδείκτες.

Ο δεξιός τύπος της (16) λέγεται *κανονική prenex μορφή* της ϕ. Το πλεονέκτημά αυτού του τύπου είναι ότι όλοι οι ποσοδείκτες είναι συγκεντρωμένοι μπροστά και έτσι μπορούμε να δούμε τον αριθμό και τις εναλλαγές των ποσοδεικτών, και να εκτιμήσουμε την λογική του πολυπλοκότητα. Η ακολουθία των ποσοδεικτών $(Q_1x_1)\cdots(Q_kx_k)$ της κανονικής μορφής λέγεται *πρόθεμα* (prefix) του τύπου.

5.3 Αναδρομικότητα και ορισιμότητα

Επιστρέφουμε στα ορίσιμα σύνολα και την ιεραρχία των Σ_n-, Π_n-συνόλων της § 3.1. Μπορούμε τώρα να δούμε ότι κάθε ορίσιμο σύνολο στο $\mathbb{N}$ θα είναι Σ_n ή Π_n σύνολο για κάποιο n. Το απλό γεγονός που χρησιμοποιείται στις αποδείξεις είναι ότι δύο λογικά ισοδύναμοι τύποι ορίζουν το ίδιο σύνολο στο $\mathbb{N}$.

Λήμμα 5.3.1 *Έστω Σ_n, Π_n οι κλάσεις των Σ_n-, Π_n-συνόλων αντίστοιχα. Τότε:*
(α) $Def(\mathbb{N}) = \bigcup_n(\Sigma_n \cup \Pi_n)$.
(β) $X \in \Sigma_n \iff -X \in \Pi_n$.
(γ) Γιά κάθε n, $\Sigma_n \cup \Pi_n \subseteq \Delta_{n+1} = \Sigma_{n+1} \cap \Pi_{n+1}$.
(δ) Κάθε κλάση Σ_n και Π_n είναι κλειστή ως προς τομή και ένωση. Οι κλάσεις Δ_n είναι επί πλέον κλειστές ως προς το συμπλήρωμα.

Απόδειξη. (α) Προφανώς $\bigcup_n(\Sigma_n \cup \Pi_n) \subseteq Def(\mathbb{N})$. Έστω $X \in Def(\mathbb{N})$, $X \subseteq \mathbb{N}^n$ και έστω ότι το X ορίζεται με τον τύπο $\phi(x_1, \ldots, x_n)$. Από το Λήμμα 5.2.3, έστω

$\phi^*(x_1,\ldots,x_n)$ η κανονική prenex μορφή της ϕ. Επειδή $\phi \models\mid \phi^*$,

$$X = \{(a_1,\ldots,a_n) : \mathbb{N} \models \phi(\underline{a_1},\ldots,\underline{a_n})\} = \{(a_1,\ldots,a_n) : \mathbb{N} \models \phi^*(\underline{a_1},\ldots,\underline{a_n})\}.$$

Δηλαδή το X ορίζεται από την ϕ^*, και $\phi^* = (Q_1x_1)\cdots(Q_kx_k)\psi$, με ψ χωρίς ποσοδείκτες. Τώρα είναι προφανές ότι η ϕ^* είναι Σ_n ή Π_n-τύπος για κάποιο n, πράγμα που καθορίζεται από το $(Q_1x_1)\cdots(Q_kx_k)$ πρόθεμα. Π.χ. αν αυτό είναι $\forall\forall\exists\exists\forall$, η ϕ^*, και άρα το X, είναι Π_3.

(β) Έστω ότι το X ορίζεται με τον Σ_n τύπο ϕ με κανονική μορφή: $(\exists_1x_1)\cdots(Q_nx_n)\psi$. Τότε το $-X$ ορίζεται από τον τύπο:

$$\neg\phi = \neg[(\exists x_1)\cdots(Q_kx_n)\psi]$$

όπου ο τελευταίος ισοδυναμεί με την βοήθεια των βασικών ισοδυναμιών με $(\forall x_1)\cdots(\check{Q}_nx_n)\neg\psi$ όπου $\check{\exists} = \forall$ και $\check{\forall} = \exists$. Άρα ο $(\forall x_1)\cdots(\check{Q}_nx_n)\neg\psi$ είναι Π_n, και συνεπώς $-X \in \Pi_n$.

(γ) Η κανονική μορφή ενός τύπου, και ειδικά το πρόθεμά του, δεν είναι μοναδικά. Π.χ. λόγω της βασικής ισοδυναμίας (21) μπορεί κανείς να προσθέσει σε ένα πρόθεμα εικονικές μεταβλητές. Έτσι αν ϕ είναι ένας Σ_n τύπος, και u είναι μια μεταβλητή που δεν υπάρχει στον ϕ, ο $(\forall u)\phi$ είναι P_{n+1} σύμφωνα με τον ορισμό 5.1.8 και $\phi \models\mid (\forall u)\phi$ σύμφωνα με την ισοδυναμία (21). Αν λοιπόν $X \in \Sigma_n$ και το X ορίζεται με τον ϕ, τότε το X ορίζεται με τον $(\forall u)\phi$, άρα $X \in \Pi_{n+1}$. Συνεπώς $\Sigma_n \subseteq \Pi_{n+1}$ και όμοια δείχνουμε ότι $\Pi_n \subseteq \Sigma_{n+1}$.

Επίσης με (ταυτόχρονη) επαγωγή μπορούμε να δείξουμε ότι $\Sigma_n \subseteq \Sigma_{n+1}$ καί $\Pi_n \subseteq \Pi_{n+1}$. Πράγματι, με εικονικές μεταβλητές αμέσως έχουμε ότι $\Sigma_0 \subseteq \Sigma_1$ και $\Pi_0 \subseteq \Pi_1$. Ας υποθέσουμε ότι $\Sigma_n \subseteq \Sigma_{n+1}$ καί $\Pi_n \subseteq \Pi_{n+1}$. Έστω $X \in \Sigma_{n+1}$. Τότε το X ορίζεται με έναν τύπο $(\exists x)\phi$, όπου ο ϕ είναι Π_n. Από την υπόθεση της επαγωγής ο Π_n ισοδυναμεί με κάποιον Π_{n+1} τύπο, άρα ο $(\exists x)\phi$ ισοδυναμεί με κάποιον Σ_{n+2} τύπο, δηλαδή το $X \in \Sigma_{n+2}$. Άρα $\Sigma_{n+1} \subseteq \Sigma_{n+2}$. Τελικά βλέπουμε ότι $\Sigma_n \subseteq \Pi_{n+1} \cap \Sigma_{n+1}$, και $\Pi_n \subseteq \Pi_{n+1} \cap \Sigma_{n+1}$, άρα $\Sigma_n \cup \Pi_n \subseteq \Sigma_{n+1} \cap \Pi_{n+1} = \Delta_{n+1}$.

(δ) Με ταυτόχρονη επαγωγή στο n δείχνουμε ότι οι Σ_n και Π_n είναι κλειστές ως προς $\cap$ και $\cup$. Για τις $\Sigma_0 = \Pi_0$ αυτό είναι προφανές. Έστω ότι ισχύει για n και έστω $X, Y \in \Sigma_{n+1}$. Αυτά ορίζονται από τύπους της μορφής $(\exists x)\phi$ και $(\exists x)\psi$ αντίστοιχα, όπου οι ϕ, ψ είναι Π_n. Το $X \cup Y$ ορίζεται από τον τύπο $(\exists x)\phi \vee (\exists x)\psi$ ο οποίος από την ισοδυναμία (19) γράφεται $(\exists x)(\phi \vee \psi)$. Από την υπόθεση της επαγωγής ο $\phi \vee \psi$ ισοδυναμεί με Π_n τύπο, άρα ο $(\exists x)(\phi \vee \psi)$ ισοδυναμεί με Σ_{n+1}. Άρα $X \cup Y \in \Sigma_{n+1}$. Το $X \cap Y$ ορίζεται από τον τύπο $(\exists x)\phi \wedge (\exists x)\psi$. Εδώ κάνουμε αλλαγή μεταβλητής στην ψ (ισοδυναμία (20)), αντικαθιστώντας την x με μία νέα μεταβλητή y και η τελευταία γράφεται $(\exists x)\phi \wedge (\exists y)\psi$. Από την ισοδυναμία (22), η τελευταία ισοδυναμεί με $(\exists x)(\exists y)(\phi \wedge \psi)$. Από την υπόθεση της επαγωγής και πάλι, η τελεταία

είναι Σ_{n+1} και άρα $X \cap Y \in \Sigma_{n+1}$. Αυτό δείχνει την κλειστότητα του Σ_{n+1}. Όμοια δείχνεται η κλειστότητα του Π_{n+1} ως προς $\cap, \cup$, πράγμα που ολοκληρώνει την επαγωγή.

Τώρα για την κλάση Δ_n, αν $X \in \Delta_n$, τότε $X \in \Sigma_n$ και $X \in \Pi_n$, άρα, από το (β), $-X \in \Pi_n$ και $-X \in \Sigma_n$, άρα $-X \in \Delta_n$. QED

Τα αποτελέσματα της προηγούμενης Πρότασης οφείλονται στις καθαρά *λογικές* ιδιότητες των τύπων (λογικές ισοδυναμίες) και δεν έχουν να κάνουν με το *μαθηματικό* τους περιεχόμενο, δηλαδή τις μαθηματικές ιδιότητες του $\mathbb{N}$. Παρακάτω θα δούμε ένα αποτέλεσμα που είναι μαθηματικού και όχι (μόνο) λογικού περιεχομένου, δηλαδή ισχύει μόνο στη δομή $\mathbb{N}$ (και ίσως και άλλες ''παρόμοιες'') αλλά όχι σε κάθε L_A-δομή. Ένας τύπος ϕ μπορεί να ισοδυναμεί με ένα άλλο ψ *μέσα στην* $\mathbb{N}$ *μόνο*, λόγω των συγκεκριμένων ιδιοτήτων του $\mathbb{N}$, δηλαδή να έχουμε $\mathbb{N} \models \phi \leftrightarrow \psi$, και άρα οι ϕ, ψ να ορίζουν το ίδιο σύνολο του $Def(\mathbb{N})$ χωρίς οι ϕ, ψ να είναι λογικά ισοδύναμες.

Λήμμα 5.3.2 *Κάθε κλάση Σ_n, Π_n είναι κλειστή ως προς φραγμένους ποσοδείκτες. Δηλαδή αν $\phi \in \Sigma_n$ (Π_n), τότε και οι $(\forall x < y)\phi$, $(\exists x < y)\phi$ ανήκουν στην Σ_n (Π_n).*

Απόδειξη. Με ταυτόχρονη επαγωγή στο n. Για $n = 0$ ο ισχυρισμός είναι προφανής από τον ορισμό της Σ_0. Έστω ισχύει για n, δηλαδή οι κλάσεις Σ_n και Π_n είναι κλειστές ως προς φραγμένους ποσοδείκτες, και έστω ϕ ένας Σ_{n+1} τύπος. Τότε $\phi \models| (\exists u)\psi$, όπου η ψ είναι Π_n. Άρα $(\exists x < y)\phi \models| (\exists x < y)(\exists u)\psi$. Από την ισοδυναμία (17), η τελευταία ισοδυναμεί με $(\exists u)(\exists x < y)\psi$. Από τη υπόθεση της επαγωγής η $(\exists x < y)\psi$ είναι Π_n, άρα η $(\exists u)(\exists x < y)\psi$ είναι Σ_{n+1}. (Μέχρις εδώ και πάλι χρησιμοποιήσαμε μόνο λογική.)

Έστω τώρα ο τύπος $(\forall x < y)\phi \models| (\forall x < y)(\exists u)\psi$. Θα δείξουμε ότι υπάρχει Σ_{n+1} τύπος σ τέτοιος ώστε

$$\mathbb{N} \models (\forall x < y)(\exists u)\psi \ \leftrightarrow \ \sigma.$$

Έστω $\mathbb{N} \models (\forall x < y)(\exists u)\psi$. Το νόημα του τύπου είναι ότι για κάθε $x < y$ υπάρχει ένα u τέτοιο ώστε να αληθεύει ο ψ. Για κάθε $x \in \mathbb{N}$ έστω $f(x) \in \mathbb{N}$ το ελάχιστο τέτοιο u. Όταν όμως τα x αυτά φράσσονται από ένα $y \in \mathbb{N}$, είναι προφανές ότι τα αντίστοιχα $f(x)$ θα φράσσονται από κάποιο $w \in N$. Δηλαδή θα ισχύει στο $\mathbb{N}$ η πρόταση $(\exists w)(\forall x < y)(\exists u < w)\psi$. Και επειδή η τελευταία συνεπάγεται την πρώτη, οι δυό ισχυρισμοί είναι ισοδύναμοι μέσα στο $\mathbb{N}$, δηλαδή

$$\mathbb{N} \models (\forall x < y)(\exists u)\psi \ \leftrightarrow \ (\exists w)(\forall x < y)(\exists u < w)\psi.$$

Από την υπόθεση της επαγωγής, ο τύπος $(\forall x < y)(\exists u < w)\psi$ είναι Π_n, άρα ο $(\exists w)(\forall x < y)(\exists u < w)\psi$ είναι Σ_{n+1} και είναι ο ζητούμενος σ.

Η απόδειξη της κλειστότητας του Π_n να γίνει σαν άσκηση. QED

Εξ ορισμού ένας Σ_n τύπος είναι της μορφής $(\exists \overline{x}_1)(\forall \overline{x}_2)(\exists \overline{x}_3)\cdots(Q\overline{x}_n)\psi$, όπου $\psi \in \Sigma_0$ και κάθε $Q\overline{x}_i$ είναι ένα μπλόκ ομοειδών ποσοδεικτών. Στην παρακάτω πρόταση δείχνουμε ότι *μέσα στο* $\mathbb{N}$ μπορούμε να πάρουμε τον ψ έτσι ώστε κάθε τέτοιο μπλόκ να αποτελείται από *έναν* μόνο ποσοδείκτη.

Λήμμα 5.3.3 *Αν ο ϕ είναι Σ_n, τότε υπάρχει $\psi \in \Sigma_0$ τέτοιος ώστε*

$$\mathbb{N} \models \phi \ \leftrightarrow\ (\exists x_1)(\forall x_2)(\exists x_3)\cdots(Qx_n)\psi.$$

Και ανάλογα αν ο ϕ είναι Π_n.

Απόδειξη. Αρκεί να δείξουμε ότι για κάθε τύπο της μορφής $(\exists x_1)\cdots(\exists x_m)\sigma$ με $\sigma \in \Sigma_n$ (ή $\sigma \in \Pi_n$) , υπάρχει $\sigma' \in \Sigma_n$ (ή $\sigma' \in \Pi_n$ αντίστοιχα) τέτοιος ώστε

$$\mathbb{N} \models (\exists x_1)\cdots(\exists x_m)\sigma \ \leftrightarrow\ (\exists x)\sigma',$$

και όμοια για κάθε τύπο $(\forall x_1)\cdots(\forall x_m)\sigma$. Όμως αυτό προκύπτει απ' τους εξής τετριμμένους μετασχηματισμούς:

$$\mathbb{N} \models (\exists x_1)\cdots(\exists x_m)\sigma \ \leftrightarrow\ (\exists x)(\exists x_1 < x)\cdots(\exists x_m < x)\sigma,$$

και

$$\mathbb{N} \models (\forall x_1)\cdots(\forall x_m)\sigma \ \leftrightarrow\ (\forall x)(\forall x_1 < x)\cdots(\forall x_m < x)\sigma.$$

Θέτοντας $\sigma' = (\exists x_1 < x)\cdots(\exists x_m < x)\sigma$ και $\sigma' = (\forall x_1 < x)\cdots(\forall x_m < x)\sigma$, από το Λήμμα 5.3.2, οι σ' και σ ανήκουν στην ίδια κλάση Σ_n ή Π_n, και άρα έχουμε αυτό που θέλουμε.

[Ένας άλλος τρόπος είναι να κωδικοποιήσουμε την n-άδα των μεταβλητών $x_1, \ldots, x_n$ με μία, οπότε έχουμε

$$\mathbb{N} \models (\exists x_1)\cdots(\exists x_m)\sigma(x_1, \ldots, x_n) \ \leftrightarrow\ (\exists x)\sigma((x)_1, \ldots, (x)_n).$$

Τότε $\sigma' = \sigma((x)_1, \ldots, (x)_n)$, και είναι εύκολο να δείξει κανείς ότι αυτές ανήκουν στην ίδια κλάση της ιεραρχίας Σ_n, Π_n.] QED

Πρόταση 5.3.4 *(α) Κάθε Σ_0 σύνολο είναι βασικό αναδρομικό.*
(β) Κάθε Σ_1 σύνολο είναι α.α.
(γ) Κάθε Δ_1 σύνολο είναι αναδρομικό.

Απόδειξη. (α) Οι τύποι Σ_0 παράγονται από ατομικούς τύπους $t = s$, $t < s$ με συνδέσμους και φραγμένους ποσοδείκτες. Τα σύνολα που ορίζονται με τύπους $t = s$ και $t < s$ (και τις αρνήσεις τους) είναι β.α. όπως προκύπτει από την Πρόταση 2.3.2. Οι σύνδεσμοι $\wedge$, $\vee$ αντιστοιχούν στις πράξεις $\cap$ και $\cup$ των συνόλων. Αλλά η κλάση των

β.α. συνόλων είναι κλειστή ως προς τομή, ένωση και φραγμένους ποσοδείκτες όπως δείξαμε στη Πρόταση 2.3.3.

(β) Έστω X ένα Σ_1 σύνολο. Από το Λήμμα 5.3.3, το X ορίζεται από έναν τύπο $(\exists x)\phi(x,y)$, όπου ο $\phi(x,y)$ είναι Σ_0. Από το (α), η σχέση $\phi(x,y)$ είναι αναδρομική, και άρα το X είναι α.α. από την πρόταση 2.6.4.

(γ) Έστω $X \in \Delta_1$. Αφού $X \in \Sigma_1$, από το (β), το X είναι α.α. Επίσης το $X \in \Pi_1$, άρα $-X \in \Sigma_1$, οπότε και το $-X$ είναι α.α. Από την Πρόταση 2.6.2 (β), το X είναι αναδρομικό. QED

Το κεντρικό θεώρημα αυτής της παραγράφου είναι ουσιαστικά το αντίστροφο του (γ) του προηγουμένου. Μια συνάρτηση $f : \mathbb{N}^k \to \mathbb{N}$ θα λέμε ότι είναι Σ_n, αν το γράφημά της είναι Σ_n, δηλαδή αν υπάρχει Σ_n τύπος $\phi(x_1,\ldots,x_k,y)$, τέτοιος ώστε για κάθε $a_1,\ldots,a_k,b \in \mathbb{N}$,

$$f(a_1,\ldots,a_k) = b \iff \mathbb{N} \models \phi(\underline{a_1},\ldots \underline{a_k},\underline{b}).$$

Θεώρημα 5.3.5 (Gödel) *Κάθε ολική αναδρομική συνάρτηση είναι* Σ_1.

Απόδειξη. Η απόδειξη γίνεται με επαγωγή στα βήματα ορισμού των αναδρομικών συναρτήσεων.

(α) Οι αρχικές συναρτήσεις ορίζονται από πολύ απλούς τύπους χωρίς ποσοδείκτες, άρα είναι Σ_0 ορίσιμες. Συγκεκριμένα, η συνάρτηση S ορίζεται από τον τύπο $\phi(x,y) := (y = S(x))$. Η σταθερά συνάρτηση $c_0(x) = 0$ ορίζεται από τον τύπο $\phi(x,y) := (y = \underline{0})$. Η προβολή π_{nm} ορίζεται από τον τύπο $\phi(x_1,\ldots,x_n,y) := (y = x_m)$.

(β) Έστω ότι η f παράγεται με σύνθεση από τις h και $g_1,\ldots,g_m$, δηλαδή

$$f(x_1,\ldots,x_k) = h(g_1(x_1,\ldots,x_k),\ldots,g_m(x_1,\ldots,x_k)),$$

και έστω ότι οι h και $g_1,\ldots,g_m$ ορίζονται με Σ_1 τύπους ψ και $\sigma_1,\ldots,\sigma_m$ αντίστοιχα. Τότε η προηγούμενη γράφεται:

$$f(a_1,\ldots,a_k) = b \Leftrightarrow (\exists x_1)\cdots(\exists x_m)[\bigwedge_{i=1}^{m} g(a_1,\ldots,a_k) = x_i \;\&\; h(x_1,\ldots,x_m) = b].$$

Όμως

$$g(a_1,\ldots,a_k) = x_i \iff \mathbb{N} \models \sigma_i(\underline{a_1},\ldots \underline{a_k},x_i)$$

και

$$h(x_1,\ldots,x_m) = b \iff \mathbb{N} \models \psi(x_1,\ldots,x_m,\underline{b}).$$

Βάσει των δύο τελευταίων η πιο πάνω γράφεται:

$$f(a_1,\ldots,a_k)=b \Leftrightarrow \mathbb{N}\models(\exists x_1)\cdots(\exists x_m)[\bigwedge_{i=1}^{m}\sigma_i(\underline{a_1},\ldots\underline{a_k},x_i)\ \wedge\ \psi(x_1,\ldots,x_m,\underline{b})].$$

Αλλά αφού οι τύποι σ_i και ψ είναι Σ_1, το ίδιο είναι όλος ο τύπος του δεξιού μέρους που ορίζει την f, βάσει των λημμάτων 5.3.1 και 5.3.2.

(γ) Έστω ότι η f παράγεται με ελαχιστοποίηση από την g, δηλαδή

$$f((x_1,\ldots,x_k)=(\mu y)(g(x_1,\ldots,x_k,y)=1),$$

και έστω ότι η g ορίζεται με τον Σ_1 τύπο $\psi(x_1,\ldots,x_k,y,z)$. Τότε

$$f(a_1,\ldots,a_k)=b \Leftrightarrow [g(a_1,\ldots,a_k,b)=1\ \&\ (\forall x<b)(g(a_1,\ldots,a_k,x)\neq 1)].$$

Αυτή με τη βοήθεια της ψ γράφεται

$$f(a_1,\ldots,a_k)=b \Leftrightarrow \mathbb{N}\models\psi(\underline{a_1},\ldots,\underline{a_k},\underline{b},\underline{1})\ \wedge\ (\forall x<\underline{b})\neg\psi(\underline{a_1},\ldots,\underline{a_k},x,\underline{1})).$$

Ο τύπος δεξιά που ορίζει την f είναι προφανώς Σ_1 όταν ο ψ είναι Σ_1, βάσει των λημμάτων 5.3.1 και 5.3.2.

(δ) Έστω, τέλος, ότι η f παράγεται από τις h και g με το σχήμα βασικής αναδρομής, δηλαδή

$f(\overline{x},0)=g(\overline{x})$,

$f(\overline{x},y+1)=h(\overline{x},y,f(\overline{x},y))$,

και οι h,g ορίζονται με τους Σ_1 τύπους ψ και σ αντίστοιχα. Τότε η έκφραση

$$f(\overline{x},m)=y$$

ισοδυναμεί με τον ισχυρισμό:

‘‘Υπάρχει ακολουθία $z_0,z_1,\ldots,z_m$ τέτοια ώστε

$$\begin{array}{lcl} z_0 & = & g(\overline{x}) \\ z_1 & = & h(\overline{x},0,z_0) \\ \ldots & \ldots & \ldots\ldots\ldots \\ z_{m-1} & = & h(\overline{x},m-2,z_{m-2}) \\ z_m=y.\text{‘‘} & & \end{array}$$

Χρησιμοποιώντας κωδικοποίηση, η έκφραση αυτή γράφεται:

$$(\exists z)[(z)_0=g(\overline{x})\ \wedge\ (z)_m=y\ \wedge(\forall i<m)((z)_i=h(\overline{x},i-1,(z)_{i-1})].$$

Δεδομένου ότι οι g και h είναι Σ_1, η δε συνάρτηση $(x)_y=z$ είναι Σ_0 (β.α.), αμέσως προκύπτει ότι η f είναι Σ_1. Αυτό ολοκληρώνει τα βήματα της επαγωγής και την απόδειξη. QED

Θεώρημα 5.3.6 *(α) Ένα σύνολο είναι αναδρομικό αν και μόνον αν είναι* Δ_1.
(β) Ένα σύνολο είναι α.α. αν και μόνον αν είναι Σ_1.

Απόδειξη. (α) Η μία κατεύθυνση είναι η Πρόταση 5.3.4 (γ). Για το αντίστροφο έστω X αναδρομικό. Τότε η χαρακτηριστική του συνάρτηση C_X είναι ολική αναδρομική, άρα Σ_1 από το Θεώρημα 5.3.5. Δεδομένου ότι $x \in X \iff C_X(x) = 1$, αμέσως έπεται ότι το X είναι Σ_1. Επίσης το $-X$ είναι αναδρομικό και συνεπώς όμοια Σ_1. Οπότε το X είναι συγχρόνως Σ_1 και Π_1.

(β) Επίσης η μία κατεύθυνση είναι η 5.3.4 (β). Για το αντίστροφο έστω X α.α. Από την πρόταση 2.6.4, το X ορίζεται με μία σχέση της μορφής $(\exists x)((x, y) \in Y)$, όπου Y αναδρομικό. Από το (α), το Y είναι Σ_1, άρα προφανώς και το X είναι Σ_1. QED

6 Τυπική Αριθμητική. Αποδειξιμότητα, μη πληρότητα

6.1 Peano αριθμητική

Στα τέλη του 19ου (1889) ο Giuseppe Peano ήταν ο πρώτος που σκέφτηκε να θεμελιώσει τη θεωρία των φυσικών αριθμών πάνω σε ένα μικρό σχετικά σύνολο θεμελιωδών προτάσεων (αξιωμάτων) που αφορούν τις βασικές πράξεις $+, \cdot, S, \underline{0}$, με την ελπίδα ότι από αυτά θα απέρρεαν με λογικό τρόπο όλες οι άλλες. Το σύστημα του δεν ήταν ακριβώς αυτό που σήμερα ονομάζουμε ''πρωτοβάθμια Peano αριθμητική'' ή απλώς ''Peano αριθμητική'' (δες [5] για το αυθεντικό σύστημα του Peano). Η κύρια διαφορά βρίσκεται στο αξίωμα επαγωγής. Ο Peano χρησιμοποίησε το *δευτεροβάθμιο αξίωμα επαγωγής*:

$$(I^2) \qquad (\forall X)[0 \in X \wedge (\forall x)(x \in X \to x{+}1 \in X) \ \to \ (\forall y)(y \in X)].$$

Από τα σχολικά μαθηματικά μας έχουν μάθει να θεωρούμε ως αξίωμα επαγωγής την παραπάνω πρόταση. Όμως για να είμαστε ακριβείς το αξίωμα αυτό δεν αναφέρεται μόνο σε αριθμούς, όπως θα απαιτούσε μια καθαρόαιμη θεωρία αριθμών, αλλά και σε *σύνολα* αριθμών (στην παραπάνω πρόταση η μεταβλητή X διατρέχει σύνολα, ενώ οι x, y αριθμούς, εξ ού και δευτεροβάθμιο), πράγμα που το κάνει πολύ ισχυρό αλλά λογικά μη αποδεκτό. Όταν μιλάμε για αριθμούς και τη συμπεριφορά τους σε σχέση με την πρόσθεση, τον πολλ/σμό κλπ, δεν μπορούμε συγχρόνως να μιλάμε για συμπεριφορά *συνόλων αριθμών*. Αυτό παύει να είναι αριθμητική με την τρέχουσα έννοια (δηλαδή πρώτου βαθμού) και γίνεται αριθμητική δευτέρου βαθμού. Αποδεικνύεται ότι η μόνη L_A-δομή που ικανοποιεί το I^2 είναι το $\mathbb{N}$ (η κάθε σύνολο ισόμορφο μ' αυτό), δηλαδή το I^2 *χαρακτηρίζει* το $\mathbb{N}$.

Σήμερα, στη θέση του I^2 χρησιμοποιούμε την *πρωτοβάθμια* εκδοχή του, ότι δηλαδή μόνον τα *ορίσιμα* σύνολα έχουν την ιδιότητα που ισχυρίζεται το I^2. Τα ορίσιμα σύνολα

αντιπροσωπεύονται από ιδιότητες $\phi(x)$ της L_A, (όπου η $\phi(x)$ μπορεί να περιέχει κι άλλες ελεύθερες μεταβλητές εκτός από τη x). Για κάθε τέτοια ιδιότητα, έχουμε το αντίστοιχο αξίωμα I_ϕ:

$$(I_\phi) \qquad [\phi(0) \wedge (\forall x)(\phi(x) \to \phi(x+1))] \to (\forall y)\phi(y).$$

Συνεπώς στη θέση του I^2 έχουμε ένα άπειρο σύνολο πρωτοβάθμιων αξιωμάτων

$$I = \{I_\phi : \phi \in F(L_A)\},$$

με την ίδια συντακτική μορφή. Το I λέγεται *(πρωτοβάθμιο) αξιωματικό σχήμα επαγωγής*.

Εκτός από το I, χρειαζόμαστε μερικά αξιώματα, που περιέχουν τις ιδιότητες της συνάρτησης S και τους αναδρομικούς ορισμούς των $+$ και $\cdot$. Αυτά είναι τα εξής (παραλείπουμε τους καθολικούς ποσοδείκτες, δηλαδή γράφουμε $\phi(\overline{x})$ αντί για $(\forall \overline{x})\phi(\overline{x})$):

$(P1)$ $s(x) \neq \underline{0}$.
$(P2)$ $s(x) = s(y) \to x = y$.
$(P3)$ $x + \underline{0} = x$.
$(P4)$ $x + S(y) = S(x + y)$.
$(P5)$ $x \cdot \underline{0} = \underline{0}$.
$(P6)$ $x \cdot S(y) = x \cdot y + x$.

Έστω

$$PA^- = \{P1, \ldots, P6\} \text{ και } PA = PA^- \cup I.$$

Το σύστημα των αξιωμάτων PA λέγεται *πρωτοβάθμια Peano αριθμητική*, ή *τυπική αριθμητική* (formal aritmetic) σε αντιδιαστολή προς τη θεωρία της δομής $\mathbb{N}$, $Th(\mathbb{N})$, που είδαμε στο προηγούμενο κεφάλαιο, και ονομάσαμε ''πλήρη αριθμητική''. Φυσικά οι θεωρίες αυτές δεν είναι ασύμβατες, ήδη είναι προφανές ότι όλα τα αξιώματα του PA αληθεύουν στο $\mathbb{N}$, άρα $PA \subseteq Th(\mathbb{N})$. Ισχύει όμως το αντίστροφο; Μπορεί κάθε $\phi \in Th(\mathbb{N})$ να παραχθεί με λογικά μέσα από τα αξιώματα του PA; Ο Gödel έδειξε ότι η απάντηση είναι όχι, και στο κεφάλαιο αυτό θα δώσουμε μια απόδειξη αυτού του σημαντικού θεωρήματος. Προηγουμένως όμως πρέπει να ορίσουμε με αυστηρό τι σημαίνει ''παράγεται με λογικά μέσα από το PA''. Αυτή είναι η έννοια της *τυπικής απόδειξης*, δηλαδή της απόδειξης όπως ορίζεται στη λογική. Θα κάνουμε λοιπόν και πάλι μια σύντομη παρέκβαση στο πεδίο της στοιχειώδους λογικής.

6.2 Λογικά αξιώματα, τυπική απόδειξη

Στις § 3.1 και 3.2 κάναμε μια εισαγωγή στις σημασιολογικές έννοιες της λογικής, αυτές δηλαδή που εμπεριέχουν τον όρο ''αλήθεια'', όπως αληθής πρόταση, λογικό συμπέρασμα, ταυτολογία κλπ. Συμπληρωματική της αλήθειας είναι η συντακτική έννοια της

''απόδειξησ''. Η (τυπική) απόδειξη προϋποθέτει την ύπαρξη μιας τυπικής λογικής, δηλαδή ενός συστήματος που αποτελείται από μια *τυπική γλώσσα*, *λογικά αξιώματα* και *κανόνες παραγωγής*. Η πιο συνηθισμένη τυποποίηση για τις ανάγκες της αριθμητικής είναι η τυποποίηση κατά Hilbert, όπου η έμφαση δίνεται στα λογικά αξιώματα παρά στους κανόνες παραγωγής. Η τυπική γλώσσα θα είναι αυτή που ήδη ξέρουμε, η $L_A = \{+, \cdot, S, \underline{0}\}$ μαζί με τα υπόλοιπα standard λογικά σύμβολα. Τα αξιώματα είναι ορισμένα μοτίβα ταυτολογιών που τα θεωρούμε θεμελώδη, ενώ έχουμε δύο μόνον κανόνες παραγωγής. Το τυπικό σύστημα θα το ονάζουμε *Κατηγορηματικό Λογισμό* (Predicate Calculus), και θα το συμβολίζουμε **PC**. Τα αξιώματα του **PC** είναι στην πραγματικότητα *σχήματα αξιωμάτων* και όχι μεμονωμένοι τύποι. Π.χ. κάθε τύπος της μορφής $\phi \to (\psi \to \phi)$ είναι αξίωμα, ότι και να είναι οι ϕ, ψ. Μ' άλλα λόγια χρησιμοποιούμε την άπειρη οικογένεια

$$\Pi 1 = \{\phi \to (\psi \to \phi) : \phi, \psi \in F(L_A)\}.$$

Επίσης τα άξιώματα που δίνουμε παρακάτω χρησιμοποιούν μόνον τους συνδέσμους $\to$ και $\neg$, και τον ποσοδείκτη $\forall$. Οι υπόλοιποι σύνδεσμοι και ο $\exists$ μπορούν να θεωρηθούν συντομογραφίες, βάσει των γνωστών λογικών ισοδυναμιών:

$$\phi \vee \psi := \neg\phi \to \psi, \quad \phi \wedge \psi := \neg(\phi \to \neg\psi), \quad (\forall x)\phi := \neg(\exists x)\neg\phi.$$

Αξιώματα του PC.
$\Pi 1 = \{\phi \to (\psi \to \phi) : \phi, \psi \in F(L_A)\}$.
$\Pi 2 = \{(\phi \to (\psi \to \sigma)) \to ((\phi \to \psi) \to (\phi \to \sigma)) : \phi, \psi, \sigma \in F(L_A)\}$.
$\Pi 3 = \{(\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi) : \phi, \psi \in F(L_A)\}$.
$\mathrm{K}1 = \{(\forall x)\phi(x) \to \phi(t) : \phi \in L_A,\ t \in T(L_A)\}$.
$\mathrm{K}2 = \{(\forall x)(\phi \to \psi) \to (\phi \to (\forall x)\psi) : \phi, \psi \in F(L_A),$ η x δεν είναι ελεύθερη στον $\phi\}$.

(Eq) Αξιώματα ισότητας. (Μ' αυτά εννοούμε όλες τις τετριμμένες ιδιότητες της σχέσης $x = y$, δηλαδή ανακλαστικότητα, συμμετρικότητα, μεταβατικότητα και αντικαταστασιμότητα: Αν $x = y$, τότε $t(x) = t(y)$ και $\phi(x) \leftrightarrow \phi(y)$, για κάθε όρο t και τύπο ϕ.)

Κανόνες Παραγωγής του PC.
1) *Modus Ponens (MP)*: Από τους τύπους ϕ και $\phi \to \psi$ παράγεται ο ψ.
2) *Κανόνας Γενίκευσης (ΚΓ)*: Από τον τύπο ϕ παράγεται ο $(\forall x)\phi$.

Συχνά για λόγους ευκολίας ταυτίζουμε το **PC** με το σύνολο των αξιωμάτων, δηλαδή

$$\mathbf{PC} = \Pi 1 \cup \Pi 2 \cup \Pi 3 \cup \mathrm{K}1 \cup \mathrm{K}2 \cup \mathrm{Eq}.$$

Ερχόμαστε τώρα στην έννοια της απόδειξης μέσα στο στο τυπικό σύστημα **PC**.

Ορισμός 6.2.1 Έστω $\Sigma \subseteq F(L_A)$ και $\phi \in F(L_A)$. *Απόδειξη του ϕ από το Σ* λέγεται κάθε πεπερασμένη ακολουθία τύπων $\phi, \ldots, \phi_n$ τέτοια ώστε $\phi_n = \phi$ και για κάθε $i = 1, \ldots, n$,

(α) είτε $\phi_i \in \Sigma$,

(β) είτε $\phi_i \in \mathbf{PC}$,

(γ) είτε ο ϕ_i παράγεται με τον MP από δύο προηγούμενους, δηλαδή υπάρχουν $j, k < i$ έτσι ώστε $\phi_k = \phi_j \to \phi_i$,

(δ) είτε παράγεται με τον ΚΓ από έναν προηγούμενο, δηλαδή $\phi_i = (\forall x)\phi_j$ για κάποιο $j < i$, με την προϋπόθεση ότι η μεταβλητή x δεν εμφανίζεται ελεύθερη στο Σ.

Λέμε ότι ο ϕ *αποδεικνύεται* ή *παράγεται από το Σ*, ή ότι είναι *θεώρημα του Σ*, και συμβολίζουμε $\Sigma \vdash \phi$, αν υπάρχει μια απόδειξη του ϕ από το Σ. Η ϕ λέγεται *λογικό θεώρημα* και συμβολίζουμε $\vdash \phi$, αν $\emptyset \vdash \phi$, δηλαδή αν η ϕ παράγεται μόνο από τα λογικά αξιώματα.

Ορισμός 6.2.2 Το Σ λέγεται *ασυνεπές* (inconsistent) ή *αντιφατικό* αν $\Sigma \vdash \bot$ (δηλαδή $\Sigma \vdash \phi \wedge \neg\phi$ για κάποιο ϕ). Αλλιώς λέγεται *συνεπές*.

Αποδεικνύεται (δες ασκήσεις) ότι για κάθε ϕ, $\bot \vdash \phi$, δηλαδή από μια αντίφαση τα πάντα αποδεικνύονται και το ίδιο συμβαίνει με κάθε ασυνεπές σύνολο. Συνεπώς ένα αντιφατικό σύνολο είναι λογικά και μαθηματικά τετριμμένο.

Η σχέση $\Sigma \vdash \phi$ είναι το συντακτικό ανάλογο της σημασιολογικής σχέσης $\Sigma \models \phi$ (του λογικού συμπεράσματος). Μάλιστα, τα θεμελιώδη θεωρήματα Ορθότητας και Πληρότητας της βασικής λογικής αποδεικνύουν την ισοσυναμία τους.

Θεώρημα 6.2.3 (Θεώρημα Ορθότητας) *Για κάθε $\Sigma \subseteq F(L_A)$ και $\phi \in F(L_A)$,*

$$\Sigma \vdash \phi \;\Rightarrow\; \Sigma \models \phi.$$

Ισοδύναμα: Αν το Σ είναι ικανοποιήσιμο (δηλαδή οι τύποι του Σ καθίστανται συγχρόνως αληθείς σε κάποια L_A-δομή M), τότε το Σ είναι συνεπές.

Απο το προηγούμενο έπεται ότι τα $Th(\mathbb{N})$ και PA είναι συνεπή σύνολα προτάσεων αφού ικανοποιούνται στη δομή $\mathbb{N}$. Πιο σημαντικό είναι το επόμενο.

Θεώρημα 6.2.4 (Θεώρημα Πληρότητας) *Για κάθε $\Sigma \subseteq F(L_A)$ και $\phi \in F(L_A)$,*

$$\Sigma \models \phi \;\Rightarrow\; \Sigma \vdash \phi.$$

Ισοδύναμα: Αν το Σ είναι συνεπές, τότε είναι ικανοποιήσιμο.

Για αποδείξεις των θεωρημάτων αυτών και άλλες λεπτομέρειες πάνω στη βασική λογική, που θα τον βοηθήσουν να δουλέψει τις ασκήσεις που δίνονται παρακάτω, αναγνώστης μπορεί να συμβουλευθεί το [10].

Ασκήσεις

6.2.1 Δείξτε ότι η σχέση $\vdash$ είναι ανακλαστική, μεταβατική και μονότονη (δηλαδή, $\Sigma \vdash \phi$ και $\Sigma \subseteq \Sigma' \Rightarrow \Sigma' \vdash \phi$.

6.2.2 Δείξτε ότι αν $\Sigma \vdash \phi$, τότε υπάρχει πεπερασμένο $\Sigma_0 \subseteq \Sigma$ τέτοιο ώστε $\Sigma_0 \vdash \phi$.

6.2.3 Δείξτε ότι αν $Con(\Sigma) = \{\phi : \Sigma \vdash \phi\}$, τότε $Con(Con(\Sigma)) = Con(\Sigma)$.

6.2.4 Δείξτε ότι $\vdash \phi$ αν και μόνον αν η ϕ είναι ταυτολογία.

6.2.5 Κάντε συντακτικά (δηλαδή χωρίς τη βοήθεια του θεωρήματος πληρότητας) τις παρακάτω αποδείξεις:
(α) $\vdash \phi \to \phi$, (β) $\{\phi \to \psi, \psi \to \sigma\} \vdash \phi \to \sigma$, (γ) $\{\phi \to (\psi \to \sigma), \psi\} \vdash \phi \to \sigma$, (δ) $\neg\neg\phi \to \phi$.

6.2.6 Δείξτε (αν είναι δυνατόν χωρίς τη βοήθεια του θεωρήματος πληρότητας) το *Θεώρημα Παραγωγής* (Deduction Theorem): Για κάθε $\Sigma \subseteq F(L_A)$ και $\phi, \psi \in F(L_A)$,

$$\Sigma \vdash \phi \to \psi \;\Leftrightarrow\; \Sigma \cup \{\phi\} \vdash \psi.$$

6.2.7 Δείξτε συντακτικα ότι: (α) $\vdash \phi \to \neg\neg\phi$, (β) $\vdash (\phi \to \psi) \to (\neg\psi \to \neg\phi)$, (γ) $\vdash (\neg\phi \to \neg\psi) \to (\psi \to \phi)$, (δ) $\vdash \phi \wedge \psi \to \psi \wedge \phi$, (ε) $\vdash \phi \wedge \psi \to \phi$, (ζ) $\vdash \phi \wedge \psi \to \psi$, (η) $\phi \to (\psi \to (\phi \wedge \psi)$, (ϑ) $\vdash \phi(\neg\phi \to \psi)$, (ι) $\bot \to \phi$ για κάθε ϕ.

6.2.8 Δείξτε τα συντακτικά ισοδύναμα όλων των βασικών λογικών ισοδυναμιών της § 3.2.

6.2.9 Δείξτε για κάθε Σ και ϕ, ότι $\Sigma \nvdash \phi$ αν και μόνον αν το $\Sigma \cup \{\neg\phi\}$ είναι συνεπές.

6.2.10 Δείξτε με τη βοήθεια του θεωρήματος πληρότητας το
Θεώρημα Συμπάγειας: Έστω Σ σύνολο τύπων. Αν κάθε πεπερασμένο υποσύνολο του Σ είναι ικανοποιήσιμο, τότε το Σ είναι ικανοποιήσιμο.

6.3 Η Θεωρία PA από πιο κοντά

''Θεωρία'' στη λογική λέγεται κάθε σύνολο προτάσεων T μιας τυπικής γλώσσας, κλειστό ως προς $\vdash$. Συχνά το σύνολο αυτό παράγεται από ένα σύνολο αξιωμάτων Σ, δηλαδή το T είναι το σύνολο των *συνεπειών ή θεωρημάτων* του Σ και αυτο το συμβολίζουμε $T = Con(\Sigma) = \{\phi : \Sigma \vdash \phi\}$. Συχνά αναφερόμαστε και στα δύο χρησιμοποιώντας το όνομα του συνόλου των αξιωμάτων, δηλαδή ''θεωρία Σ'', παρόλο που, *ως σύνολα*, τα Σ και T μπορεί να διαφέρουν σημαντικά.

Ας επανέρθουμε τώρα στη θεωρία της Peano αριθμητικής PA που ορίσαμε στην § 4.1. Σε αντιδιαστολή προς την πλήρη αριθμητική, όπου ενδιαφερόμαστε για προτάσεις ϕ για τις οποίες $\mathbb{N} \models \phi$, εδώ ενδιαφερόμαστε για προτάσεις ϕ τέτοιες ώστε $PA \vdash \phi$. Όπως είπαμε πιο πάνω με τον όρο Peano αριθμητική εννοούμε συχνά και το σύνολο $Con(PA)$ των θεωρημάτων του PA. Και αφού $\mathbb{N} \models PA$, από το Θεώρημα Ορθότητας αμέσως προκύπτει ότι

$$PA \vdash \phi \;\Rightarrow\; \mathbb{N} \models \phi. \tag{17}$$

δηλαδή $Con(PA) \subseteq Th(\mathbb{N})$. Τί πρέπει να συμβαίνει για να ισχύει το αντίστροφο της (17); Είναι εύκολο να δούμε ότι το αντίστροφο της (17) ισοδυναμεί με το να είναι η PA *πλήρης*[6].

Ορισμός 6.3.1 Ένα σύνολο προτάσεων Σ μιας τυπικής γλώσσας L λέγεται *πλήρες* (complete) αν για κάθε $\phi \in S(L)$, $\Sigma \vdash \phi$ ή $\Sigma \vdash \neg\phi$.

Προφανώς η πλήρης αριθμητική $Th(\mathbb{N})$ είναι πλήρης θεωρία. Οπότε αμέσως προκύπτει το επόμενο.

Λήμμα 6.3.2 $\mathbb{N} \models \phi \Rightarrow \; PA \vdash \phi$ *(δηλαδή* $Con(PA) = Th(\mathbb{N})$*) αν και μόνον αν η* PA *είναι πλήρης.*

Η πληρότητα μιας θεωρίας είναι μια πολύ επιθυμητή ιδιότητα - η δεύτερη πιο επιθυμητή μετά την συνέπεια. Πλήρης θεωρία σημαίνει θεωρία που δεν αφήνει ''αναπάντητα'' ερωτήματα: Για κάθε ερώτημα ϕ, έχει μια απάντηση είτε για το ϕ είτε για το $\neg\phi$ (και φυσικά μόνο για το ένα, αν είναι συνεπής). Θα δείξουμε παρακάτω ότι η PA δεν είναι πλήρης μ' έναν κάπως έμμεσο αλλά ισχυρότερο τρόπο (δηλαδή δείχνοντας κάτι περισσότερο από την μη πληρότητα), που είναι συγχρόνως μια καλή εφαρμογή των αναδρομικών και α.α. συνόλων. Συγκεκριμένα μέσα από την απόδειξη θα δούμε και το πρώτο παράδειγμα συνόλου που είναι α.α. χωρίς να είναι αναδρομικό. Στην ουσία, η διαφορά ανάμεσα σε μια πλήρη και σε μια μηπλήρη αξιωματική θεωρία, είναι η διαφορά ανάμεσα σε ένα αναδρομικό και σε ένα α.α. σύνολο.

Επειδή αναφερόμαστε σε αξιωματικές θεωρίες, ας ξεκινήσουμε από αυτό το ερώτημα που φαίνεται τετριμμένο ενώ δεν είναι: Τί ακριβώς σημαίνει ''αξιωματική'' θεωρία;. Η απάντηση μοιάζει προφανής: Όταν υπάρχει ένα σύνολο αξιωμάτων. Αλλά η ερώτηση

[6]Οι όροι ''πλήρης '' και ''πληρότητα'' στη λογική συναντώνται υπό δύο έννοιες παραπλήσιες αλλά διαφορετικές που μπορεί να προκαλέσουν σύγχιση στον νεοφώτιστο. Η μία αναφέρεται σε τυπικά συστήματα, όπως το **PC**. Πλήρες τυπικό σύστημα είναι εκείνο στο οποίο τα συντακτικά μέσα του συστήματος επαρκούν για να παράγουν όλες τις ''αλήθειες'' του συστήματος. Αυτή είναι ή σημασία με την οποία ο όρος ''πληρότητα'' χρησιμοποιείται στο Θεώρημα Πληρότητας (του τυπικού συστήματος **PC**). Η δεύτερη έννοια είναι αυτή που αναφέρεται σε ένα σύνολο προτάσεων (ορισμός 6.3.1) Σ. Αυτή είναι ή σημασία με την οποία ο όρος ''πληρότητα'' χρησιμοποιείται στα Θεωρήματα Μή Πληρότητας (της θεωρίας PA).

αυτό ακριβώς προσπαθεί να διευκρινίσει: Τί είναι αυτό που κάνει ένα σύνολο προτάσεων *σύνολο αξιωμάτων*;. Ο καθένας καταλαβαίνει ότι οι προτάσεις του PA συνιστούν ένα σύνολο αξιωμάτων, αλλά γιατί και το σύνολο $Th(N)$ δεν είναι επίσης ένα σύνολο αξιωμάτων, και γενικά κάθε σύνολο Σ. Αν κάθε σύνολο προτάσεων μπορεί να θεωρηθεί ''σύνολο αξιωμάτων'', τότε κάθε θεωρία είναι αξιωματική θεωρία και ή έννοια χάνει το νόημά της.

Αν σκεφτούμε λίγο θα καταλήξουμε ότι η μόνη ιδιότητα που οφείλει να έχει ένα σύνολο αξιωμάτων είναι η *αναγνωρισιμότητα*. Δηλαδή για να είναι το Σ, σύνολο αξιωμάτων μιας θεωρίας $T \supseteq \Sigma$, πρέπει, πέραν του να ισχύει $T = Con(\Sigma)$, να μπορεί κανείς να αναγνωρίζει με έναν συστηματικό τρόπο αν μια οποιαδήποτε πρόταση της γλώσσας ανήκει ή δεν ανήκει σ' αυτό. Όμως αν εμβαθύνουμε λίγο ακόμη θα καταλήξουμε ότι αυτή η ιδιότητα δεν είναι άλλη από την *αλγοριθμικότητα*. Πρέπει απλώς να έχουμε κάποιον ολικό αλγόριθμο με τον οποίο να αποφασίζουμε αν $\phi \in \Sigma$ ή $\phi \notin \Sigma$. Συνεπώς ένα σύνολο Σ μπορεί να θεωρηθεί σύνολο αξιωμάτων αν και μόνον αν είναι αλγοριθμικό. Βέβαια το Σ δεν είναι ακριβώς υποσύνολο του $\mathbb{N}$ (ή κάποιου $\mathbb{N}^k$), αλλά μπορεί να γίνει με *κωδικοποίηση*.

Χρησιμοποιώντας όσα ειπώθηκαν στην § 1.3 αλλά και στην § 2.7 για αλφάβητα και κωδικοποιήσεις, και θυμίζοντας ότι κάθε όρος και κάθε τύπος της L_A, είναι μια λέξη από το αλφάβητο L_A, σε κάθε όρο t και κάθε τύπο ϕ της L_A αντιστοιχεί μονοσήμαντα ένας *κώδικας* ή *αριθμός Gödel* των t και ϕ, που τον συμβολίζουμε $\lceil t \rceil$ και $\lceil \phi \rceil$ αντίστοιχα. Έτσι τα σύνολα των $T(L_A)$, $F(L_A)$, $S(L_A)$ των όρων, τύπων και προτάσεων της L_A, ''μεταφράζονται'' σε υποσύνολα του $\mathbb{N}$, τα οποία ας παραστήσουμε με $\lceil T(L_A) \rceil$, $\lceil F(L_A) \rceil$, $\lceil S(L_A) \rceil$. Δηλαδή

$$\lceil T(L_A) \rceil = \{\lceil t \rceil : t \in T(L_A)\}, \qquad \lceil F(L_A) \rceil = \{\lceil \phi \rceil : \phi \in F(L_A)\},$$

$$\lceil S(L_A) \rceil = \{\lceil \phi \rceil : t \in S(L_A)\}.$$

Γενικότερα, αν $\Sigma \subseteq F(L_A)$, θέτουμε

$$\lceil \Sigma \rceil = \{\lceil \phi \rceil : \phi \in \Sigma\}.$$

Λήμμα 6.3.3 *Τα σύνολα $\lceil T(L_A) \rceil$, $\lceil F(L_A) \rceil$, $\lceil S(L_A) \rceil$ είναι αναδρομικά υποσύνολα του $\mathbb{N}$.*

Απόδειξη. Ο ορισμός των συνόλων $T(L_A)$, $F(L_A)$, $S(L_A)$, γίνεται με αναδρομή, και η αναδρομή αυτή προφανώς μεταβιβάζεται στους κώδικες. QED

Ορισμός 6.3.4 Έστω T μια θεωρία. Η T λέγεται *αξιωματική* ή *αξιωματικοποιήσιμη* (axiomatizable), αν υπάρχει Σ τέτοιο ώστε $T = Con(\Sigma)$ και το $\lceil \Sigma \rceil$ είναι αναδρομικό. Αν το Σ αυτό είναι πεπερασμένο, η T λέγεται *πεπερασμένα αξιωματικοπόιήσιμη*.

Η T λέγεται *αλγοριθμική* (decidable) αν το $\lceil T \rceil$ είναι αναδρομικό.

Πρόταση 6.3.5 *Τα σύνολα* $\lceil PA \rceil$ *και* $\lceil \mathbf{PC} \rceil$ *είναι αναδρομικά, άρα οι θεωρίες* $Con(PA)$ *και* $Con(\mathbf{PC})$ *είναι αξιωματικές.*

Απόδειξη. Το PA αποτελείται από το PA^-, που είναι πεπερασμένο, άρα αλγοριθμικό, και το σχήμα επαγωγής $I = \{I_\phi : \phi \in F(L_A)\}$. Τώρα *κάθε* αξιωματικό σχήμα αποτελεί αλγοριθμικό σύνολο προτάσεων επειδή όλες οι προτάσεις του σχήματος ακολουθούν το ίδιο συντακτικό μοτίβο το οποίο είναι προφανώς αλγοριθμικά ελέγξιμο. Επικαλούμενοι εν ανάγκη τη Θέση του Church, προκύπτει ότι οι κώδικες τέτοιων αλγοριθμικών συνόλων αποτελούν αναδρομικά σύνολα.

Όμοια το **PC** αποτελείται από πεπερασμένο αριθμό αξιωματικών σχημάτων. QED

Εν συνεχεία θεωρούμε τις *τυπικές αποδείξεις* που κατασκευάζονται με υποθέσεις από το ένα σύνολο Σ. Θυμίζουμε ότι μια τέτοια απόδειξη είναι μια πεπερασμένη ακολουθία τύπων $p = (\phi_1, \ldots, \phi_n)$ που πληρεί τις συνθήκες του ορισμού 6.2.1. Η p αποκτά αμέσως έναν αριθμό Gödel $\lceil p \rceil$ θέτοντας

$$\lceil p \rceil = \langle \lceil \phi_1 \rceil, \ldots, \lceil \phi_n \rceil \rangle.$$

Για κάθε Σ θεωρήστε το σύνολο

$$Prf(\Sigma) = \{(\phi, p) : \text{η } p \text{ είναι απόδειξη της } \phi \text{ από το } \Sigma\}.$$

Θέτουμε

$$\lceil Prf(\Sigma) \rceil = \{(\lceil \phi \rceil, \lceil p \rceil) : (\phi, p) \in Prf(\Sigma)\}.$$

Λήμμα 6.3.6 *Αν το* $\lceil \Sigma \rceil$ *είναι αναδρομικό, το σύνολο* $\lceil Prf(\Sigma) \rceil$ *είναι επίσης αναδρομικό. Συνεπώς το* $\lceil Prf(PA) \rceil$ *είναι αναδρομικό.*

Απόδειξη. Αρκεί να παρατηρήσουμε ότι για κάθε αλγοριθμικό Σ, το $Prf(\Sigma)$ είναι αλγοριθμικό, όπου ο αλγόριθμος εμπεριέχεται στον ορισμό 6.2.1, και επειδή επί πλέον το **PC** είναι αλγοριθμικό, όπως εξηγήσαμε στην πρόταση 6.3.5. Η αλγοριθμικότητα των Σ και **PC** είναι απαραίτητη, καθώς για να δούμε αν η ακολουθία $p = (\phi_1, \ldots, \phi_n)$ είναι απόδειξη, πρέπει να ελέγξουμε για καθε ϕ_i, αν $\phi_i \in \Sigma$, ή $\phi \in \mathbf{PC}$ κλπ. Για να οδηγεί ο έλεγχος αυτός πάντα σε απάντηση, πρέπει τα Σ και **PC** να είναι αλγοριθμικά.

Απο τη Θέση του Church η αλγοριθμικότητα του $Prf(\Sigma)$ μεταφράζεται σε αναδρομικότητα του $\lceil Prf(\Sigma) \rceil$. Ο άλλος ισχυρισμός προκύπτει αμέσως απ' τον πρώτο αφού το $\lceil PA \rceil$ είναι αναδρομικό, όπως είδαμε στην 6.3.5. QED

Λήμμα 6.3.7 *Αν το* $\lceil \Sigma \rceil$ *είναι αναδρομικό, το σύνολο* $\lceil Con(\Sigma) \rceil$ *είναι α.α. Συνεπώς το* $\lceil Con(PA) \rceil$ *είναι α.α.*

Απόδειξη. Αρκεί να παρατηρήσουμε ότι $\phi \in Con(\Sigma)$ αν και μόνον αν υπάρχει απόδειξη της ϕ στο Σ. Σε επίπεδο κωδίκων αυτό γράφεται

$$n \in \lceil Con(\Sigma) \rceil \iff (\exists x)((n,x) \in \lceil Prf(\Sigma) \rceil).$$

Αφού το $\lceil Prf(\Sigma) \rceil$ είναι αναδρομικό, από την παραπάνω ισουναμία και την πρόταση 2.6.4 παίρνουμε ότι το $\lceil Con(\Sigma) \rceil$ είναι α.α. QED

Πρόταση 6.3.8 *Αν μια θεωρία T είναι αξιωματικοποιήσιμη και πλήρης, τότε είναι αλγοριθμική.*

Απόδειξη. Έστω ότι η T είναι αξιωματικοποιήσιμη, δηλαδή $T = Con(\Sigma)$, όπου Σ αλγοριθμικό, και έστω η T (ή το Σ) είναι πλήρης, δηλαδή $\Sigma \vdash \phi$ ή $\Sigma \vdash \neg\phi$ για κάθε ϕ. Αλλά τότε, αφού $T = \{\phi : \Sigma \vdash \phi\}$, θα είναι

$$-T = \{\phi : \Sigma \nvdash \phi\} = \{\phi : \Sigma \vdash \neg\phi\}.$$

Επειδή Σ αλγοριθμικό, από το 6.3.7 έπεται ότι και το T και το $-T$ είναι α.α., άρα T αλγοριθμικό. QED

Από την προηγούμενη πρόταση προκύπτει ότι αν μια θεωρία είναι αξιωματικοποιήσιμη αλλά όχι αλγοριθμική, τότε δεν είναι πλήρης. Θα δείξουμε στην επόμενη παράγραφο ότι αυτό ακριβώς συμβαίνει με την PA. Το $Con(PA)$ δεν είναι αλγοριθμικό, και άρα η PA δεν είναι πλήρης.

6.4 Περιγράψιμα σύνολα. Πρώτο θεώρημα μη πληρότητας

Υπάρχει κάτι ανάλογο των ορίσιμων συνόλων στη θεωρία PA; Τα ορίσιμα σύνολα ορίζονται στο $\mathbb{N}$ με τη βοήθεια της σχέσης $\models$. Άρα αρκεί να αντικαταστήσουμε το $\mathbb{N}$ με PA και τη σχέση $\models$ με $\vdash$, και να λάβουμε υπ' όψη ότι η PA δεν είναι κατ' ανάγκη πλήρης. Ο παρακάτω ορισμός είναι το ανάλογο του ορισμού 5.1.6.

Ορισμός 6.4.1 Ένα σύνολο $X \subseteq \mathbb{N}^k$ λέγεται *ασθενώς περιγράψιμο* (weakly representable) αν υπάρχει τύπος $\phi(x_1, \ldots, x_k)$ τέτοιος ώστε για κάθε $n_1, \ldots, n_k \in \mathbb{N}$,

$$(n_1, \ldots, n_k) \in X \;\Leftrightarrow\; PA \vdash \phi(\underline{n_1}, \ldots, \underline{n_k}).$$

Το X λέγεται *περιγράψιμο* (representable) αν επί πλέον και το $-X$ είναι ασθενώς περιγράψιμο, δηλαδή υπάρχει $\psi(x_1, \ldots, x_k)$ τέτοιος ώστε

$$(n_1, \ldots, n_k) \notin X \;\Leftrightarrow\; PA \vdash \psi(\underline{n_1}, \ldots, \underline{n_k}).$$

[Αποδεικνύεται ότι στον παραπάνω ορισμό του περιγράψιμου συνόλου, αν οι τύποι ϕ ψ είναι Σ_1, τότε μπορούμε να πάρουμε $\psi = \neg\phi$.]

Παραδειγματα

(1) Το σύνολο $\{(x, y) : x = y\}$ είναι περιγράψιμο.

Απόδειξη. Αρκεί να δείξουμε ότι

$$m = n \;\Rightarrow\; PA \vdash \underline{m} = \underline{n},$$

$$m \neq n \;\Rightarrow\; PA \vdash \underline{m} \neq \underline{n}.$$

ή ισοδύναμα,

$$m = n \;\Rightarrow\; PA \vdash S^m(\underline{0}) = S^n(\underline{0}),$$
$$m \neq n \;\Rightarrow\; PA \vdash S^m(\underline{0}) \neq S^n(\underline{0}).$$

Για την πρώτη συνεπαγωγή αυτό που έχουμε να δείξουμε είναι ότι $PA \vdash S^m(\underline{0}) = S^m(\underline{0})$. Αλλά αυτό προκύπτει απ' το ότι το $x = x$ είναι λογικό αξίωμα (του **PC**) άρα $PA \vdash t = t$ για κάθε όρο t. Για τη δεύτερη, αρκεί να δείξουμε ότι

$$m > n \;\Rightarrow\; PA \vdash S^m(\underline{0}) \neq S^n(\underline{0}).$$

Με επαγωγή στο n (επαγωγή όχι μέσα στο σύστημα PA αλλά στον ''πραγματικό κόσμο'').

Γιά $n = 0$, αρκεί να δείξουμε ότι για κάθε $m > 0$, $PA \vdash S^m(\underline{0}) \neq \underline{0}$. Αλλά αυτό προκύπτει πράγματι απ' το αξίωμα Π1 του PA, που λέει $(\forall x)(S(x) \neq \underline{0})$. Βάζοντας στη θέση του x τον όρο $S^{m-1}(\underline{0})$, έχουμε το ζητούμενο.

Έστω ότι ισχύει για $m > n$ δηλαδή $PA \vdash S^m(\underline{0}) \neq S^n(\underline{0})$, και αποδεικνύουμε για $m > n + 1$. Δηλαδή ότι αν $m > n + 1$, τότε $PA \vdash S^m(\underline{0}) \neq S^{n+1}(\underline{0})$. Τώρα από τα αξιώματα της ισότητας έχουμε ότι $PA \vdash x = y \to S(x) = S(y)$. Από δώ έπεται ότι αν $PA \vdash t = r$, τότε $PA \vdash S(t) = S(r)$, ή ισοδύναμα, αν $PA \nvdash S(t) = S(r)$, τότε $PA \nvdash t = r$. Έστω ότι $PA \nvdash S^m(\underline{0}) \neq S^{n+1}(\underline{0})$. Τότε $PA \nvdash S^{m-1}(\underline{0}) \neq S^n(\underline{0})$. Όμως αφού $m > n + 1$, είναι $m - 1 > n$, και από την υπόθεση της επαγωγής, $PA \vdash S^{m-1}(\underline{0}) \neq S^n(\underline{0})$, αντίφαση. Συνεπώς $PA \vdash S^m(\underline{0}) \neq S^{n+1}(\underline{0})$, και άρα η επαγωγή δουλεύει για κάθε n.

(2) Η πράξη $+$, δηλαδή το σύνολο $\{(x, y, z) : x + y = z\}$, είναι περιγράψιμη.

Απόδειξη.

Αρκεί να δείξουμε ότι:

(α) $m + n = k \;\Rightarrow\; PA \vdash \underline{m} + \underline{n} = \underline{k}$,

(β) $m + n \neq k \;\Rightarrow\; PA \vdash \underline{m} + \underline{n} \neq \underline{k}$,

ή ισοδύναμα

(α) $m+n=k \;\Rightarrow\; PA \vdash S^m(\underline{0}) + S^n(\underline{0}) = S^k(\underline{0})$,
(β) $m+n \neq k \;\Rightarrow\; PA \vdash S^m(\underline{0}) + S^n(\underline{0}) \neq S^k(\underline{0})$.
(α): Αρκεί να δείξω ότι για κάθε m, n,

$$PA \vdash S^m(\underline{0}) + S^n(\underline{0}) = S^{m+n}(\underline{0}).$$

Με επαγωγή στο n. Για $n=0$, έχουμε $PA \vdash S^m(\underline{0}) + \underline{0} = S^m(\underline{0})$ το οποίο ισχύει λόγω του αξιώματος Π3 του PA. Έστω ότι ισχύει για n, δηλαδή

$$PA \vdash S^m(\underline{0}) + S^n(\underline{0}) = S^{m+n}(\underline{0}).$$

Τότε

$$S^m(\underline{0}) + S^{n+1}(\underline{0}) = S^m(\underline{0}) + S(S^n(\underline{0})),$$

και από το αξίωμα Π4, το PA αποδεικνύει

$$S^m(\underline{0}) + S(S^n(\underline{0})) = S(S^m(\underline{0}) + S^n(\underline{0})),$$

άρα, λόγω της υπόθεσης της επαγωγής, το τελευταίο ισούται με $S(S^{m+n}(\underline{0})) = S^{m+n+1}(\underline{0})$, δηλαδή

$$PA \vdash S^m(\underline{0}) + S^{n+1}(\underline{0}) = S^{m+n+1}(\underline{0}).$$

(β): Αφού, όπως δείξαμε στο (α) το PA αποδεικνύει ότι $S^m(\underline{0}) + S^n(\underline{0}) = S^{m+n}(\underline{0})$, θέτοντας $m+n=l$, αρκεί να δείξουμε ότι $l \neq k \Rightarrow PA \vdash S^l(\underline{0}) \neq S^k(\underline{0})$. Αυτό όμως το δείξαμε ήδη στο παράδειγμα (1).

Ασκήσεις

6.4.1. Δείξτε ότι κάθε περιγράψιμο σύνολο είναι ορίσιμο.

6.4.2. Δείξτε ότι αν X περιγράψιμο, και το $-X$ είναι περιγράψιμο.

6.4.3. Δείξτε ότι ο πολλ/σμός, η διάταξη, η διαιρετότητα είναι περιγράψιμες πράξεις/σχέσεις.

Το κρίσιμο ερώτημα είναι: Ποιά ακριβώς από τα ορίσιμα σύνολα είναι περιγράψιμα, και ποιά ασθενώς περιγράψιμα; Το ερώτημα αυτό σχετίζεται στενά με το ερώτημα: Ποιές από τις προτάσεις που αληθεύουν στο $\mathbb{N}$ αποδεικνύονται στο PA; Είδαμε στα πιο πάνω παραδείγματα και τις ασκήσεις ότι οι βασικές πράξεις, η διάταξη κλπ, είναι περιγράψιμα. Αυτό μπορεί να γενικευτεί σχετικά εύκολα στο εξής:

Πρόταση 6.4.2 *(α) Για κάθε Σ_1 πρόταση ϕ, $\mathbb{N} \models \phi \;\Rightarrow\; PA \vdash \phi$. Δηλαδή οι Σ_1 προτάσεις είναι αληθείς αν και μόνον αν αποδεικνύονται.*
(β) Κάθε Σ_1 σύνολο είναι ασθενώς περιγράψιμο.
(γ) Κάθε Δ_1 σύνολο είναι περιγράψιμο.

Απόδειξη. (α) Με επαγωγή στο μήκος των Σ_1 προτάσεων. Δείχνουμε πρώτα τον ισχυρισμό για τις Σ_0 προτάσεις. Ουσιαστικά, τα πιο πάνω παραδείγματα και οι ασκήσεις δείχνουν ότι για οποιουσδήποτε όρους t, s, $\mathbb{N} \models t = s \;\Rightarrow\; PA \vdash t = s$, και $\mathbb{N} \models t \neq s \;\Rightarrow\; PA \vdash t \neq s$, δηλαδή ο ισχυρισμός ισχύει για ατομικές προτάσεις και τις αρνήσεις τους. Έστω ότι ισχύει για ϕ, ψ και τις αρνήσεις τους. Τότε εύκολα βλέπουμε ότι θα ισχύει για $\phi \wedge \psi$, $\phi \vee \psi$ και τις αρνήσεις τους. Πράγματι, έστω $\mathbb{N} \models \phi \wedge \psi$. Τότε $\mathbb{N} \models \phi$ και $\mathbb{N} \models \phi$. Από την υπόθεση της επαγωγής, $PA \vdash \phi$ και $PA \vdash \psi$, άρα $PA \vdash \phi \wedge \psi$. Αν τώρα $\mathbb{N} \models \neg(\phi \wedge \psi)$, δηλαδή $\mathbb{N} \models \neg\phi \vee \neg\psi$, τότε $\mathbb{N} \models \neg\phi$ ή $\mathbb{N} \models \neg\psi$, άρα από την υπόθεση της επαγωγής $PA \vdash \neg\phi$ ή $PA \vdash \neg\psi$, και άρα $PA \vdash \neg(\phi \wedge \psi)$ (από τις στοιχειώδεις ιδιότητες του $\vdash$). Έστω τώρα ότι ισχύει ο ισχυρισμός για τη ϕ, και δείχνουμε ότι ισχύει για $(\forall x < \underline{n})\phi(x)$ και $(\exists x < \underline{n})\phi(x)$. Έστω $\mathbb{N} \models (\forall x < \underline{n})\phi(x)$. Αυτό ισοδυναμεί με $\mathbb{N} \models \bigwedge_{k<n} \phi(\underline{k})$. Από την υπόθεση της επαγωγής $PA \vdash \bigwedge_{k<n} \phi(\underline{k})$, απ' όπου με επαγωγή $PA \vdash (\forall x < \underline{n})\phi(x)$. Όμοια για την άρνηση αυτής και για τον φραγμένο ποσοδείκτη $\exists x < \underline{n}$. Αυτό αποδεικνύει τον ισχυρισμό για κάθε Σ_0 πρόταση. Τώρα έστω ϕ μια Σ_1 πρόταση. Αυτή είναι της μορφής $(\exists \overline{x})\phi(\overline{x})$, όπου η ϕ είναι Σ_0. Έστω $\mathbb{N} \models (\exists \overline{x})\phi(\overline{x})$. Τότε $\mathbb{N} \models \phi(\underline{n_1}, \ldots, \underline{n_k})$, για κάποια $n_1, \ldots, n_n \in \mathbb{N}$. Αφού ο $\phi(\underline{n_1}, \ldots, \underline{n_k})$ είναι Σ_0, $PA \vdash \phi(\underline{n_1}, \ldots, \underline{n_k})$. Οπότε από τις ιδιότητες της $\vdash$, $PA \vdash (\exists \overline{x})\phi(\overline{x})$. Αυτό ολοκληρώνει την απόδειξη του ισχυρισμού.

(β) Έστω X ένα Σ_1 υποσύνολο του $\mathbb{N}^k$, και έστω $\phi(\overline{x})$ ο Σ_1 τύπος που το ορίζει. Τότε από το (α) θα έχουμε, για κάθε $n_1, \ldots, n_k \in \mathbb{N}$,

$$(n_1, \ldots, n_k) \in X \;\Leftrightarrow\; \mathbb{N} \models \phi(\underline{n_1}, \ldots, \underline{n_k}) \;\Leftrightarrow\; PA \vdash \phi(\underline{n_1}, \ldots, \underline{n_k}).$$

Αυτό δείχνει ότι το X είναι ασθενώς περιγράψιμο.

(γ) Έστω X ένα Δ_1 υποσύνολο του $\mathbb{N}^k$. Τότε τα X και $-X$ ορίζονται με Σ_1 τύπους ϕ, ψ, αντίστοιχα στο $\mathbb{N}$. Άρα από το (β) είναι περιγράψιμα και συνεπώς το X είναι περιγράψιμο. QED

Πρόταση 6.4.3 *(α) Κάθε α.α σύνολο είναι ασθενώς περιγράψιμο.*
(β) Κάθε αναδρομικό σύνολο είναι περιγράψιμο.

Απόδειξη. Από το θεώρημα 5.3.6, τα α.α. και τα Σ_1 σύνολα ταυτίζονται, όπως επίσης και τα αναδρομικά με τα Δ_1. Άρα το πόρισμα προκύπτει αμέσως από την 6.4.2 (β). QED

Το αντίστροφο του προηγουμένου ισχύει επίσης.

Πρόταση 6.4.4 *(α) Κάθε ασθενώς περιγράψιμο σύνολο είναι α.α.*
(β) Κάθε περιγράψιμο σύνολο είναι αναδρομικό.

Απόδειξη. Έστω ότι το X είναι ασθενώς περιγράψιμο. Τότε για κάποιον τύπο $\phi(\overline{x})$,

$$(n_1, \ldots, n_k) \in X \iff PA \vdash \phi(\underline{n_1}, \ldots, \underline{n_k}).$$

Όμως έχουμε δει στην προηγούμενη παράγραφο 4.3 ότι για κάθε τύπο ϕ,

$$PA \vdash \phi \iff (\exists x)((\ulcorner \phi \urcorner, x) \in \ulcorner Prf(PA) \urcorner),$$

και ότι το $\ulcorner Prf(PA) \urcorner$ είναι αναδρομικό σύνολο. Συνδυάζοντας τις δύο προηγούμενες παίρνουμε ότι

$$(n_1, \ldots, n_k) \in X \iff (\exists x)((\ulcorner \phi(\underline{n_1}, \ldots, \underline{n_k}) \urcorner, x) \in \ulcorner Prf(PA) \urcorner).$$

Αλλά η δεξιά σχέση προφανώς ορίζει ένα α.α. σύνολο.

(β) Έστω X είναι περιγράψιμο. Τότε τα X, $-X$ είναι ασθενώς περιγράψιμα, άρα α.α. από το (α), και συνεπώς το X είναι αναδρομικό. QED

Από τις προτάσεις 6.4.3 και 6.4.4 παίρνουμε ότι

Θεώρημα 6.4.5 *(α) Ένα σύνολο είναι ασθενώς περιγράψιμο αν και μόνον αν είναι α.α.*

(β) Ένα σύνολο είναι περιγράψιμο αν και μόνον αν είναι αναδρομικό.

Συνοψίζοντας τους χαρακτηρισμούς των αναδρομικών και α.α. συνόλων που δίνει το τελευταίο και το θεώρημα 5.3.6, έχουμε:

$$\text{αναδρομικά σύνολα } = \Delta_1 = \text{ περιγράψιμα},$$

$$\text{αναδρομικά απαριθμήσιμα } = \Sigma_1 = \text{ ασθενώς περιγράψιμα}.$$

Έχουμε δει (ότι λήμμα 6.3.7) ότι το $Con(PA)$ είναι α.α. σύνολο. Όμως το επόμενο είναι πολύ σημαντικότερο.

Θεώρημα 6.4.6 (A. Church) *Το σύνολο $Con(PA)$ δεν είναι αλγοριθμικό.*

Απόδειξη. Η απόδειξη είναι ένα κλασσικό διαγώνιο επιχείρημα. Για κάθε τύπο $\phi(x)$, ας γράψουμε $\phi = \phi_n$ αν $\ulcorner \phi \urcorner = n$. (Δηλαδή αριθμούμε τους τύπους με τους αριθμούς Gödel.) Ας υποθέσουμε ότι το $Con(PA)$ είναι αλγοριθμικό, δηλαδή ότι το $\ulcorner Con(PA) \urcorner$ είναι αναδρομικό. Έστω

$$M = \{(m, n) : \ulcorner \phi_m(n)) \urcorner \notin \ulcorner Con(PA) \urcorner\},$$

και έστω

$$K = \{m : (m, m) \in M\}.$$

Αφού το $\lceil Con(PA) \rceil$ είναι αναδρομικό, το ίδιο θα είναι και τα σύνολα M και K. Άρα το K είναι περιγράψιμο σύμφωνα με τους πιο πάνω χαρακτηρισμούς. Έστω $\theta(x)$ τύπος που περιγράφει (ασθενώς) το K στο PA, δηλαδή

$$n \in K \iff PA \vdash \theta(\underline{n}).$$

Έστω $\lceil \theta(x) \rceil = c$. Αυτό σημαίνει $\theta(x) = \phi_c(x)$, και η προηγούμενη γράφεται

$$n \in K \iff PA \vdash \phi_c(\underline{n}).$$

Ειδικά για $n = c$ θα πάρουμε

$$c \in K \iff PA \vdash \phi_c(\underline{c}). \tag{18}$$

Από την άλλη μεριά, από τον ορισμό του K,

$$c \in K \Leftrightarrow (c, c) \in M \Leftrightarrow \lceil \phi_c(c)) \rceil \notin \lceil Con(PA) \rceil \Leftrightarrow PA \nvdash \phi_c(c). \tag{19}$$

Από τις (18) και (19) παίρνουμε αντίφαση που αποδεικνύει το θεώρημα. QED

Θεώρημα 6.4.7 (Πρώτο Θεώρημα μηΠληρότητας) *Η θεωρία PA δεν είναι πλήρης, δηλαδή υπάρχει $\phi \in S(L_A)$ τέτοια ώστε $PA \nvdash \phi$ και $PA \nvdash \neg\phi$.*

Απόδειξη. Η θεωρία $Con(PA)$ είναι αξιωματική. Αν ήταν πλήρης θα ήταν αλγοριθμική, λόγω της 6.3.8. Όμως δεν είναι λόγω του προηγουμένου θεωρήματος. QED

Πόρισμα 6.4.8 *Υπάρχει σύνολο α.α. αλλά όχι αναδρομικό.*

Απόδειξη. Το $Con(PA)$ είναι τέτοιο. QED

Το θεώρημα μη πληρότητας προκάλεσε έκπληξη όταν εμφανίστηκε, αλλά και εξακολουθεί να εκπλήσσει: Αν το PA αφήνει αναπάντητα ερωτήματα, αυτό σημαίνει ότι κάτι λείπει από τα αξιώματά του. Όμως τι θα μπορούσε να είναι αυτή η ιδιότητα των πράξεων $+, \cdot, S$ που ξεχάσαμε να συμπεριλάβουμε; Κανείς δεν έχει μια απάντηση σ' αυτό. Αλλά ας υποθέσουμε ότι κάποιος βρίσκει πράγματι ένα νέο αξίωμα που είναι εύλογο και δεν προκύπτει από τα υπάρχοντα. Μπορεί να ελπίζει πως αν το προσθέσει στα αξιώματα του PA, το νέο σύστημα θα γίνει πλήρες; Η απάντηση είναι όχι! Διότι το θεώρημα μη πληρότητας δεν είναι ένα μεμονωμένο φαινόμενο που αφορά απλώς το σύστημα PA, αλλά ισχύει *για κάθε θεωρία που επεκτείνει την PA*. Πράγματι, ισχύει το εξής γενικότερο:

Θεώρημα 6.4.9 *Έστω T μια αξιωματικοιήσιμη θεωρία σε μια γλώσσα $L \supseteq L_A$, με σύνολο αξιωμάτων $\Sigma \supseteq PA$ (ή γενικότερα $Con(\Sigma) \supseteq Con(PA)$). Τότε υπάρχει $\phi \in S(L)$ τέτοια ώστε $T \nvdash \phi$ και $T \nvdash \neg\phi$.*

Απόδειξη. Η απόδειξη είναι ακριβώς ίδια μ' εκείνη του θεωρήματος 6.4.7, αντικαθιστώντας απλώς το PA με το Σ. Επειδή $Con(\Sigma) \supseteq Con(PA)$, μέσα στην T διαθέτουμε όλο το μηχανισμό κωδικοποίησης που οδηγεί στα σύνολα $\lceil\Sigma\rceil$, $\lceil Prf(\Sigma)\rceil$ κλπ, τα οποία είναι αναδρομικά υποσύνολα του $\mathbb{N}$. Στη θέση των περιγράψιμων συνόλων έχουμε τώρα τα Σ-περιγράψιμα, και η απόδειξη του 6.4.7 μεταφράζεται στο ότι το σύνολο $Con(\Sigma)$ δεν είναι αλγοριθμικό. Άρα από το 6.3.8, η T δεν είναι πλήρης. QED

Από το προηγούμενο προκύπτει ότι όσα νέα αξιώματα η αξιωματικά σχήματα και να προσθέσουμε στο PA, η μη πληρότητα θα είναι παρούσα, σαν μια έμφυτη εσωτερική ατέλεια όλων των αξιωματικών συστημάτων που περιέχουν ως τμήμα τους τη βασική θεωρία αριθμών. Όσο για την αιτία αυτής της ατέλειας, μπορεί κανείς να την αναζητήσει όχι σε μεταφυσικούς λόγους, αλλά απλώς στην μη αναμενόμενη (μέχρι την απόδειξη του θεωρήματος) ικανότητα των φυσικών αριθμών να *κωδικοποιούν*, δηλαδή να αναπαριστούν με ακρίβεια γλωσσικά φαινόμενα, και άρα να ''μιλούν για τον εαυτό τους''.

6.5 Η αλήθεια (στο $\mathbb{N}$) δεν ορίζεται

Είδαμε στην προηγούμενη παράγραφο ότι η θεωρία της Peano αριθμητικής $Con(PA)$ είναι ένα Σ_1-ορίσιμο σύνολο, δηλαδή όχι απλώς ορίσιμο αλλά και με έναν τύπο σχετικά πολύ απλό (Σ_1). Είναι φυσικό να ρωτήσουμε τι συμβαίνει με την θεωρία της πλήρους αριθμητικής $Th(\mathbb{N})$. Είναι το σύνολο $Th(\mathbb{N})$ ορίσιμο; Ο A. Tarski έδειξε το 1931 ότι το $Th(\mathbb{N})$ δεν είναι ορίσιμο. Αφού το $Th(\mathbb{N})$ περιέχει ακριβώς τις αληθείς προτάσεις της γλώσσας, L_A, το γεγονός αυτό το εκφράζουμε λέγοντας ότι ''η αλήθεια στο $\mathbb{N}$ δεν είναι ορίσιμη''.

Θεώρημα 6.5.1 (Tarski 1931) *Το σύνολο $Th(\mathbb{N})$ δεν είναι ορίσιμο.*

Απόδειξη. Πρόκειται για ένα ακόμα κλασσικό διαχώνιο επιχείρημα. Άς συμβολίσουμε πάλι με ϕ_n έναν τύπο ϕ της γλώσσας L_A, αν $\lceil\phi\rceil = n$. Και ας θέσουμε $\psi_n = \phi_n(\underline{n})$. Αν το $Th(\mathbb{N})$ είναι ορίσιμο, τότε και το υποσύνολό του $X = \{\psi_n : \mathbb{N} \models \psi_n\}$ είναι ορίσιμο, έστω με τον τύπο $\sigma(x)$. Δηλαδή για κάθε n,

$$\mathbb{N} \models \sigma(\underline{n}) \iff n \in X \iff \mathbb{N} \models \psi_n. \tag{20}$$

Έστω $m = \lceil\neg\sigma(x)\rceil$. Απο την (20),

$$\mathbb{N} \models \psi_m \iff \mathbb{N} \models \sigma(\underline{m}).$$

Όμως από τον ορισμό του m, $\psi_m = \neg\sigma(\underline{m})$ και συνεπώς

$$\mathbb{N} \models \psi_m \iff \mathbb{N} \models \neg\sigma(\underline{m}).$$

Οι δύο τελευταίες δίνουν αντίφαση, που αποδεικνύει το θεώρημα. QED

Αναφορές

[1] George Boolos, *The logic of provability*, Cambridge U.P., 1993.

[2] Douglas S. Bridges, *Computability*, Springer-Verlag, 1994.

[3] Daniel Cohen, *Computability and Logic*, Ellis Horwood Limited, 1987.

[4] R. Epstein and W. Carnielli, *Computability, computable functions, logic, and the foundations of Mathematics*, Wadsworth and Brooks/Cole, Pacific Grove, California 1989.

[5] R. Kay, *Models of Peano Arithmetic*, Oxford Logic Guides, 1991.

[6] P. Kůrka, On topological dynamics of Turing machines, *Theoret. Comp. Sci.* **174** (1997), 203-216.

[7] P. Odifreddi, *Classical recursion theory*, North Holland P.C. 1992.

[8] C. Papadimitriou, *Computational Complexity*, Addison- Wesley P.C. 1994.

[9] Hartley Rogers, *Theory of recursive functions and effective computability*, McGraw-Hill, 1967.

[10] Αθ. Τζουβάρας, *Στοιχεία Μαθηματικής Λογικής*, Εκδόσεις Ζήτη, Θεσσαλονίκη 1986.

[11] Γιώργος Τουρλάκης *Εισαγωγή στην Υπολογιστική*, Πανεπ. Εκδόσεις Κρήτης, 1994.