Linear-fractional Function, Elliptic Curves, and Parameterized Jacket Matrices

Moon Ho Lee
moonho@chonbuk.ac.kr
and
Veselin Vladislavov Vavrek
veselin@chonbuk.ac.kr

Institute of Information and Communication
Chonbuk National University
Jeonju 561-756, Korea

Contents

1 Introduction and Preliminaries

This technical report presented here is the next steps of research started in [21]. The main considered objects are linear-fractional functions (l.f.f.). One of the aims of this report is not only to present the (new) results, but also to show the logic of l.f.f., and to show the areas, where they can be used.

In this paper we shall study some properties of elliptic curves, and parameterized Jacket matrices. The main instrument to explore this object is linear fractional function (l.f.f.). These functions have really interesting properties. On the other hand while studding parameterized Jacket matrices we also study l.f.f. functions. So in particular, Jacket matrices are related to the elliptic curve, and so to elliptic curve cryptography.

Interesting topics studied in this paper are

1. Demonstrate an implementation of Williams $p+1$ algorithm, using l.f.f.. - We shall demonstrate that iteration of l.f.f. acts as multiplication over one special group. Using this we shall show, how to factorize the number $n = pq$, where p and q are primes, if we know, that $p+1$ has only prime divisors with small value (for example ≤ 10000). This result is presented in Section 2.3.

2. One trick about elliptic curves. - We shall demonstrate how the linear-fractional function can be used to find a correspondence between GF(p) points of two elliptic curves. This result is presented in Section 4.4, and its subsections.

3. Paley complex Hadamard Conference matrices. - Paley Conference matrices are well known, and will be introduce here in introduction. Next we shall show, that these matrices can be generalized to contain a p roots of unity (p prime), and also that they can be obtained - applying equivalence operations - from matrices generated using-second order recurrences (i.e. similar to Fibonacci sequences). This result is presented in Section 5.1.1.

4. Some generalizations of Paley construction II. - If the reader knows Paley construction II there is noting to say more - we only generalize. The essential part of construction is that it produces Jacket matrices, combining two small (special type of) matrices. This result is presented in Section 5.1.2 and Section 5.2.1.

5. Construction of parameterized Jacket matrices. - As noted in introduction, parameterized Jacket matrices can be used to study l.f.f.. Using tensor (or Kronecker) product we can construct such matrices. We shall demonstrate one other non-trivial construction. This result is presented in Section 5.2.1.

Also there are some row, but interesting ideas (i.e. it is proved almost noting up to know, but the idea exists).

1. Is there infinite many prime Fibonacci numbers? - The next idea is not new, but similarly as Williams $p+1$ method the form of explanation is essential. So the question is still open. Using only main properties of action of linear-fractional function in finite field we reformulate the question to study the length of cycles in projective closure of finite field.

2. Considering algeraic-combinatorial sets. - Special M-step operation has been introduced, which acts on subset of square matrices. Using this operation and space we plain to construct large integer factorization algorithm (similarly as William's $p+1$ or Pollard's $p-1$ algorithms). The idea is presented in Section 3, and its subsections.

3. Attack the conjecture, that does not exists circulant Hadamard matrix of order bigger than 4. In other word conjecture can be explained as that Jacket equations for circulant Jacket matrix

has not ± 1 solution. So we looking for connection between Jacket equation and anther one set of equations, which can be studied easily. We found some equations, obtained recursively, and hope that using invariant theory we can succeed. The idea is presented in Section 5.3, and its subsections.

In the text we shall use some known, but complicated objects, which is better to define preliminary. Such are Paley Conference matrices and projective closure of the field $\mathrm{GF}(p)$.

1.1 Paley Conference Matrices

Paley Conference matrices are closely related with l.f.f.. In Section 2.2 we shall demonstrate something more about this conection. In Section 5.1.1. we also study a properties of this matrices.

If we select a finite field $GF(p)$, and write its elements as $c_1, c_2, \ldots, c_p$, then a Paley Conference matrix $A = (a_{i,j})_{i,j=1}^{p+1}$ is defined as follow.

$$a_{i,j} = \begin{cases} 0, & i = j; \\ 1, & i = 1, j \neq 1; \\ 1, & j = 1, i \neq 1; \\ \chi_2(c_{i-1} - c_{j-1}), & \text{otherwise.} \end{cases}, \quad \text{where } \chi_2(x) := \begin{cases} 0, & x = 0; \\ +1, & \exists y \in GF(p) : y^2 = x; \\ -1, & \text{otherwise;} \end{cases}. \tag{1}$$

Here we shall call the function χ_2 a quadratic character. We shall use this next, in lot of places, not only for Paley Conference matrices.

Main property of this matrix is that it is orthogonal. First row is orthogonal to all other rows, since $\sum_{x \in \mathrm{GF}(p)} \chi_2(x) = 0$.

Now we shall prove, that any two other rows u and v are orthogonal. It is easy to show, that

$$S_i := \sum_{x \in \mathrm{GF}(p)} x^i = \begin{cases} p, & i \equiv 0 \pmod p; \\ 0, & i \not\equiv 0 \pmod p. \end{cases}, \tag{2}$$

using substitute $x \to \lambda x$. Thus $S_i = \lambda^i S_i$. Also we use Euler criteria, i.e. that

$$x^{\frac{p-1}{1}} \equiv \binom{x}{p} \pmod p. \tag{3}$$

So

$$\sum_{x \in \mathrm{GF}(p)} \chi_2((x-u)(x-v)) = \sum_{x \in \mathrm{GF}(p) \setminus \{0\}} ((x-u)(x-v))^{\frac{p-1}{2}} = \sum x^p + \text{lower degrees} = p - 1.$$

So using that in first column of Paley matrix we have ones, we prove orthogonality of these rows.

1.2 Projective Closure of $\mathrm{GF}(p)$

Usually projective closure is considered as geometric operation, and it is applied to elements of linear space. In this paper we dont want general definition, because our vector space will be one dimensional, and over the finite field $\mathrm{GF}(p)$. Next we shall give two different definitions. They give us different objects, but they are equivalent (in algebraic point of view).

First definition is simply to consider ∞, as additional element. So we can also define that $\frac{1}{0} = \infty$, and $\frac{1}{\infty} = 0$. Next for any element s in the field $s + \infty = \infty$, and if s is non-zero $s\infty = \infty$.

All definitions in above are not meaningless. Aim is to make linear fractional function

$$x \to \frac{ax + b}{cx + d}$$

one to one correspondence. As we can see later this is essential for our next consideration.

Not everything seems OK, since we must prove, that our definitions

$$\frac{1}{0} = \infty,\ \frac{1}{\infty} = 0,\ s + \infty = \infty,\ s^*\infty = \infty.$$

satisfies algebraic laws, like associative, distributive etc. For example obviously $\frac{1}{1-\frac{1}{1-x}} = 1 - \frac{1}{x}$, but if we select $x = \infty$ would be satisfied?

Next we shall demonstrate one another construction of projective closure. It is not so intuitive, but with it we would not have the problems, like explained above.

Consider the set

$$g_{a,b} \subset (\mathrm{GF}(p) \times \mathrm{GF}(p)),\ g_{a,b} := (a, b).\,(\mathrm{GF}(p))^*.$$

So projective closure is defined as

$$F := \{g_{a,b} \,|\, a \neq 0 \text{ or } b \neq 0\}.$$

Obviously if $\lambda \in GF(p),\ \lambda \neq 0$, then $g_{a,b} = g_{\lambda a, \lambda b}$. So we can consider F, as set which contain only element of the forms $g_{a,1}$ or $g_{1,0}$. A map of elements, presented here, and in previous definition is as follow

$$a \in \mathrm{GF}(p):\ a \leftrightarrow g_{a,1} \text{ and } \infty \leftrightarrow g_{1,0}.$$

Even if we can not define multiplication of elements, this definition has some advantages, which we shall see in next sections.

In the next if we use first definition we shall write $GF(p) \cup \{\infty\}$, while for the second we shall use $\overline{GF(p)}$.

2 Linear-fractional Function

The main object, which we shall research in this paper, is linear-fractional function, or linear-fractional transformation. In next section we shall demonstrate the main properties, while in Sections 2.2 we shall explain some (external) results, which we shall use in other places in this paper.

In [21] it is shown, that an acting of linear-fractional function over finite field $\mathrm{GF}(p)$ has the following property. Let select non-fixed point, i.e. an element from $\mathrm{GF}(p)$ which image on considered l.f.f. is not the same element. If we start to apply consistently this l.f.f. then the size of obtained cycle does not depend on the selected start point. Also it is shown, that if there is fixed points (it is possible to has not), they are exactly 2.

Section 2.3 contains one interesting demonstration. How l.f.f. can be used in explanation of Williams $(p+1)$ algorithm [20]. This is an algorithm, which factor the number n, if we know that n has a prime devisor p, such that $p+1$ have only prime factors of small value (for example ≤ 10000).

2.1 Main Properties

Linear-fractional transformation has one very important property. It maps the points of projective closure of the field $(\mathrm{GF}(p) \cup \{\infty\})$ with himself, and this map is one to one correspondence. Prove this is almost trivial. Let

$$y = \frac{x+a}{x+b},$$

and next we calculate

$$(x+b)y = x+a \Rightarrow x(y+1) = a - by \Rightarrow x = \frac{a-by}{y-1}.$$

Suppose the map is not one to one, we can conclude

$$\frac{x_1+a}{x_1+b} = y = \frac{x_2+a}{x_2+b}, x_1 \neq x_2 \Rightarrow x_1 = \frac{a-by}{y-1} = x_2.$$

This is obviously contradiction. In above presented calculations, we must also consider a case, when denominator become 0 (and so obtain ∞), or x_1 or x_2 is ∞.

L.f.f. seems better, if we consider the second definition of projective closure of the $\mathrm{GF}(p)$, i.e.

$$\overline{\mathrm{GF}(p)} := \left\{(a,b).\left(\mathrm{GF}(p)\right)^* \subset \left(\mathrm{GF}(p) \times \mathrm{GF}(p)\right) \mid a \neq 0 \text{ or } b \neq 0\right\}$$

Remember, that maping of $\mathrm{GF}(p) \cup \{\infty\}$ to $\overline{\mathrm{GF}(p)}$ is defined as follow. Every $x \in \mathrm{GF}(p)$ go to $(x,1).(\mathrm{GF}(p))^* \in \overline{\mathrm{GF}(p)}$, and $\infty \to (1,0).(\mathrm{GF}(p))^*$. So

$$\text{If } x \to \frac{ax+b}{cx+d} \text{ then } (x,1).\left(GF(p)\right)^* \to \left(\frac{ax+b}{cx+d},1\right).\left(GF(p)\right)^* \equiv$$

$$\equiv (ax+b, cx+d).\left(GF(p)\right)^*.$$

We can present more clearly this map, if we write couples $(a,b).(\mathrm{GF}(p))^* \in \overline{\mathrm{GF}(p)}$ in vertical notation, and omit $(\mathrm{GF}(p))^*$ factor.

$$\begin{pmatrix} x \\ 1 \end{pmatrix} \to \begin{pmatrix} ax+b \\ cx+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix}$$

We see, that l.f.f. acts as linear operator. Of course ones again we must consider the case, when $cx + d = 0$, or $x = \infty$.

Last essential property of l.f.f. is that composition of two (different) l.f.f. is still l.f.f. This can be checked directly, but it is consequence of presented above, i.e. that l.f.f. acts as linear operator.

2.2 Action over finite field

In introduction we note, that the main stufy of this paper is l.f.f., and can be considered as continuation of [21]. That is why we shall present some results of [21], which we shall use in this paper.

Consider some prime p, and projective closure of this field $\mathrm{GF}(p) \cup \{\infty\}$. Select $\alpha \in \mathrm{GF}(p) \backslash \{4\}$ and define the function

$$\phi_\alpha(x) := \frac{1}{1 - x/\alpha};$$
$$f_{i+1}(\alpha) := \alpha(f_i(\alpha) - f_{i-1}(\alpha)),$$

and denote

$$\phi_\alpha^{[i]}(x) := \underbrace{\phi_\alpha(\phi_\alpha(\dots \phi_\alpha(}_{i} x)) \dots).$$

The following proposition hold

Proposition 1.

1. $\forall x \in \mathrm{GF}(p) : \phi_\alpha^{[i]}(x) = x \Leftrightarrow f_w(\alpha) = 0$;
2. *Let* $c \in \mathrm{GF}(p^2)$, *then* $f_w(c + 1/c + 2) = 0 \Leftrightarrow |\langle c \rangle| \Big| w$.
3. *Let* $c \in \mathrm{GF}(p^2)$, *then* $c + 1/c + 2 \in \mathrm{GF}(p) \Leftrightarrow c^{p+1} = 1$ or $c^{p-1} = 1$.

Here we consider $\mathrm{GF}(p^2)$ as quadratic extension of $\mathrm{GF}(p)$. From this proposition it follows, that function ϕ_α induces a cycles of the same lengths in $\mathrm{GF}(p) \cup \{\infty\}$, and that the length divide $p + 1$, or $p - 1$. Also it is possible to have a 2 fixed points.

Using Proposition 1 we can study existence of nega-circulant form of Paley Conference matrices. This have been proved in [4].

One interesting demonstration of presented above properties is a proof of quadratic reciprocity law. More interesting is not the result, while the following comparison:

$$\left(\frac{-1}{q}\right) q = (-1)^{\frac{q-1}{2}} q = \prod_{i=1}^{\frac{q-1}{2}} \left(\zeta^i - \frac{1}{\zeta^i}\right); \tag{4}$$

$$\zeta^i - \frac{1}{\zeta^i} \in K' \Leftrightarrow \left(\frac{\left(\zeta^i - \frac{1}{\zeta^i}\right)^2}{K'}\right) \Leftrightarrow \left(\frac{p}{q}\right) = 1, \tag{5}$$

and

$$\left(\frac{-1}{q}\right) q = \left(\sum_{\left(\frac{i}{p}\right)=1} (\zeta^2)^i - \sum_{\left(\frac{i}{p}\right)=-1} (\zeta^2)^i\right)^2; \tag{6}$$

$$\sum_{\left(\frac{i}{p}\right)=1} (\zeta^2)^i, \sum_{\left(\frac{i}{p}\right)=-1} (\zeta^2)^i \in \mathrm{GF}(p) \Leftrightarrow \left(\frac{p}{q}\right) = 1. \tag{7}$$

Here ζ is a primitive $(2q)^{\text{th}}$ root of 1 in suitable extension of GF(p), while K' is specific extension of GF(p), which definition we shall omit.

The key equations, of noted above proof of quadratic reciprocity law, are (4) and (5), while (6) and (7) are key equations of one another algebraic proof (probably the smaller one). Equation (4) and (6) are often a start point of proofs of the problem, known as "determine the sign of Gauss sum".

Next we shall present one idea concerning prime Fibonacci numbers. It is not known are they infinitely many. We can study prime Fibonacci numbers, as follow. Consider linear-fractional function ϕ_α and it induce cycles of length s. We know that this number is the order of element a, which is satisfied with

$$\alpha = a + 2 + \frac{1}{a}. \tag{8}$$

If a is selected such that $\alpha = -1$, then polynomials $\{(-1)^i f_i(-1)\}$ will be Fibonacci sequence. By Proposition 1 we know that $f_s(-1) = 0$ in GF(p) which means that $f_s(-1)$ is divisible by p. Also by Proposition 1, we have that $|\langle a\rangle| = s$.

Now we can present the idea. We want to "test" is a prime p a Fibonacci number. If

$$a = \frac{-3 \pm \sqrt{5}}{2} \tag{9}$$

then $\alpha = 1$ in (8). So $f_{|\langle a\rangle|}(0)$ is smaller Fibonacci number, which is divided by p. If $|\langle a\rangle|$ is so small that $\left(\frac{1+\sqrt{5}}{2}\right)^{|\langle a\rangle|} + 1 < 2p$ then it follows, that $f_{|\langle a\rangle|}(0) = p$, i.e. p is prime Fibonacci number.

Our next task is to find good presentation of degrees of a. Opening the brackets of we obtain

$$a^i = \left(\frac{-3 \pm \sqrt{5}}{2}\right)^i = (s_i/2^i) + \sqrt{5}(t_i/2^i),$$

where s_i and t_i are integers. So

$$a^{i+1} = ((s_i/2^i) + \sqrt{5}(t_i/2^i))((-3/2) + \sqrt{5}(1/2)) = ((-3s_i + 5t_i)/2^{i+1}) + \sqrt{5}((-3t_i + s_i)/2^{i+1}).$$

If we present values s_i and t_i as vector, then multiplication by a can be presented in matrix form as follow

$$\begin{pmatrix} -3/2 & 5/2 \\ 1/2 & -3/2 \end{pmatrix} \begin{pmatrix} s_i/2^i \\ t_i/2^i \end{pmatrix} = \begin{pmatrix} s_{i+1}/2^{i+1} \\ t_{i+1}/2^{i+1} \end{pmatrix}.$$

As shown in [21] we can modify the above matrix (applying substitution $y = ax + b$) to the form corresponding to studied linear-fractional function in [21]. So instead of studying order of a we can again study the length of cycles induces by linear-fractional function.

Explained above idea can be used to reformulate considered problem. Is there infinite number of primes p, such that the order of element a in (9) to be enough small. Next we can study asymptotic properties. Similarly to Dirichlet theorem it is good also to find some algebraic properties. As first step we can try to find the rule, when (9) is quadratic residue. In [21] it is shown that rule, when $\frac{-5+\sqrt{5}}{2}$ is quadratic residue, and probably we can do something similar in our case. So this first task seems feasible.

Note that this method is not universal one. So we can not attack even Lucas numbers for primarily, since in this case the length of cycle is not required to be small. Lucas numbers not start from 0, which is the beginning of cycle in Fibonacci case. Also in Lucas case it is not know, even if the cycle pass trough 0.

2.3 Williams p+1 algorithm

Pollard's $p-1$ algorithm [12] give as a method to factor the composite integer n, if one of prime factors p is such that $p-1$ has only prime divisors of small value - for example ≤ 10000. The idea of this algorithm is, based on Fermat's little theorem

$$x^{p-1} \equiv 1 (\text{mod } p).$$

This is satisfied for all co-prime to n integers x. So $(x^{p-1} - 1 \bmod n)$ is divided by p. If this integer is not 0, we conclude that $\gcd(x^{p-1} - 1 \bmod n, n)$ is non-trivial divisor of n. Calculation of great common divisor can be applyed effectively using Euclidean algorithm, and so we can factor n.

The same method works, if we can calculate $(x^{(p-1)S} - 1 \bmod n)$ instead of $(x^{p-1} \bmod n)$, for some integers S. To find such integer let first calculate all possible prime divisors of $p-1$: $\{p_1, p_2, \ldots, p_s\}$, for example all primes less than 10000. By assumption, we can find all such candidates. We conclude that

$$p-1 \text{ divide } (p_1^{V_1}, p_2^{V_2}, \ldots, p_s^{V_s}),$$

where V_i are enough large, i.e. we can select such that $p_2^{V_2+1}$ does not divide $p-1$. So, $(p_1^{V_1}.p_2^{V_2}.\ldots.p_s^{V_s}) = (p-1)S$ for some integer S.

Calculate $(x^{(p-1)S} - 1 \bmod n)$ is alredy easy. The idea is to calculate consecutively the numbers $b_r := (\prod_{i=1}^{r} x^{p_i^{V_i}} \bmod n)$. First we should select random coprime to n number $x = b_0$. The number b_{i+1} is obtained from b_i calculating $(\ldots(((b_i)^{\overbrace{p_{i+1})^{p_{i+1}})\ldots)^{p_{i+1}}}^{V_{i+1}}} \bmod n$.

Why Pollard's algorithm works? Intuitively we can present this as follow. The ring $\mathbb{Z}_n^*$ has non complicated structure, since $\mathbb{Z}_p^*$ is subgroup where all elements have small orders. In our presentations of William's $p+1$ algorithm [20] we shall demonstrate, that even if $\mathbb{Z}_n^*$ seems good (i.e. all prime divisors p of n, are such that $p-1$ have at least one large prime factor), but there is a prime divisor p, such that $p+1$ has small prime factors, then we can succeed with factorization. The bad $p-1$ structure will be removed - applying some type of factorization - to remain only a good $p+1$ part.

Start with details. In Pollard's algorithm we consider $\text{GF}(p)$, and acts over this field multiplying consecutivaly the element, i.e. calculate its degrees. In Williams' $p+1$ algorithm we shall use projective closure of the field $\text{GF}(p)$, and acts over it, using iterations of l.f.f..

In Section 2.2 we show (using [21]), that l.f.f. of the form

$$\phi_\alpha(x) = \frac{1}{1 - x/\alpha}$$

induce in $\overline{\text{GF}(p)}$ a cycles of one and the same length $|\phi_\alpha|$. Also it is shown, that $|\phi_\alpha|$ divide $p-1$ or $p+1$. In the same paper [21] also it is proved, that the number n_- of elements $\alpha \in \text{GF}(p) \backslash \{0, 4\}$ which satisfied $|\phi_\alpha| \,\big|\, p-1$, are almost the half of all elements of $\text{GF}(p)$ - i.e. $n_-/p \to 1/2$, when $p \to \infty$.

Compose the method is now easy. Select random α, and suppose, that $\phi_\alpha(x)$ induces cycles, which divide $p+1$. With probability $1/2$ we shall succeed, i.e. this is very large probability. Similarly as in Pollard's algorithm we can select random integer x, and calculate

$$N := \phi_\alpha^{[p_1^{V_1} p_2^{V_2} \ldots p_s^{V_s}]}(x).$$

Remember that with $\cdot^{[\cdot]}$ we denote the iteration of the function. We can calculate N, since from Section 2.1 we know, that any l.f.f. can be presented as second order linear operator, or as 2×2 matrix. So iterations of ϕ_α corresponds to degrees of this matrix.

Value N calculated above is $\equiv x(\text{mod GF}(p))$, since $p+1$ divide $p_1^{V_1} p_2^{V_2} \dots p_s^{V_s}$ by assumption, and since the length of cycles induces by ϕ_α divide $p+1$. So $\phi_\alpha^{[p_1^{V_1} p_2^{V_2} \dots p_s^{V_s}]}$ acts as identity modulo (p). Consider its presentation as 2×2 matrix

$$\text{If} M_N := \begin{pmatrix} 0 & \alpha \\ -1 & \alpha \end{pmatrix}^{p_1^{V_1} p_2^{V_2} \dots p_s^{V_s}} \text{ then } M_N \equiv \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \pmod{p}.$$

If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\gcd(b, n) = p$, and so we can factor n.

3 Cycles in algeraic-combinatorial sets

In this section we shall demonstrate one special operation. Motivation to introduce this operation is as follow. In Williams $p+1$ method it is studied some cycles induced in projective closure of the GF(p). This set is not mathematical group, but it can be used to factorize the large integer numbers, satisfying special properties. So here we try to apply the next step, i.e. to generate different set, with special operation, and hope that this combination can be used to factorize an large integers.

3.1 Markov normalization and M-step

By definition Markov matrix is any matrix, with non-negative coefficients, and such that the sum of elements of any row is equal to 1. We shall consider only condition, of sums, skipping requirement "≥ 0", since we shall consider the matrices over finite field. These matrices we shall call Markov type.

First essential question is: Can we convert random matrix to Markov type, only applying multiplication of the columns by some scalars? The answer is trivial. If the matrix is

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}$$

then multiplying the columns by components of n-tuple $\lambda = (\lambda_1, \dots, \lambda_n)$ we obtain Markov type matrix, if

$$\left| \begin{array}{l} \lambda_1 a_{1,1} + \lambda_1 a_{1,2} + \dots + \lambda_n a_{1,n} = 1 \\ \lambda_1 a_{2,1} + \lambda_1 a_{2,2} + \dots + \lambda_n a_{2,n} = 1 \\ \qquad\qquad \vdots \\ \lambda_1 a_{n,1} + \lambda_1 a_{n,2} + \dots + \lambda_n a_{n,n} = 1 \end{array} \right. \tag{10}$$

From linear algebra it is well known, that this system of equations have allays unique solution, if det A 0. In this case the answer is positive, and there are many algorithms to calculate the solution λ.

The tranformation

$$A \rightarrow \begin{pmatrix} \lambda_1 a_{1,1} & \dots & \lambda_n a_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_1 a_{n,1} & \dots & \lambda_n a_{n,n} \end{pmatrix}$$

where λ satisfying (10), we shall call Markov normalization.

Motivation for operation above are Jacket matrices. They are invariant, on multiplication of nonzero scalar of their rows and columns, and so Markov normalization preserver Jacket property. Unfortunately if we first multiply a row of matrix by scalar, and next apply the procedure presented above, we shall obtain an different matrix. So in the set of matrices equivalent to fixed Jacket matrix A (i.e. obtained by multiplying the rows and columns by scalars) there is so many with Markov type. So Markov normalizing does not give us Markov normal form of$A$. We need additional restrictions.

It is natural to require not only the sums of rows to be one, but also the sum of columns. If we have such matrix, then it remains the same, if we apply the operation above, but also it remains the same, if we transpose - apply - transpose. So as single operation we shall consider

Markov normalizing, following by transposing. Shortly we shall talk about M-step. Note that we can generalized M-step, if we use some another fixed values, instead of ones on the RHS of (10).

Considering the action of M-steps over all set of matrices is not interesting, since after first M-step the sum of columns becames ones. So we shall consider action with M-steps only on the set

$$S = \{ \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} \mid \text{for } s = 1, 2, \dots, n : \sum_{i=1}^{n} a_{i,s} = 1 \}.$$

To apply M-step it is require that the determinant of matrix to be non-zero. So starting from one matrix, consequently applying the operation it is possible to go in the stage, where we must stop. In this case we have a path. In other situations it is possible to obtain a cycle. It is easy to show, that for elements in S two different matrices goes to one and same, if in M-step we multiply some of columns by 0! We shall obtain a matrix with zero determinant (and even of special type).

3.2 Properties in case of 2×2 matrices

Our research continue with studding the case of 2×2 matrices over finite field GF(p). Next result are formulated after computer search, but it seems, that they are easy to prove.

List of properties is:

1. There are $p - 3$ Jacket matrices.
2. If $p - 3 \equiv 2 \pmod 4$ (i.e. $p \equiv 1 \pmod 4$), then M-step fix two point

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} \text{ and } \begin{pmatrix} x_2 & x_1 \\ x_1 & x_2 \end{pmatrix} \text{ where } x_{1,2} = \frac{1 \pm \sqrt{-1}}{2}.$$

3. All Jacket matrices, excluding fixed point, are included in M-step cycles of length 4.
4. In the set of Jacket matrices it is satisfied

$$\text{If M-step: } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} e & f \\ g & h \end{pmatrix} \text{ then M-step: } \begin{pmatrix} f & e \\ h & g \end{pmatrix} \to \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

We shall call two cycles of 2×2 matrices conjugated, iff they contain Jacket matrices, and the second cycle contain matrix $A^{\|}$, for matrix A in first cycle. Here with $\cdot^{\|}$ we denote horizontal flip of matrix argument.

5. If $\lfloor \frac{p-3}{4} \rfloor$ is odd then we have exactly 1 self-conjugate cycle, otherwise we have not any self-conjugate cycles.

3.3 Why study M-steps?

First let answer to the question: What are M-steps in practices? It is easy to show that this is not linear operation, and so its properties are not trivial. On the other hand this operation is closely related with system of linear operation, and so it is natural to expect good properties.

We shall present here 3 ideas, where M-step cycles can be used (as method) in the future. Note, that all these three directions are closely related to research presented in [21].

1. Factoring integers attacks.

This is main motivation to study M-steps, and it is already noted in Section 3.

2. Quadratic residue.

In the previous section it is shown, that if $p \equiv 1 \pmod 4$, then M-step cycles have fixed points. There is similar property, about the cycles obtained by iteration of linear-fractional function [21] in projective closure of the field $GF(p)$. But in [21] it is shown, how to use this property to prove quadratic reciprocity law (q.r.l.). *So can we prove q.r.l. using M-step cycles?*

3. Recurrence relations.

In case of 2×2 matrices we can calculate explicitly the iterations. So in first 4 steps we obtain:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a(d-b)/D & c(d-b)/D \\ b(a-c)/D & d(a-c)/D \end{pmatrix} \to \begin{pmatrix} a(d-c\frac{d-b}{a-c})/D & c(d\frac{a-c}{d-b}-c)/D \\ b(a\frac{d-b}{a-c}-b)/D & d(a-b\frac{a-c}{d-b})/D \end{pmatrix} \to$$

$$\to \begin{pmatrix} a(d-b\frac{d\frac{a-c}{d-b}-c}{a-b\frac{a-c}{d-b}})/D & c(d\frac{a-b\frac{a-c}{d-b}}{d\frac{a-c}{d-b}-c}-b)/D \\ b(a\frac{d\frac{a-c}{d-b}-c}{a-b\frac{a-c}{d-b}}-c)/D & d(a-c\frac{a-b\frac{a-c}{d-b}}{d\frac{a-c}{d-b}-c})/D \end{pmatrix}, \ D = ad-bc$$

The idea is clear, i.e. we have special type of iteration of linear fractional function. *Are there any other interesting properties about this recurrence dependences?*

4 Elliptic Curves

An elliptic curve is a smooth, projective algebraic curve of genus one, on which there is a specified point O. For our aims is enough to define elliptic curve as plane algebraic curve with equation of the form

$$y^2 = x^3 + ax^2 + bx + c,$$

where polynomial at the right side must have 3 different roots.

Next we shall demonstrate some basic properties of elliptic curve, and also we shall explain an application of these curves in cryptography.

4.1 Preliminaries

Essential property of elliptic curves is that it is possible to define rule of addition of points. This addition satisfied associative low, and even is group (if we consider projective closure of the curve).

To explain this law we can simply use definitions as follow

<table>
<tr><th>GF(s) What s?</th><th>Info</th></tr>
<tr><td>odd prime p
$p > 3$</td><td>Equation form: $y^2 = x^3 + ax + b$
<table>
<tr><th>Different points?</th><th>Sum</th></tr>
<tr><td>$P \neq Q$</td><td>$\lambda := (y_P - y_Q)/(x_P - x_Q)$,
$x_{P+Q} = \lambda^2 - x_P - x_Q$,
$y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P$.</td></tr>
<tr><td>$P = Q$</td><td>$\lambda := (3x_P^2 + a)/(2y_P)$
$x_{2P} = \lambda^2 - 2x_P$
$y_{2P} = -y_P + \lambda(x_P - x_R)$</td></tr>
</table></td></tr>
<tr><td>2^k</td><td>Equation form: $y^2 + xy = x^3 + ax^2 + b$
<table>
<tr><th>Different points?</th><th>Sum</th></tr>
<tr><td>$P \neq Q$</td><td>$\lambda := (y_P - y_Q)/(x_P - x_Q)$,
$x_{P+Q} = \lambda^2 + \lambda + x_P + x_Q + a$,
$y_{P+Q} = \lambda(x_P + x_{P+Q}) + x_{P+Q} + y_P$.</td></tr>
<tr><td>$P = Q$</td><td>$\lambda := x_P + y_P/x_P$,
$x_{2P} = \lambda^2 + \lambda + a$,
$y_{2P} = x_P^2 + (\lambda^2 + 1)x_{2P}$.</td></tr>
</table></td></tr>
</table>

We can obtain this equations in natural way, using elliptic functions and more specially Weierstrass's $\wp$ function. Elliptic functions are 2 periodic complex (analytic) functions. Also geometric interpretation is interesting: For two points P and Q, the line pass trough them intersect the curve in point $-(P+Q)$. Identity element (0) is infinite point of projective closure. For more information see [8].

In practical applications it is consider elliptic curve with coefficients in finite field GF(p), and point with coordinates in this field.

The number of $(\mathrm{GF}(p))^2$ points on the curve is equal to the size of additive group on elliptic curve. This number is very essential parameter, but it is difficult to calculate. In [13] is given a limit of this number.

Elliptic curve group have applications in cryptography, for example in discrete logarithm problem.

In this text we shall show, that we can use l.f.f. to studding the number of points of elliptic curve group, i.e. we shall find a relation between this numbers for two different elliptic curves.

4.2 GF(p) points over $y^2 = x(x-1)(x+1)$.

One well known proposition concerning elliptic curves (and one of simplest non-trivial such) is as follow. If GF(p) is finite field with $p \equiv 1 (\mathrm{mod}\ 4)$, then the elliptic curve of form

$$y^2 = x(x-1)(x+1) \tag{11}$$

has $2a$ points on $(\mathrm{GF}(p))^2$, where a is the odd positive integer, which satisfies $p = a^2 + b^2$, for some another integer b. We introduce the method, presented in Section 4.4 exactly to attack this statement (in different way, than well known one).

One relatively short proof of this result is presented in [8], but in next lines we shall sketch an idea, the main step in which is due by Gauss.

Our first step of this proof can be completed as follow. Number of GF(p) point depends on how many numbers $x(x-1)(x+1)$, $x \in \mathrm{GF}(p)$ are quadratic residues. Obviously we can determine this number, if calculate

$$\sum_{x \in \mathrm{GF}(p)} \left(\frac{x(x-1)(x+1)}{p} \right) = \sum_{x \in \mathrm{GF}(p)} \left(\frac{x(x^2-1)}{p} \right),$$

and using (2), (3) in Section 1, and binomial theorem we conclude, that we must calculate the binomial coefficient $\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$.

Next we can use the property (which is difficult), that

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p},$$

where a is as explained after eq. (11). The last congruence has been proved in [5]. Gauss idea is to introduce the numbers

$$S_{U,V} = \#\{x \,|\, x \in U, x+1 \in V\}$$

and

$$T_{U,V} = \#\{(x,y) \,|\, x \in U, y \in V, 1 + x + y = 0\}.$$

Here U and V pass trough all combinations of cosets of cyclic subgroup K of index 4: $[GF(p)^* : K] = 4$. Next idea is to calculate the number of solutions of

$$1 + x + y + z = 0,\ x \in U, y \in v, z \in W$$

in two different ways, using numbers $S_{U,V}$ and $T_{U,V}$. To complete the proof it is necessary to use some additional arguments, and lot of calculations, since for all combinations of cosets are considered separately.

4.3 Linear-fraction correspondence

In subsections we shall consider actions of l.f.f. which modified elliptic curves. We shall consider the modifications, which preserved number if GF(p) points, and such which only preserves the property, that roots are in GF(p).

4.3.1 Trivial transformations

In this subsection we shall study trivial transformations for elliptic curves. They are not so interesting, but we want to show, that the idea of main trick, presented in next sections, is not complicated prove of trivial operations.

The number of points (x, y) with $x, y \in \mathrm{GF}(p)$ which lie on elliptic curve

$$y^2 = (x-u)(x-v)(x-w),\ u \neq v \neq w \neq u.$$

depends on (i.e. can be explained easyly by) number

$$\#\left\{x \in \{0,1,\ldots,p-1\} \,|\, \chi_2\left((x-u)(x-v)(x-w)\right) = 1\right\},\ u \neq v \neq w \neq u.$$

Obviously only condition

$$\chi_2\left((x-u)(x-v)(x-w)\right) = 1$$

is essential, and so in next we shall write only it.

Next we consider only the following elliptic curves

$$y^2 = x(x-1)(x-a),\ a \in \{2,3,\ldots,p-1\}.$$

We want to find another elliptic curve, with the same number of solutions.

We start with

$$\chi_2\left(x(x-1)(x-a)\right) = 1.$$

Applying the substitution $x \to x+1$ we obtain

$$\chi_2\left((x+1)((x+1)-1)\left((x+1)-a\right)\right) = 1.$$

Simplifying and applying the substitution $x \to \frac{1}{x}$ lead to

$$\chi_2\left((\frac{1}{x}+1)(\frac{1}{x})(\frac{1}{x}-(a-1))\right) = 1.$$

Since $\chi_2(ab) = \chi_2(a)\chi_2(b)$ and so $\chi_2(x) = \chi_2(\frac{1}{x})$. Next find

$$\chi_2\left((\frac{1}{x}+1)(x)(\frac{1}{x}-(a-1))\right) = 1.$$

Dividing and multiplying by x^2 obtain

$$\chi_2\left((1+x)(x)(1-(a-1)x)\right)\chi_2(\frac{1}{x^2}) = 1.$$

Applying once again such operation, but with $a-1$:

$$\chi_2\left((1+x)(x)(\frac{1}{a-1}-x)\right)\chi_2(a-1) = 1.$$

Next we apply the substitution $x \to -x$

$$\chi_2\left((-x+1)(-x)(\frac{1}{a-1}-(-x))\right)\chi_2(a-1) = 1.$$

Simplifying this expression finally we obtain

$$\chi_2\left((x-1)(x)(x-\frac{1}{1-a}))\right)\chi_2(a-1)=1.$$

or

$$\chi_2\left(x(x-1)(x-\frac{1}{1-a}))\right)\chi_2(a-1)=1.$$

We can conclude, that if some elliptic curve have roots 0, 1, a then number of GF(p) points can be calculated finding the number of points for the curve with roots 0, 1, $\frac{1}{(1-a)}$.

4.3.2 GF(p) roots of cubic equation

One of the Sun results presented in [18] gives as the condition when the cubic equation x^3+ax+b (there is also some additional conditions) have solution in GF(p). As prewsented in [7] this result can be used to study elliptic curves. We shall present only this part of Theorem 4.1. in [18], which is interesting to us.

Theorem 2. (Sun) *Let $p>3$ be a prime, $a,b,s\in\mathbb{Z}_p$, $ab\not\equiv 0(modp)$ and $s^2\equiv -3(b^2-4a)\pmod p$. Then the congruence $x^3-3ax-ab\equiv 0\pmod p$ is solvable if and only if $s/b+1+2\omega$ can be presented as cub in Eisenstein integers modulo p: $\{a+b\omega\,|\,a,b\in\mathbb{Z}_p\}$.*

Next we shall consider only calculations in GF(p). So $f(x):=x^3-3ax-ab=0$ wolud have solutions, iff $f(xb)=0$ have solution. So

$$x^3-3ax-ab=0\Leftrightarrow x^3b^3-3axb-ab=0\Leftrightarrow x^3-3\frac{a}{b^2}x-\frac{a}{b^2}=0 \tag{12}$$

If denote $N:=\frac{a}{b^2}$ we can reformulate Sun theorem as follow

Theorem 2'. *Let $p>3$ be a prime, $N\in$ GF(p), $N\neq 0$ and $s:=\sqrt{-3(1-4N)}\in$ GF(p). Then the equation $x^3-3Nx-N=0$ is solvable if and only if $s+1+2\omega$ can be presented as cub in Eisenstein integers modulo p: $\{a+b\omega\,|\,a,b\in$ GF(p)$\}$.*

Next we will not use variables a and b in meaning in Theorem 1, and so we can overwrite meaning immediately.

Suppose that equation $x^3-3Nx-N=0$ have root in GF(p). In sake of convenience we shall consider $(\lambda x)^3-3N(\lambda x)-N=0$ for some parameter λ, which we shall define later. Let the root is $c\in$ GF(p), and so

$$(\lambda x)^3-3N(\lambda x)-N=(x-c)(x^2+Ux+V)=(x-c)(x-\frac{a-\sqrt{b}}{2})(x-\frac{a+\sqrt{b}}{2}), \tag{13}$$

for some $a,b\in$ GF(p). Next since the coefficient before x^2 is zero we obtain that $c=-\frac{a-\sqrt{b}}{2}-\frac{a+\sqrt{b}}{2}=-a$ and thus

$$(\lambda x)^3-3N(\lambda x)-N=(x+a)(x^2-ax+\frac{a^2-b}{4})=x^3-3\frac{a^2+b/3}{4}x-\frac{ab-a^3}{4}=$$

$$=x^3-3\frac{a^2+b/3}{4}x-\frac{a^2+b/3}{4}\cdot\frac{ab-a^3}{a^2+b/3}.$$

Now similarly as in (12) we select $\lambda = \frac{ab-a^3}{a^2+b/3}$ and so

$$N = \left(\frac{a^2+b/3}{4}\right) / \left(\frac{ab-a^3}{a^2+b/3}\right)^2.$$

Next we calculate

$$-3(1-4N) = -3\frac{(ab-a^3)^2-(a^2+b/3)^3}{(ab-a^3)^2} = \cdots = b\left(\frac{3a^2-b/3}{ab-a^3}\right)^2.$$

So if we have a root in GF(p), then $s = \sqrt{-3(1-4N)}$ is in GF(p) iff b is square and so from (13) equation $x^3 - 3Nx - N = 0$ has 3 roots in GF(p).

The equation $x^3 - 3Nx - N = 0$ we can transformed as follow

$$x^3 - 3Nx - N = 0 \Leftrightarrow x(x^2-3N) = N \Leftrightarrow x = \frac{N}{x^2-3N},$$

and so if define

$$\psi(x) := \frac{N}{x^2-3N},$$

we have that $x \in$ GF(p) satisfied $x^3 - 3Nx - N = 0$, if it is fixed applying ψ.

Action of ψ over GF(x) $\cup \{\infty\}$ form the graph of the following form ($x \to \psi(x)$ are oriented edges, while the elements of GF(x) $\cup \{\infty\}$ are vertexes). Cycles, which elements are linked to roots of binary trees.

These graphs does not seems to have some specific structure, but in the next table we have presented some computer search for $N = 1$. In the table p is the prime characteristic of the field GF(p), while in column "type" we list the size of cycles.

p	type	p	type	p	type	p	type
5	1; 1	31	6	67	1; 3; 7; 11	103	1; 16
7	1; 3	37	1; 2; 3	71	1; 7	107	1; 1; 1; 5; 6
11	1; 2	41	1; 2	73	1; 18	109	4
13	1; 2	43	1; 7	79	2; 4; 7	113	1; 1; 1; 4; 4
17	3	47	1; 1; 1; 2	83	2; 10	127	1; 3; 7
19	2	53	2; 4; 5	89	1; 2; 3	131	1; 4
23	2	59	1; 3; 4	97	1; 4		
29	1; 2; 3	61	2; 11	101	1; 2		

Now we shall demonstrate, that we can find some information, about such type of graph, in theoretical way.

Proposition 3. *Number of the sub-graphs of the form*

is equal to $\left\lfloor \frac{\frac{p-1}{2}-\chi_2(3N)-\chi_2(6N)-1}{4} \right\rfloor$, *where* χ_2 *is usual quadratic character over* GF(p).

Proof It is obvious that $\psi(x) = \psi(y)$ if and only if $x = \pm y$. So we must consider the situations in which ($t \neq 0$)

$$\left| \begin{array}{l} \psi(x) = \frac{N}{x^2-3N} = t; \\ \psi(y) = \frac{N}{y^2-3N} = -t. \end{array} \right. \Leftrightarrow \left| \begin{array}{l} 3N + \frac{N}{t} = x^2; \\ 3N - \frac{N}{t} = y^2. \end{array} \right. \Leftrightarrow \left| \begin{array}{l} 3N + \frac{N}{t} - \text{ nonzero square}; \\ 3N - \frac{N}{t} - \text{ nonzero square}. \end{array} \right.$$

We can write the system above using χ_2 as follow

$$\left| \begin{array}{l} \chi_2(3N + \frac{N}{t}) = 1; \\ \chi_2(3N - \frac{N}{t}) = 1. \end{array} \right. \Leftrightarrow \left| \begin{array}{l} \chi_2(\frac{N}{t} + 3N) = 1; \\ \chi_2((\frac{N}{t} + 3N) - 6N) = \chi_2(-1). \end{array} \right.$$

When t pass through all nonzero elements in GF(p) the element $\frac{N}{t} + 3N$ pass trough GF(p)$\backslash\{3N\}$. Consider the Paley Conference matrix P of order $p+1$. The number which we want to find is equal to number of columns $\binom{+1}{\chi_2(-1)}$ in the matrix $\binom{p_2}{p_{(1+6N \mod p)}}$ and in positions different from first. Here p_i denote the $i-th$ row of matrix P.

To complete the proof we must use that P is orthogonal matrix, and the first row consists of ones. We must also consider separately the case when characteristic p is prime of the forms $4k+1$ or $4k+3$. ■

Note, that these sub-graphs can be contained even in cycles.

4.3.3 Graph representation

Our next idea is as follow

$$x^3 - 3Nx - N = 0 \xrightarrow{x \to \frac{1}{x}} x^3 + 3x^2 - \frac{1}{N} = 0 \xrightarrow{x \to x-1} x^3 - 3x + 2 - \frac{1}{N} = 0$$

If we define $B := 2 - \frac{1}{N}$, we obtain

$$x^3 - 3x + B = 0 \xrightarrow{x \to Bx} x^3 - 3\left(\frac{1}{B}\right)^2 x - \left(\frac{1}{B}\right)^2 = 0 \tag{14}$$

If $x \in$ GF(p) is root of polynomial $x^3 - 3Nx - n$, then we have also a root in GF(p) of the last equation in (14). The same is preserved, if we have 3 different roots. So the transformation

$$N \to \frac{1}{\left(\frac{1}{N} - 2\right)^2}$$

preserves essential property about the roots in GF(p). Note that it is better to consider reciprocal values, since in this case we have

$$\frac{1}{N} \to \left(\frac{1}{N} - 2\right)^2.$$

So the transformation becomes polynomial type.

By computer search we found the following

Property 4. *For all primes* p, $3 < p < 135$ *we construct the graphs induced by the transformation*

$$\theta(x) = (x-2)^2$$

on the elements of $\mathrm{GF}(p) \cup \{\infty\}$. *Similarly as in previous section these graph consists of cycles and binary trees are connected to them. However*

- *All trees are complete binary trees, excluding if they contain* 0.
- *There exists trees of height 1, but all other bigger trees have one and the same height.*

Of cource we suppouse, that this result is satisfied for general p. From Sun theorem if follows, that $\varepsilon(N) := \chi_3\left(\frac{\sqrt{-3(1-4N)}+1+2\omega}{p}\right)$ is 0 for the all trees joined to one and same cycle or is not zero for all elements. It is interesting to check is it $\varepsilon(N)$ is complete invariant!

In the next table we present some more information about Property 3.

p	1-height trees type	big tree height	type	p	1-height trees type	big tree height	type
5	1;	2	1;	61	5; 5; 5;	2	1; 1; 2; 4;
7	1;	3	1;	67	1; 5; 5; 5;	2	1; 4; 4;
11	2;	2	1; 1;	71	2; 3; 12;	3	1; 1; 3;
13	3;	2	1; 1;	73	18	3	1; 1; 3;
17	1; 3;	4	1;	79	1; 6; 12;	4	1; 2;
19	1; 3;	2	1; 2;	83	10; 10;	2	1; 1; 3; 6;
23	5;	3	1; 1;	89	1; 2; 3; 4; 12;	3	1; 5;
29	1; 2; 4;	2	1; 3;	97	3; 21;	5	1; 1;
31	1; 2; 4;	5	1;	101	1; 4; 4; 8; 8;	2	1; 2; 10;
37	9;	2	1; 1; 3;	103	1; 4; 4; 8; 8;	3	1; 6;
41	1; 3; 6;	3	1; 2;	107	26;	2	1; 1; 3; 9;
43	1; 3; 6;	2	1; 5;	109	20; 5; 2;	2	1; 1; 3; 9;
47	11;	4	1; 1;	113	1; 9; 9; 9;	4	1; 3;
53	1; 3; 9;	2	1; 6;	127	1; 3; 3; 6; 6; 6; 6;	7	1;
59	14;	2	1; 1; 2; 4;	131	2; 6; 6; 6; 6; 6;	2	1; 1; 5; 5; 5;

In is interesting to note, that twin primes have the same "1-height tree type", or the same "big tree height" and "type". Also the "big tree height" can be determined as maximal integer h, such that 2^h divide $p - \left(\frac{-1}{p}\right)$. Also the sum of cycles lengths, connected with "1-height trees" is $\lfloor p/4 \rfloor$.

In the end we demonstrate how the roots of polynomial are changed applying second transformation.

$$x \to \frac{1}{\frac{1}{N} - 2}\left(1 + \frac{1}{x}\right)$$

If we denote with x_i and N_i values of x and N obtained applying the transformation, then

$$x_3 = \frac{N_3}{1 - 2N_3}\left(1 + \frac{\frac{1}{N_2} - 2}{1 + \frac{\frac{1}{N_1} - 2}{1 + \frac{1}{x}}}\right)$$

i. e. obviously x_i can be presented as continuous fraction.

4.4 Main trick

Consider for example elliptic curve

$$y^2 = x(x-\alpha)(x-\beta), \tag{15}$$

and let suppose, that α and β, $\alpha, \beta \in \mathrm{GF}(p)$ are squares in the field, i.e. $\alpha = a^2$, $\beta = b^2$, for some $a, b \in \mathrm{GF}(p)$. Similarly as in previous section we shall demonstrate next, that there is connection between number of $\mathrm{GF}(p)$ points on this curve, and another one.

Note that presented in next section trick is simple, but this not mean that it is not interesting. For example the identity $a^2 - b^2 = (a-b)(a+b)$ is trivial, but it have applications in quadratic sieve factoring method.

4.4.1 Relations between rows

Consider Paley matrix of order $p+1$. The problem of calculating the number of points $(x, y) \in (\mathrm{GF}(p) \times \mathrm{GF}(p))$ over given elliptic curve can be transformed easily to calculation of $+1$ of bitwise multiplication of 3 rows of considered Paley matrix. Next relations of positions of these 3 rows we shall study, but we will not write this explicitly.

We start research, with writing (15) in the form

$$y^2 = x(x-a^2)(x-b^2). \tag{16}$$

We want to find the numbers of points $(x, y) \in (\mathrm{GF}(p) \times \mathrm{GF}(p))$, which satisfied eq. (16). We shall denote this number as $\#(x, y|a^2, b^2)$. Points, with $y = 0$ we can find directly – they are the couples $(0, 0)$, $(a^2, 0)$ and $(b^2, 0)$. Using this we can show easily that

$$\#(x, y|a^2, b^2) = 3 + 2.\#\left\{x \,|\, x(x-a^2)(x-b^2) \text{ is quadratic residue in } \mathrm{GF}(p)\right\}. \tag{17}$$

Let denote with $\chi_2(x)$ a quadratic character in $\mathrm{GF}(p)$, defiend in Section 1.1.

We are interesting for which x is satisfied $\chi_2\left(x(x-a^2)(x-b^2)\right) = 1$? From properties of χ_2 we obtain $\chi_2\left(x(x-a^2)(x-b^2)\right) = \chi_2(x)\chi_2(x-a^2)\chi_2(x-b^2)$. So, to answer the question we consider the triples $\left(\chi_2(x), \chi_2(x-a^2), \chi_2(x-b^2)\right)$.

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
$\chi_2(x)$	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1
$\chi_2(x-a^2)$	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1
$\chi_2(x-b^2)$	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1

In this table with S_i we denote a set of elements $x \in \mathrm{GF}(p)$, such that $\left(\chi_2(x), \chi_2(x-a^2), \chi_2(x-b^2)\right)$ are as showed in corresponding column. It is obviously, that

$$\sum_{i=1}^{8} |S_i| = |S_1| + |S_2| + |S_3| + |S_4| + |S_5| + |S_6| + |S_7| + |S_8| = |\mathrm{GF}(p)\backslash\{0, a^2, b^2\}| = p - 3. \tag{18}$$

It is well known, that number of quadratic residues is equal to the number of quadratic non-residues. That is why, considering any of the rows we obtain (we use also that numbers 0, a^2 and b^2 are not

considered, i.e. they are not in all S_i)

$$\begin{aligned}
&+|S_1|+|S_2|+|S_3|+|S_4|-|S_5|-|S_6|-|S_7|-|S_8| = -2,\\
&+|S_1|+|S_2|-|S_3|-|S_4|+|S_5|+|S_6|-|S_7|-|S_8| = -\chi_2(-1)-\chi_2(b^2-a^2),\\
&+|S_1|-|S_2|+|S_3|-|S_4|+|S_5|-|S_6|+|S_7|-|S_8| = -\chi_2(-1)-\chi_2(a^2-b^2).
\end{aligned} \tag{19}$$

The last series of equations we obtain using that the set $\{(x-c)(x-d)\,|\,x\in \mathrm{GF}(p)\}$, $c\neq d$, contain one more quadratic non-residues, than quadratic residues. We already prove such statement, when we prove orthogonality of Paley conference matrix in Section 1.1. There we show, that inner product of any 2 different rows is 0.

The equations are

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
$\chi_2(x)\chi_2(x-a^2)$	+1	+1	−1	−1	−1	−1	+1	+1
$\chi_2(x-a^2)\chi_2(x-b^2)$	+1	−1	−1	+1	+1	−1	−1	+1
$\chi_2(x)\chi_2(x-b^2)$	+1	−1	+1	−1	−1	+1	−1	+1

and so using presented above property show that the equations are

$$\begin{aligned}
&+|S_1|+|S_2|-|S_3|-|S_4|-|S_5|-|S_6|+|S_7|+|S_8| = -1-\chi_2(b^2-a^2),\\
&+|S_1|-|S_2|-|S_3|+|S_4|+|S_5|-|S_6|-|S_7|+|S_8| = -1-1 = -2,\\
&+|S_1|-|S_2|+|S_3|-|S_4|-|S_5|+|S_6|-|S_7|+|S_8| = -1-\chi_2(a^2-b^2).
\end{aligned} \tag{20}$$

Linear equations (18), (19) and (20) are 7, and there is 8 variables. If we find one more equation, we can solve the system and find

$$\#\left\{x\,|\,x(x-a^2)(x-b^2) \text{ is quadratic residue}\right\} = |S_1|+|S_4|+|S_6|+|S_7|, \tag{21}$$

which would complete out task - cf. (17).

4.4.2 Calculations

This section we start with the following

Essential note 1. *Calculations in previous section we consider only to show that counting x^2 satisfying*

$$\chi_2(x^2(x^2-a^2)(x^2-b^2)) = 1$$

instead of x satisfying

$$\chi_2(x(x-a^2)(x-b^2)) = 1$$

is not essential restriction, i.e. one number can be easily obtained by the other.

Let try to find $|S_1|+|S_4|$. Similarly as in (21) we can write

$$^1\!/_2.\#\left\{x\,|\,x^2(x^2-a^2)(x^2-b^2) \text{ is quadratic residue}\right\} = |S_1|+|S_4|,$$

Obviously we can exclude the x^2 from the expression above. If we use also that $u^2-v^2=(u-v)(u+v)$, the equation above can be written as

$$^1\!/_2.\#\left\{x\,|\,(x-a)(x+a)(x-b)(x+b) \text{ is quadratic residue}\right\} = |S_1|+|S_4|.$$

Now we shall introduce a linear-fractional function. We shall use already presented in Section 3.3 equation

$$\forall s \neq 0 : s \text{ is quadratic residue} \Leftrightarrow \frac{1}{s} \text{ is quadratic residue.} \tag{22}$$

To "switch" to l.f.f. we shall use the lemma below, which can be proved easily using (22). For the sake of convenience (in next considerations) we put a labels of rows and columns of table in this lemma.

Lemma 5. *For fixed $x \notin \{a, b, -a, -b\}$ the expression $(x-a)(x+a)(x-b)(x+b)$ is quadratic residue, iff any of elements in the table*

	🜚	🜳	🜔	🜨
A	$\frac{x-a}{x+a}\frac{x-b}{x+b}$	$\frac{x-a}{x+a}\frac{x+b}{x-b}$	$\frac{x+a}{x-a}\frac{x-b}{x+b}$	$\frac{x+a}{x-a}\frac{x+b}{x-b}$
B	$\frac{x-a}{x-b}\frac{x+a}{x+b}$	$\frac{x-a}{x-b}\frac{x+b}{x+a}$	$\frac{x-b}{x-a}\frac{x+a}{x+b}$	$\frac{x-b}{x-a}\frac{x+b}{x+a}$
C	$\frac{x-a}{x+b}\frac{x-b}{x+a}$	$\frac{x-a}{x+b}\frac{x+a}{x-b}$	$\frac{x+b}{x-a}\frac{x-b}{x+a}$	$\frac{x+b}{x-a}\frac{x+a}{x-b}$

is quadratic residue.

Next we shall consider some fraction from Lemma 5, and denote it in general form $\frac{x-c}{x-e}\frac{x-d}{x-f}$. Instead of all expression

$$\tfrac{1}{2}.\#\left\{x\backslash\{0,a,b,-a,-b\} \;\middle|\; \frac{x-c}{x-e}\frac{x-d}{x-f} \text{ is quadratic residue}\right\} = |S_1| + |S_4|.$$

we shall use only write the content in the set brackets

$$x\backslash\{0,a,b,-a,-b\} \;\middle|\; \chi_2(\frac{x-c}{x-e}\frac{x-d}{x-f}) = 1$$

Next we shall use, that the function $y = \frac{x-c}{x-e}$ is one to one correspondence of $x \in \mathrm{GF}(p)\backslash\{e\}$ to $y \in \mathrm{GF}(p)\backslash\{1\}$, and thus continue our calculations as

$$y\backslash\{1, \frac{c}{e}, \frac{a-c}{a-e}, \frac{b-c}{b-e}, \frac{a+c}{a+e}, \frac{b+c}{b+e}\} \;\middle|\; \chi_2(y\frac{y-\frac{c-d}{e-d}}{y-\frac{c-f}{e-f}})\chi_2(\frac{e-d}{e-f}) = 1\ . \tag{23}$$

Here on left if some of denominator is 0, we skip this term.

If on right side we replace linear fraction as multiplication, then we obtain new elliptic curve. Now we must consider the cases in Lemma 5. The values of columns 🜚 and columns 🜨 are reciprocal, and similarly the columns 🜳 and 🜔. So, obtained elliptic curves are connected with trivial operation $x \to 1/x$. Next let consider columns 🜚 and 🜳. In this case operation is like

$$x(x-u)(x-v) \to x(1/x-u)(1/x-v) = x^2(1/x)((1/x)-u)((1/x)-v),$$

and so again one curve is obtained by other applying trivial operation (and it is not interesting).

We conclude that we must consider only cases in column ✝. In all cases using (22) and (23) we obtain

$$\begin{aligned}
&\text{A: } x\backslash\{1,-1,0,-\tfrac{a-b}{a+b},-\tfrac{b+a}{a-b}\} \;\big|\; \chi_2(x(x+\tfrac{a-b}{a+b})(x+\tfrac{a+b}{a-b}))\chi_2(\tfrac{a+b}{a-b})=1;\\
&\text{B: } x\backslash\{1,\tfrac{a}{b},0,\tfrac{2a}{a+b},\tfrac{a+b}{2b}\} \;\big|\; \chi_2(x(x-\tfrac{2a}{a+b})(x-\tfrac{a+b}{2b}))\chi_2(\tfrac{a+b}{2b})=1;\\
&\text{C: } x\backslash\{1,-\tfrac{a}{b},0,-\tfrac{a-b}{2b},\tfrac{2a}{a-b}\} \;\big|\; \chi_2(x(x+\tfrac{a-b}{2b})(x-\tfrac{2a}{a-b}))\chi_2(-\tfrac{2b}{a-b})=1\,.
\end{aligned} \tag{24}$$

Some additional details concerning these equations we shall present in next section.

4.5 Improvement of method and partial cases

In this section, we shall make some remarks, about our selection (16) of root of elliptic curve, i.e. that thay are (0; Square; Square). Is this essential restriction?

Obviously, if the roots of elliptic curve are in GF(p) then we can obtain a zero root applying suitable replacement $x \to x - c$. If we apply the substitution $x \to \lambda x$, then we obtain the curve

$$\Big(\frac{y}{\lambda}\Big)^2 = \lambda x(x-\frac{\alpha}{\lambda})(x-\frac{\beta}{\lambda}).$$

If λ is not sqare then removing first λ on right side we obtain elliptic curve, which GF(p) points are "complement" of original curve. So if we find the points on modified curve, automatically it gives the number of points on original one.

We make all this calculations above, to show that is we have roots like (0, Non square, Non square), then we can convert the curve to curve of the required form (0, Square, Square).

Next we show what happen if we apply shifts. Let consider the roots 0, α, β. If α, β are squares, or both are not squares, then we can apply construction, explained in next section. That is why we shall consider only the case in which α is square, while β is not.

p	0	α	β	$-\alpha$	0	$\beta-\alpha$	$-\beta$	$\alpha-\beta$	0
$4k+1$	0	square	not square	square	0	X	not square	X	0
$4k+3$	0	square	not square	not square	0	X	square	not X	0

We see, that if $p = 4k+1$ then not depending on "value" of X (i.e. "square" or "not square") we have "solution". We can not conclude this in the case $p = 4k+3$.

Our next question is: What happen if we select elliptic curve, considered in Section 3.2 and apply the method?

First we shall apply suitable simplification of (24), only applying trivial transformations. We want to obtain one of the roots to be 1.

$$\begin{aligned}
&\text{A: } x\backslash\{1,-1,0,-\tfrac{a-b}{a+b},-\tfrac{b+a}{a-b}\} \;\Big|\; \chi_2(-1)\chi_2(x(x-1)(x-\big(\tfrac{a-b}{a+b}\big)^2))=1\\
&\text{B: } x\backslash\{1,-1,0,-\tfrac{a-b}{a+b},-\tfrac{a+b}{a-b}\} \;\Big|\; \chi_2(+1)\chi_2(x(x-1)(x-\tfrac{4ab}{(a+b)^2}))=1;\\
&\text{C: } x\backslash\{1,-1,0,-\tfrac{a-b}{a+b},-\tfrac{a+b}{a-b}\} \;\Big|\; \chi_2(\tfrac{-4ab}{(a-b)^2})\chi_2(x(x-1)(x-\tfrac{(a-b)^2}{-4ab}))=1\,.
\end{aligned} \tag{25}$$

Now we can start with considering of interesting elliptic curve

$$y^2 = x(x-1)(x+1)$$

where p must be of the form $4k+1$ (otherwise GF(p) points are simply $\frac{p-1}{2}$). In this case $a=1$ and $b=i$, where $i \in$ GF(p) is "imaginary unit", i.e. $i.i=-1$. Substituting these values in equations above we obtain

$$\begin{aligned}
&\text{A: } x\backslash\{1,-1,0,+i,-i\} \mid \chi_2(-1)\chi_2(x(x-1)(x+1)) = 1\,;\\
&\text{B: } x\backslash\{1,-1,0,+i,-i\} \mid \chi_2(+1)\chi_2(x(x-1)(x-2)) = 1\,;\\
&\text{C: } x\backslash\{1,-1,0,+i,-i\} \mid \chi_2(+2)\chi_2(x(x-1)(x-\tfrac{1}{2})) = 1\,.
\end{aligned}$$

and obviously all this curves are obtained by start one applying trivial transformations.

Presented above result is very disappointed!!! What happen if all curves are obtained by start curve, applying trivial transformations??? We must check... Let in (25) we put $a=1$ and $b=s$. Correspondence between start curve and obtained new is as follow

$$x(x-1)(x-s^2) \quad \rightarrow \quad x(x-1)(x-\left(\frac{1-s}{1+s}\right)^2).$$

Let $b=s^2$. In next formula

$$b \rightarrow \left(\frac{1-\sqrt{b}}{1+\sqrt{b}}\right)^2 = \frac{1+b-2\sqrt{b}}{1+b+2\sqrt{b}} = \frac{(1+b)^2+4b-2\sqrt{b}(1+b)}{(1+b)^2-4b} = \frac{1+b^2+6b-2b\sqrt{b}-2\sqrt{b}}{(1-b)^2}$$

one can see how complicated calculations we obtain, and it is obvious that they are far from trivial transformation presented in Section 4.3.1. That we obtain something new is intuitively clear, since we can not "split" s^2 applying trivial transformations.

5 Jacket matrices

The Jacket matrices are a generalization of complex Hadamard matrices. The property of Jacket matrices is, that for any 2 rows $(a_{i,1},\ldots,a_{i,n})$ and $(a_{j,1},\ldots,a_{j,n})$ it is necessary to have the Jacket condition

$$\sum_{s=1}^{n}\frac{a_{i,s}}{a_{j,s}}=0. \tag{26}$$

Obviously complex Hadamard matrices satisfy this condition, i.e. they are Jacket matrices.

Requirement of (26) instead of usual inner product give as bad algebraic properties, about Jacket matrices - for example multiplication of two Jacket matrices in general is not Jacket matrix. However, Jacket matrices have some interesting combinatorial properties. For example if we multiply by non-zero element some row or column, then the matrix remain Jacket. This type of equivalence operation split the space in large classes of matrices. In orthogonal case we can multiply only by ± 1.

We also need one modification of such matrices.

Definition 1. *A matrix $A=(a_{i,j})_{i,j=1}^{n}$ is called Jacket Conference matrix, if*

1. *We have $a_{i,i}=0$, $i=1,2,\ldots,n$;*
2. *We have $a_{i,j}=0$, $i\neq j$, $i,j=1,2,\ldots,n$.*

and also if it satisfy the following restricted Jacket condition

$$\sum_{\substack{s=1\\ s\neq i,\,s\neq j}}^{n}\frac{a_{i,s}}{a_{j,s}}=0$$

In this paper we are interesting mainly from parameterized Jacket matrices. This mean that we want to construct Jacket matrices with at least one parameter x. So for example

$$Ax+B \tag{27}$$

is Jacket, then obviously the Jacket condition would look like

$$\sum_{i=1}^{n}\frac{a_{s,i}.x+b_{s,i}}{a_{s,i}.x+b_{s,i}}=0.$$

So matrix (27) is closely related to l.f.f. Studding parameterized Jacket matrices we study also l.f.f.

5.1 Hadamard case

In next subsections we shall study Hadamard and complex Hadamard matrices. All properties are obtained, while studying Jacket matrices, and so there is not very specific properties, related only to Hadamard matrices.

One of interesting theoretical research directions, explained in this technical report is connected with attack of the following

Conjecture 1. *There is not exists circulant Hadamard matrix of order bigger than* 4.

We attack the problem, considering Hadamard matrix, as Jacket, and thus we must study the system of non-linear equations.

5.1.1 Paley Complex Hadamard Conference matrices

Paley Conference matrices are well known, but they can be easily generalize, to complex Hadamard case. In this section we shall demonstrate also, that one property of Paley Conference matrices - nega-circulant form - has its equivalent in complex Hadamard case. First we need the following

Definition 2. *The matrix A, satisfying*

$$a_{i+1,j+1} = a_{i,j}, \text{ and } a_{i+1,1} = s.a_{i,n},$$

for some fixed non-zero s is called multi-circulant.

In this proof we shall use Fibonacci like sequences.

Next lemma combine in one a Lemma 1 and Lemma 2 in [17]. for the sake of completeness we shall proof these results.

Lemma 6. *Let $u_0 = 0$, $u_1 = 1$ and $u_i := a.u_{i-1} + b.u_{i-2}$, for $i \geq 2$. Here a and b are fixed constants. Let $n := \min\{i \mid i \geq 1, u_i \equiv 0 (\mathrm{mod}\ p)\}$. Then*

1. All fractions $u_i/u_{i+1} \in GF(p)$, $i = 0, 1, \ldots, n-1$ are different;

2. For some fixed integer s, $1 < s < n$ all fractions $u_i/u_{i+s} \in GF(p)$, $i = 0, 1, \ldots, \widehat{n-s}, \ldots, n-1$ are different.

Here with $\hat{x}$ we denote, that the integer x has been omitted.

Proof

1. Suppose that there exists (u_i, u_{i+1}) and (u_j, u_{j+1}), $i < j$, such that $u_i/u_{i+1} = u_j/u_{j+1}$, or similarly $u_i = \delta.u_j$ and $u_{i+1} = \delta.u_{j+1}$, for some δ. Select such pairs with minimal value of index i. Obviously $i > 0$, since otherwise $u_j = 0$ - contradiction. But obviously $u_{i-1} = (u_{i+1} - a.u_i)/b = \delta.(u_{j+1} - a.u_j)/b = \delta.u_{j-1}$, and so $u_{i-1}/u_i = u_{j-1}/u_j$ - contradiction with the choice of i.

2. Applying substitution in definition $u_{i+1} := a.u_i + b.u_{i-1}$ we can show easily, that $u_{n+s} = A.u_{n+1} + B.u_n$, for some integers A and B. If some of A and B is $\equiv 0 \bmod p$ then u_s or u_{s-1} would be $\equiv 0 \bmod p$ – this is contradiction with restrictions, about s. Now in the same way, as in p. 1 we can show, that from $u_i/u_{i+s} = u_j/u_{j+s}$, $i \neq j$ it follows that $u_i/u_{i+1} = u_j/u_{j+1}$, which is a contradiction with result above. ■

If we have Fibonacci like sequence which first $n = p+1$ elements are not zero, then from Lemma 6 it follow, that the fractions u_i/u_{i+s} form complete system of residues. In particular their sum is zero. We shall use this idea, to construct multi-circulant Jacket Conference matrix. First we need such sequence (of length $p+1$), and we already known, that such sequence exists. It is enough to select $c \in \mathrm{GF}(p^2)$ to be the element of order $p+1$, and apply the Proposition 1 in Section 2.2. It is better to write this sequence in exact form

$$u_0 = 0, u_1 = 1, \text{ and } u_{n+1} = (c + \frac{1}{c} + 2)(u_n - u_{n-1}), \text{ where } c \in \mathrm{GF}(p^2)\backslash\{+1, -1\}, |\langle c \rangle| = p+1 \tag{28}$$

Now we are ready to construct a Jacket Conference matrix.

Proposition 7. *Consider the Fibonacci like sequences with $p+1$ first elements not divisible bu p. Let define the following $(p+1)\times(p+1)$ matrix*

$$A = (a_{i,j})_{i,j=0}^{p} : a_{i,j} = u_{i+(p-j+1)}.$$

Then this matrix is multi-circulant Jacket Conference matrix.

Proof: Lemma 6 and property of sequence give as that the matrix is Jacket Conference. Now let us check whether it is multi-circulant or not. Obviously $a_{i+1,j+1} = u_{(i+1)+(p-(j+1)+1)} = u_{i+(p-j+1)} = a_{i,j}$, and so it remain to show, that there exists such s, that $a_{i+1,1} = s.a_{i,p+1}$, for all i. Let select $s = u_{p+2}$. Then it is easy to show by induction, that $u_{i+p+1} = s.u_i$. Thus

$$a_{i+1,1} = u_{i+(p-(1)+1)} = u_{i+p} = s.u_i = s.u_{i+(p-(p+1)+1)} = s.a_{i,p+1}.$$

■

This matrix can be used to obtains a complex Hadamard Conference matrix. If θ is a primitive element of $GF(p)$, then any non-zero element can be written as θ^s, for some integer s. If we apply the substitution $\theta^s \to \xi^s$, where ξ is primitive $p-1^{\text{th}}$ root of one, we shall obtain a remarked relation between Jacket Conference matrix and this complex Hadamard Conference matrix.

We can determine exact value of coefficient s in the proof of Proposition 7, i.e. value of u_{p+2}. We need calculations in next proposition later.

Proposition 8. *For sequence (28) we have that $u_{p+2} = c + \frac{1}{c} + 2$.*

Proof: Let assume $a := c + \frac{1}{c} + 2$. From theory of recurrence equations we know that u_i can be presented as $u_i = u.x_1^i + v.x_2^i$, where x_1 and x_2 are roots of quadratic equation $x^2 - ax + a = 0$ (we consider only the case in which the roots are different: $a \neq 0$, $a \neq 4$), and so

$$x_1 + x_2 = x_1.x_2 = a. \tag{29}$$

Using $u_0 = 0$, $u_1 = 1$, and $u_{p+1} = 0$ we calculate

$$\begin{gathered} u_0 = u + v = 0 \Rightarrow v = -u \\ u_1 = u.x_1 - u.x_2 = 1 \\ u_{p+1} = u.x_1^{p+1} - u.x_2^{p+1} = 0 \Rightarrow x_1^{p+1} = x_2^{p+1} =: S \\ u_{p+2} = u.x_1^{p+1}.x_1 - u.x_2^{p+1}.x_2 = S(u.x_1 - u.x_2) \overset{(26)}{=} S, \end{gathered} \tag{30}$$

and it remain to show, that $S = a$.

We can consider x_1 and x_2 as elements from extended field $GF(p^2)$, so we can move all calculations over this field. Thus we can use the formulae $(a+b)^p = a^p + b^p$, and also that $\forall c \in GF(p) : c^p = c$. We start from (29) and calculate

$$x_1 + x_2 = a \Rightarrow x_1^p + x_2^p = a^p = a \Rightarrow x_1^{p+1} + x_1.x_2^p = x_1.a \Rightarrow x_2^{p+1} + x_1.x_2^p = x_1.a \Rightarrow$$

$$\Rightarrow x_2^p(x_1 + x_2) = x_1.a \Rightarrow x_2^p = x_1 \Rightarrow S = x_1.x_2 = a$$

■

We shall continue to studying the matrix A constructed in Proposition 7.

Next we shall prove that the matrix A is equivalent to matrix, which can be constructed similarly as Paley Conference matrices. We can use some results from [21], but this is not necessary, as we can see below.

We note that we can find a, such that to induce a recurrence sequence of $p+1$ non-zero elements (in GF(p)). Next, form Lemma 6 fractions u_i/u_{i+1} form complete system of residues. Similarly Paley definition in Section 1.1 we can define

$$B = (b_{i,j})_{i,j=0}^{p}$$

where

$$b_{i,j} = \begin{cases} 0, & i = j; \\ 1, & i = 1,\ j \neq 1; \\ 1, & j = 1,\ i \neq 1; \\ c_{i-1} - c_{j-1}, & \text{otherwise.} \end{cases}, \text{ for } c_i = \frac{a.u_i}{u_{i+1}}.$$

Now, we are ready to prove main statement in the section

Proposition 9. *The matrices A and B can be obtained one from the other, applying multiplication of some rows and columns by -1.*

Proof: First we shall multiply the columns $2, 3, \ldots, p+1$ of matrix A by $\frac{1}{b_{1,2}}, \frac{1}{b_{1,3}}, \ldots, \frac{1}{b_{1,p+1}}$, respectively. Thus we obtain an Jacket Conference matrix, which first row (excluding position $(1,1)$) contain only ones. With similar procedure we can make the first column to contain only ones. So we obtain new matrix C, such that

$$C = (c_{i,j})_{i,j=0}^{p};\ c_{i,j} = \begin{cases} \frac{a_{i,j}}{a_{0,j}.a_{i,0}}, & i \neq j,\ i,j \geq 1 \\ 1, & i \neq j,\ i = 0 \text{ or } j = 0 \\ 0, & i = j \end{cases}$$

From matrix C we can obtain some matrix C', as follow. Multiply first row by constant and next multiply columns $1, 2, \ldots, p$ by reciprocal of this constant. So both C' and C has ones in first row and column, but "internal" elements of matrix C' are divided by constant. So we can consider matrix C up to multiplier of "internal" part.

We want to show that $A = C$. Since we know that first row and first column of these matrices are the same (i.e. they are only ones), we must prove equality only in "internal" part. We can write this condition as

$$\frac{au_{i-1}}{u_i} - \frac{au_{j-1}}{u_j} = \varepsilon(\frac{a.u_{p+1-j+i}}{u_{p+1-j}.u_{p+1+i}}). \tag{31}$$

for some constant ε.

We shall write $U \sim V$, if $\chi(U) = \epsilon\chi(V)$, for some ϵ not depending on i and j. In this notation using that $u_{i+p+1} = s.u_i$, the eq. (31) can be presented as

$$\frac{u_{i-1}.u_j - u_{j-1}.u_i}{u_i.u_j} \sim \frac{u_{i-j}}{u_{-j}.u_{+i}}, \tag{32}$$

and we must prove it.

First we shall calculate the LHS of (32). Using the same notations as in Proposition 8, we find:

$$u_{i-1}u_j = u^2.(x_1^{i-1} - x_2^{i-1})(x_1^j - x_2^j) = u^2.(x_1^{i+j-1} + x_2^{i+j-1} - x_2^{i-1}x_1^j - x_1^{i-1}x_2^j)$$

and so

$$u_{i-1}u_j - u_{j-1}u_i = u^2.(x_2^{i-1}x_1^{j-1}(-x_1+x_2) + x_1^{i-1}x_2^{j-1}(-x_2+x_1)) =$$
$$= u^2.(x_1-x_2).x_1^{i-1}.x_2^{i-1}.(x_2^{j-i} - x_1^{j-i}) = -a^i u_{j-i}u_1 = -a^i u_{j-i} = a^j u_{i-j}.$$

In the last equation we use the following

$$u_s = u.(x_1^s - x_2^s) = u.((a/x_2)^s - (a/x_1)^s) = a^s.u.(x_2^{-s} - x_1^{-s}) = -a^s.u_{-s}.$$

Using the last two equations (7) can be proved easily.

$$u_{i-1}.u_j - u_{j-1}.u_i \sim \frac{u_i.u_j.u_{i-j}}{u_{-j}.u_{+i}},$$

$$(7) \Leftrightarrow \frac{a^j u_{i-j}}{u_i.u_j} \sim \frac{u_{i-j}}{u_i.a^{-j}.u_j} \Leftrightarrow \text{ true}$$

■

5.1.2 Generalize Paley Construction I

Original Paley construction I is based on class of symmetric conference matrices. We shall demonstrate that generalization of conference matrices, presented in previous section, can be used in modified Paley construction [9].

If p and q are odd primes, such that q divide $p-1$, then we can define q^{th} multiplicative character $\chi_q : GF(p) \to \{0, 1, \xi, \xi^2, \ldots, \xi^{q-1}\}$. Of course $\xi \in \mathtt{C}$ is primitive q^{th} root of one. Next we apply χ_q to all elements of matrix A, defined in Theorem 1 in §5.1.1. So we obtain matrix, which is naturally called a complex Hadamard Conference matrix. It contain zeros on main diagonal, and elements of norm 1 elsewhere. Also complex inner product of any two rows is 0.

Lemma 10. *For $q \geq 3$ any normalized complex Hadamard Conference matrix is symmetric, while for $q = 2$ is symmetric, or (can be converted easily (by multiplying first column by -1) to) skew-symmetric.*

Proof: The idea is slide generalization of the prove, that normalized Conference matrix are only symmetric or skew-symmetric.

Consider rows u and v, $1 < u, v \leq p+1$, $u \neq v$. Define

$$k_{s,t} := \#\left\{i \in \{2, 3, \ldots, p+1\} \mid b_{s,i} = \xi^t\right\},$$

where # denotes the number of elements in the set. Consider the product:

$$P := \prod_{i \neq u} b_{u,i}.\overline{\prod_{i \neq v} b_{v,i}} = \prod_{i \neq u} b_{u,i}.(\prod_{i \neq v} b_{v,i})^{-1}.$$

Since the matrix is complex Hadamard Conference, and first row (excluding $b_{0,0}$) contain only ones we obtain that the $k_{u,0} = k_{u,1} = \cdots = k_{u,p-1}$, and similarly $k_{v,0} = k_{v,1} = \cdots = k_{v,p-1}$. Thus we obtain that $S = 1$. On the other hand complex inner product of rows u and v.

$$b_{u,1}b_{v,1} + b_{u,2}b_{v,2} + \cdots + b_{u,p+1}b_{u,p+1} \tag{33}$$

is 0, and so its sum consists of equal numbers of $1, \xi, \xi^2, \ldots, \xi^{q-1}$. On the other hand multiplication of this numbers are obviously multiplication of elements in non-zero terms of (33), and it is $P/(a_{u,v}\overline{a_{v,u}})$. If $q > 2$ then $1\xi\xi^2 \ldots \xi^{p-1} = 1$, and $a_{u,v} = a_{v,u}$. If $p = 2$ we have $1.\xi^{2-1} = -1$, and it is possible $a_{u,v} = -a_{v,u}$ for some p. ■

The first construction of this section is given by the following

Proposition 11. *If (B) is matrix defined in this section, then*

$$C = \begin{pmatrix} B & B \\ \overline{B} & -\overline{B} \end{pmatrix} + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

is complex Hadamard matrix.

Proof: The matrix C is presented as sum of two matrices.

First we shall show, that the complex inner product (c.i.p.) of any two different rows of left matrix is 0. Select the rows u and v, $u < v$. Since B is complex Hadamard Conference matrix, if $1 \leq u, v \leq p+1$, or $p+2 \leq u, v \leq 2p+2$ the c.i.p. will be the sum of c.i.p. of left part plus c.i.p. of right part, i.e. 0. In other case $1 \leq u \leq p+1$, $p+2 \leq v \leq 2p+2$ obviously the c.i.p. of left part is not 0 in general, but it is also obvious, that it is minus of the c.i.p. of the right part, i.e. sum will be also 0.

We know, that any two rows of left part are with c.i.p. 0. We want to show that if we add the right matrix to the left this property will be preserved. Let a selected rows be a u and v, $u < v$. If $1 \leq u, v \leq p+1$, then the c.i.p. would be changed with: $(+1).\overline{a_{v,u}} + a_{u,v}.\overline{(+1)} + (-1).\overline{a_{v,u}} + a_{u,v}.\overline{(-1)} = 0$, so c.i.p. will not be changed, and it remain 0. Similarly arguments work in case $p+2 \leq u, v \leq 2p+2$. When $1 \leq u \leq p+1$, $p+2 \leq v \leq 2p+2$ we must consider two cases. If $v = u + p$, then the c.i.p. will be changed with $-1 + 1 = 0$, otherwise is $v \neq u + p$ the c.i.p. will be changed with $(+1).\overline{\overline{a_{v,u}}} + a_{u,v}.\overline{(-1)} + (-1).\overline{-\overline{a_{v,u}}} + a_{u,v}.\overline{(-1)}$ - the internal conjugation is by definition of C, while the external one by definition of complex inner product. This sum is 0, since matrix B is symmetric.

It is obviously, that matrix C consists of elements with norm one. This complete the proof. ■

In this section we shall present one more construction. We shall start with original Paley construction, but in such form, which can be easily generalized. Remember, that Paley method II [11] can be applied to produce Hadamard matrix obtained by symmetric Conference matrix.

Let C be an $m \times m$ symmetric Conference matrix, and A and B are $n \times n$ Hadamard matrices. Paley statement says, that for $n = 2$, and matrices

$$A = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{34}$$

the matrix

$$S := A \otimes C + B \otimes 1_m$$

is Hadamard. Here we denote with "$\otimes$" a Kronecker product of matrices, and with 1_m we denote identity matrix of order m.

Let us denote now, with $X^{\mathbb{N}}$ a transpose matrix of X. To check that S is Hadamard matrix we must show, that $SS^{\mathbb{N}} = mn$.

$$SS^{\mathbb{N}} = (A \otimes C + B \otimes 1_m)(A^{\mathbb{N}} \otimes C^{\mathbb{N}} + B^{\mathbb{N}} \otimes 1_m) =$$

$$= (A \otimes C)(A^{\backslash\!\backslash} \otimes C^{\backslash\!\backslash}) + (BB^{\backslash\!\backslash}) \otimes 1_m + (AB^{\backslash\!\backslash}) \otimes C + (BA^{\backslash\!\backslash}) \otimes C^{\backslash\!\backslash}.$$

Since $C^{\backslash\!\backslash} = C$ and A and C are orthogonal matrices, it follows that $A \otimes C$ is also orthogonal matrix. Matrix B is Hadamard matrix, and so

$$SS^{\backslash\!\backslash} = (mn - n) + n + (AB^{\backslash\!\backslash} + BA^{\backslash\!\backslash}) \otimes C. \tag{35}$$

The matrix S would be Hadamard (i.e. $SS^{\backslash\!\backslash} = mn$), iff

$$AB^{\backslash\!\backslash} + BA^{\backslash\!\backslash} = 0, \tag{36}$$

which holds, for matrices in (34). We shall call the pair (A, B) of Hadamard matrices matched, iff the equation (36) holds.

We can generalize Paley construction, if we find matched matrices A and B of bigger dimensions.

Proposition 12. *If (A, B) is matched, and D is Hadamard matrix then $(A, B) \otimes D := (A \otimes D, B \otimes D)$ is pair of matched matrices.*

Proof: Since A, B and D are Hadamard, the matrices $A \otimes D$ and $B \otimes D$ are also Hadamard matrices. We can obtain the following calculation to prove $(A \otimes D, B \otimes D)$ is matched pair

$$(A \otimes D)(B \otimes D)^{\backslash\!\backslash} + (B \otimes D)(A \otimes D)^{\backslash\!\backslash} = (AB^{\backslash\!\backslash} + BA^{\backslash\!\backslash}) \otimes (DD^{\backslash\!\backslash}) = 0.$$

This finish the proof. ■

Presented above proposition is not so useful, if we use as matched pair matrices from (34). Applying $\otimes D$ first, and next apply the Paley construction is the same as applying first Paley construction and next $\otimes D$.

Proposition 13. *If (X) and (Y) are $2n \times n$ matrices and the composite matrix $\begin{pmatrix} X \\ Y \end{pmatrix}$ is Hadamard, then*

$$(U, V) := (\begin{pmatrix} X \\ Y \end{pmatrix}, \begin{pmatrix} Y \\ -X \end{pmatrix})$$

is pair of matched matrices.

Proof: By definition, the first matrix is Hadamard, and obviously the second is also Hadamard. We shall check the condition (36). We can write it as

$$\langle a_v, b_u \rangle + \langle a_u, b_v \rangle = 0, \ \forall u, v \in \{1, 2, \ldots, m\} \tag{33'}$$

The matrices U and V (up to the sign) have rows of one and the same Hadamard matrix. It is easy to show that the (pay4') will be sum of two 0's inner products, excluding only the case in which the row corresponds to its "identical" row. By definition

$$u_i = -v_{i+n}, \text{ for } i = 1, 2, \ldots, n$$

and

$$u_i = v_{i-n}, \text{ for } i = n+1, n+2, \ldots, 2n.$$

Thus if the first inner product in (36) is nonzero, then it must be $\pm 2n$, while the other one would be $\mp 2n$. Thus the sum is 0. ■

5.2 General Jacket Case

We know, that parameterized Jacket matrices are connected with l.f.f. One easy construction of such matrices is as follow. Get two Jacket matrices A and B. Multiplying by variables $\{v_i\}$ the rows and/or columns of A and B we can obtain some matrices A_1 and B_1. The Kronecker product of A_1 and B_1 is also a Jacket matrix, and it is parameterized. However, applying suitable multiplication of rows and/or columns by $\{v_i^{-1}\}$ we can obtain the Kronecker product of matrices A and B. So this construction is trivial one.

In next sections we shall demonstrate, some non-trivial parameterized matrices. All of them are obtained by specific constructions, composing (small) Jacket matrices.

5.2.1 Parameterized Jacket Matrices

It is easy to check, that matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} + a \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -a & a & -1 \\ 1 & a & -a & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

is Jacket for any non-zero value of a.

In this section we shall demonstrate, that the example above can be obtained from one more general construction. The construction follows from the next proposition, which generalize (and more essential clear) the idea in [3].

Proposition 14. *Let n and m are natural numbers, $(A_1), (A_2), \ldots, (A_m)$ are $n \times n$ Jacket matrices, and $B = (b_{i,j})$ is $m \times m$ Jacket matrix. Then the matrix*

$$\begin{pmatrix} b_{1,1}A_1 & b_{1,2}A_1 & \ldots & b_{1,m}A_1 \\ b_{2,1}A_2 & b_{2,2}A_2 & \ldots & b_{2,m}A_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{m,1}A_m & b_{m,2}A_m & \ldots & b_{m,m}A_m \end{pmatrix}$$

is Jacket.

Proof: We must check the Jacket condition.

If two lines $ns + \mu_1$ and $ns + \mu_2$ are in one and the same block A_s, then since A_s is Jacket matrices it follows, that Jacket condition holds:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{b_{s,i}.a_{\mu_1,j}}{b_{s,i}.a_{\mu_2,j}} = \sum_{i=1}^{m}(\sum_{j=1}^{n} \frac{a_{\mu_1,j}}{a_{\mu_2,j}}) = \sum_{i=1}^{m} 0 = 0.$$

Suppose that first row $ns + \mu_1$ is in A_s, while the second $nt + \mu_2$ is in A_t. In this case

$$\sum_{j=1}^{n}\sum_{i=1}^{m} \frac{b_{s,i}.a_{\mu_1,j}}{b_{t,i}.a_{\mu_2,j}} = \sum_{j=1}^{n} \frac{a_{\mu_1,j}}{a_{\mu_2,j}} \sum_{i=1}^{m} \frac{b_{s,i}}{b_{t,i}} = \sum_{j=1}^{n} \frac{a_{\mu_1,j}}{a_{\mu_2,j}} 0 = 0.$$

since B is Jacket matrix. ■

If we select

$$m = n = 1;\ A_1 = \begin{pmatrix} 1 & a \\ 1 & -a \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \text{and } B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

then we obtain the matrix equivalent to matrix, presented in the beginning of this section.

To construct general parameterized matrices, we simply get suitable number of Hadamard matrices of suitable dimensions, and next multiply columns of candidates for A_i with different parameters. Multiplying the rows of A_i, or multiplying the rows or columns of B has no meaning (since we can trivially remove this parameter in the last matrix, as explained in previous section).

Note that similar proposition hold for orthogonal matrices (and even for matrices, which we can call complex orthogonal matrices), but we not obtain an interesting result.

5.2.2 Generalize Paley Construction II

Next we shall give a result presented in [9], which shows, that Paley construction can be applied to construct bigger Jacket matrices. Together with results 4.2.1 and Kronecker product this new construction gives as a third method for producing parameterized Jacket matrices. Unfortunately we use very specific matrix, which we shall define later and call it "reciprocal Jacket Conference matrix", and we do not know that there are infinite number of such matrices.

When we generalize the element type, not usual inner products are used, but complex one. Here we shall demonstrate that we can replace inner product with more unusual non-symmetric operation - Jacket condition. First we need the following

Definition 3. *A $n \times n$ square matrix A is a Jacket Conference matrix, if the following conditions holds*

1. $a_{i,i} = 0$, *for* $i = 1, 2, \ldots, n$.
2. $a_{i,j} \neq 0$, *for all* $i, j \in \{1, 2, \ldots, n\}, i \neq j$.
3. $\sum_{i \in \{1,2,\ldots,n\} \setminus \{u,v\}} a_{u,i}.(a_{i,v})^{-1} = 0$, *for all* $u, v \in \{1, 2, \ldots, n\}, u \neq v$.

The matrices defined above, we shall use to replace the usual Conference matrices. In Paley construction it is required that matrix to be symmetric.

Only a special type of such matrix we can use in construction of this section. Now we shall introduce the term reciprocally-symmetric matrix A or shortly say reciprocal, if $a_{u,v} = (a_{v,u})^{-1}$, for all $u, v \in \{1, 2, \ldots, n\}, u \neq v$.

It is easy to check that the (35) continue to be true, if we replace C with reciprocal Jacket matrix, and also modify transpose $X^{\setminus\!\setminus}$ of all Jacket conference matrices by applying element-wise invert of non diagonal entries (and denote X'). Main difficult is to show that $(A \otimes C_m).(A'_n \otimes C'_m) = (mn - n)$. As a result of such construction we shall obtain a Jacket (not Conference) matrix.

It is good to show, that there exists a reciprocal Jacket Conference matrices. Similarly to Jacket matrices we can multiply rows and columns by nonzero constants, preserving properties of matrices. That is why we can consider only matrices, which first row and column consists only of ones.

Construct Reciprocal Jacket Conference Matrix of order 3 is obviously impossible. It is easy to construct the matrix of order 4 (see below). It is possible to show that matrix or order 5 does not exists. The case 6 is so large to be considered completely in the same way, but looking for matrices

with elements χ^i, where χ is primitive 6^{th} root of unity, and we can find 3 unequivalent matrices.

$$J_4 = \begin{pmatrix} * & 1 & 1 & 1 \\ 1 & * & i & -i \\ 1 & -i & * & i \\ 1 & i & -i & * \end{pmatrix} \text{ and } {}^1J_6 = \begin{pmatrix} * & 1 & 1 & 1 & 1 & 1 \\ 1 & * & 1 & 1 & -1 & -1 \\ 1 & 1 & * & -1 & \chi^1 & \chi^4 \\ 1 & 1 & -1 & * & \chi^4 & \chi^1 \\ 1 & -1 & \chi^5 & \chi^2 & * & 1 \\ 1 & -1 & \chi^2 & \chi^5 & 1 & * \end{pmatrix}$$

Here in a place of stars stays zeros. The second matrix ${}^2J_6$ is obtained by ${}^1J_6$ applying element-wise inversions, while the third matrix ${}^3J_6$ is well know symmetric conference matrix of order 6.

5.3 Circulant Jacket Matrices

Studying parameterized Jacket matrices is closely related to l.f.f. However, we can find other relations (no so closely), considering circulant Jacket matrices. The relation is as follow:

> Circulant Jacket matrices $\leftrightarrow$ Circulant Jacket equations $\leftrightarrow$ Invariant theory $\leftrightarrow$
> $\leftrightarrow$ Continuant polynomial $\leftrightarrow$ Recurrence relations $\leftrightarrow$ Linear-fractional function

Even this sequence of relations seems very long, it is very essential, since it give us an idea to attack Conjecture 1 in Section 5.1. Some results in this direction can be found in [19] and [14].

Note, that this conjecture can be attack also in different way (not presented in this paper), using Jacket matrices. The idea is to extend a system of Jacket equations with orthogonal equations. Really, the circulant Hadamard matrix must be not only Jacket, but also an orthogonal one.

5.3.1 The Main Step

The main step which we plan to apply to succeed is explained in this section. We do not know that, it can be apply easily even if it is possible.

Consider the set of polynomials $p(a_1, a_2, \ldots, a_n)$ over Q and invariant under actions of some subgroup $G < S_n$, i.e. such that

$$\forall \sigma \in G : p(a_1, a_2, \ldots, a_n) = p(a_{\sigma(1)}, a_{\sigma(1)}, \ldots, a_{\sigma(n)})$$

form a ring, and it is called the ring of invariants of G. It is known that this ring is finitely generated, and its properties are studied in invariant theory [16]. Consider ring R of invariants of G. It is finitely generated. If we have some information about some polynomials from R, then it is naturally to suppose, that we can find some relations, about the other set of equations.

In our case we shall select G as a dihedral group of order n. We shall demonstrate that if the circulant Hadamard matrix exists, then it must be satisfied a system of polynomial equations from - this will give as necessary information, about the ring. Similarly we shall map a specifically generated recurrence sequences with system or equations of the same ring of invariants of G.

5.3.2 Jacket circulant equations

In this section we shall consider circulant Jacket matrices, i.e. the matrices of the form

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \\ \ddots & & \ddots & & \ddots \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}.$$

The Jacket condition for this matrix is

$$\sum_{i=1}^{n} \frac{a_i}{a_{i+s}} = 0, \text{ for } s = 1, 2, \dots n-1. \tag{37}$$

Considered equation (37) and also in next equation we reduce indexes modulo n, to be in the interval $\{1, 2, \dots, n\}$.

If we denote $r_i := a_i/a_{i-1}$, for $i = 1, 2, \dots, n$ then (37) can be written as

$$\sum_{i=1}^{n} \prod_{j=0}^{s} r_{i+j} = 0, \text{ for } s = 1, 2, \dots n-1, \tag{38}$$

where by definition the following condition also holds

$$\prod_{i=1}^{n} r_i = 1. \tag{39}$$

Equation (38) and (39) are introduces by Goran Bjorck, and they are connected with bi-unimodular sequences [1]. Five years later it is shown [6], that this equations also determine the complex Hadamard matrices. As we show they are even Jacket ones. Some additional information one can find in [2].

5.3.3 The Recurrence Relation

The matrix

$$M_{q_1,q_2,\dots,q_n}(x,y) := \begin{pmatrix} q_1 & x & 0 & \dots & 0 & -y \\ -x & q_2 & x & \dots & 0 & 0 \\ 0 & -x & q_3 & \dots & 0 & 0 \\ & \vdots & & \ddots & \vdots & \\ 0 & 0 & 0 & \dots & q_{n-1} & x \\ y & 0 & 0 & \dots & -x & q_n \end{pmatrix}$$

is generalization of $M_{q_1,q_2,\dots,q_n}(1,0)$ presented in [15].

We are interested from determinant of this matrix, which is polynomial of $q_1, \dots, q_n, x, y$. First we shall consider the case when $y = 0$, we can consider $x = 1$ instead of general x. The last is not essential restriction, since the replacement $1 \to x$ convert the polynomial to such with homogeneous coordinates. So we can introduce x in the end of calculations.

We can present easily a determinant with recurrence formula. We must expand it along to the last column. So

$$\det M_{q_1,q_2,\dots,q_n}(x,0) = q_n.\det M_{q_1,q_2,\dots,q_{n-1}}(x,0) + \det M_{q_1,q_2,\dots,q_{n-2}}(x,0). \tag{40}$$

Note one interesting lemma, proved by Euler

Lemma 15.

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{\ddots}{+\frac{1}{q_n}}}}} = \frac{\det\ M_{q_1,q_2,\ldots,q_n}(1,0)}{\det\ M_{q_2,q_3,\ldots,q_n}(1,0)}$$

■

The prove can be easily obtained by induction.

In our problem we need a cyclic like matrix, such that the obtained polynomials to be invariant under G. So we shall consider the matrix $M_{q_1,q_2,\ldots,q_n}(1,1)$. We shall deal with heuristic considerations in next lemma, and so we do not try to determine the signs (actually this is easy).

Lemma 16. *The polynomial*

$$\det\ M_{q_1,q_2,\ldots,q_n}(1,1)$$

can be presented as

$$\lambda_1 + \lambda_2 + \lambda_3.q_n.\det\ M_{q_1,q_2,\ldots,q_{n-1}}(1,1) + \lambda_4.\det\ M_{q_1,q_2,\ldots,q_{n-2}}(1,1) + \lambda_5.\det\ M_{q_2,q_3,\ldots,q_{n-1}}(1,1)$$

for some $\lambda_i \in \{\pm 1\}$.

Proof: For regular matrix $A = (a_{i,j})$ the determinant is defined as follow

$$\det\ A = \sum_{\tau \in S_n} (-1)^{\tau} a_{i,\tau(i)} \tag{41}$$

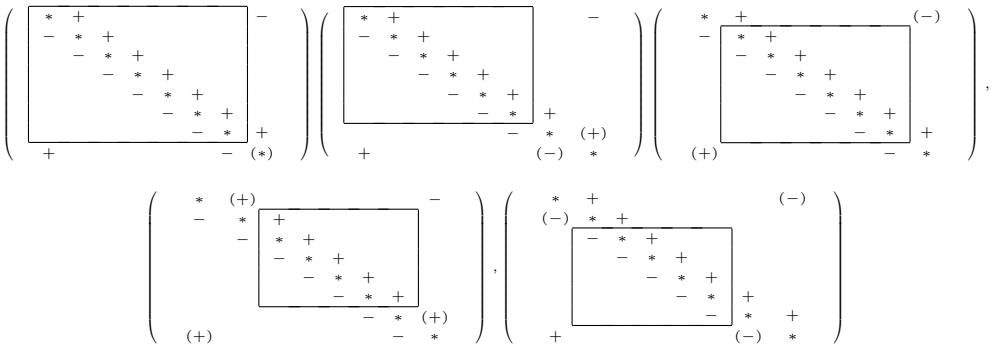
It is easy to show, that if $i_1, i_2, \ldots, i_k$, $1 \le i_1, i_2, \ldots, i_k \le n$ are different integers, and similarly about $j_1, j_2, \ldots, j_k$, and if denote $S_{\{(i_1,j_1),\ldots,(i_k,j_k)\}} := \{\tau \in S_n \,|\, \tau(i_s) = j_s, s = 1, 2, \ldots, k\}$, then it is easy to show, that

$$\det\ A = \pm \det\ A' \prod_{i=1}^{k} a_{i,\tau(i)} \tag{42}$$

where A' is a matrix obtained by removing rows $i_1, i_2, \ldots, i_n$, and columns $j_1, j_2, \ldots, j_n$ in A. Note, that the permutations in the set

$$S_n \quad \backslash S_{\{(n,n)\}} \backslash S_{\{(n,n-1),(n-1,n)\}} \backslash S_{\{(n,1),(1,n)\}} \quad \backslash S_{\{(n,1),(n-1,n),(1,2)\}} \backslash S_{\{(1,n),(2,1),(n,n-1)\}}$$

give only zero multiplications in $\det M_{q_2,q_3,\ldots,q_{n-1}}(1,1)$, according to definition (41). This can be checked directly. Now we can use (42). The considered above sets $S_{\{\cdot\}}$ correspond to the following situations, respectively:



Here with "+" and "−" we denote $+1$ and -1 respectively. We denote the elements q_i on main diagonal with "$*$", elements a_{i_s,j_s} with brackets "$(\cdot)$" and residue matrix M' with frame like this "$\boxed{\cdot}$".

In the last two cases we have lower and upper diagonal matrix, and so its determinant is multiplications of diagonal elements, i.e. $+1$ or -1. In the first 3 cases we have: $\det M_{q_1,q_2,\ldots,q_{n-1}}(1,0)$, $\det M_{q_1,q_2,\ldots,q_{n-2}}(1,0)$, $\det M_{q_2,q_3,\ldots,q_{n-2}}(1,0)$, respectively. ■

Using (40) this proposition shows, that $\det M_{q_2,q_3,\ldots,q_{n-2}}(1,1)$ can be calculated recursively. This is not usual recurrence relation, since q_i are different, but it is similar.

The essential step in this section is to show which terms occurs in definition (41).

Definition 4. *We shall say that the subset T of $\mathbb{Z}_n$ is <u>without odd holes</u>, if from $u \in T$, and $u+2k \in T$ it follows $\{u+1, u+2, \ldots, u+2k-1\} \cap T \neq \emptyset$.*

In other words, if we write indexes consequently it is not allowed to omit odd number of indexes in one stop. This must be considered also in "cyclic meaning".

Using this definition we can explain $\det M_{q_1,q_2,\ldots,q_n}(1,1)$. Similar proposition can be proved easily by induction, about $\det M_{q_1,q_2,\ldots,q_n}(1,0)$ (cf. [15]).

Proposition 17. *It is satisfied*

$$\det M_{q_1,q_2,\ldots,q_n}(1,1) = 2 + \sum_{s\in R} \prod_{i\in s} q_s$$

where R is set of all subset of $\{1,2,\ldots,n\}$ without odd holes.
Proof: Using definition of determinant (41), let calculate the coefficient of $q_{i_1} q_{i_2} \ldots q_{i_k}$. It is obvious that, to do this, we can replace all q_{i_s} with ones, and all other elements in the same row or columns with zero. Next we must replace the remaining q_i with zeros, and calculate the determinant. It is easily to show, that in such a way we shall multiply the determinants of matrices of the form

$$X = \begin{pmatrix} 0 & 1 & & & & & & \\ -1 & 0 & 1 & & & & & \\ & -1 & 0 & \ddots & & & & \\ & & \ddots & & & & & \\ & & & & & \ddots & & \\ & & & & \ddots & 0 & 1 & \\ & & & & & -1 & 0 & \end{pmatrix}$$

By induction it is easily to prove, that the determinant of even orders is 1 and odd orders is 0. So existence of odd holes lead to occurring of zero determinant. So the coefficient is 0. ■

The polynomial obtained in Proposition 17 is invariant under the action of G (dihedral group, defined in introduction). So if convert it to homogeneous polynomial $\det M_{q_1,q_2,\ldots,q_n}(x,x)$, then the coefficient at degrease of x would be also invariant.

The Main step presented in Section 5.3.1 follows (of course this is only idea up to now).

6 Acknowledgments

This research was supported by the Ministry of Knowledge Economy, Korea, under the ITFSIP (IT foreign Specialist Inviting Program) supervised by the IITA (Institute of Information Technology Advancement), C1012-0801-0001, and KRF D-2007-521-D00330, Korea.

References

[1] G. Bjorck **"Functions of modulus 1 on whose Fourier transforms have constant modulus, and "cyclic n-roots" "**, *Proceedings of the 1989 NATO Advanced Study Institute on "Recent Advances in Fourier Analysis and Its Applications"*, J. S. Byrnes & J. L. Byrnes, ed., 1990, pp.131-140.

[2] G. Bjorck, B. Saffari. **"New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries."** *C. R. Acad. Sci. Paris*, Ser. I Math. 320, No. 3, 1995, pp.319-324.

[3] Saad Bouguezel, M. Omair Ahmad, and M. N. S. Swamy **"A New Class of Reciprocal-Transpose Parametric Transforms"**, *TCAS-I - accepted 2008.*

[4] Delsarte, Ph., Goethals, J.M., and Seidel, J.J. **"Orthogonal matrices with zero diagonal"**, *Canadian Journal of Mathematics*, 23, 1971, pp.816-832.

[5] Carl Friedrich Gauss, **"Works about number theory"**, *Academy of sciences USSR*, 1959, pp.655-685. (in Russian)

[6] Uffe Haagerup, **"Cyclic p-roots of prime length p and related complex Hadamard matrices."**.

[7] Daeyeoul Kim, Ja Kyung Koo, Yoon Kyung Park **"On the elliptic curves modulo p"**, *Journal of Number Theory*, 128, 2008, pp.945-953.

[8] N. Koblitz, **"Introduction to Elliptic Curves and Modular Forms"**, *Springer-Verlag*, Berlin, 1984.

[9] Moon Ho Lee and Veselin Vl. Vavrek **"Generalizing Paley Construction II"** - *to prepare.*

[10] Moon Ho Lee and Veselin Vl. Vavrek **"Second order recurrences and Paley Conference Matrices"** - *to prepare.*

[11] Paley, R.E.A.C. **"On Orthogonal Matrices."**, *J. Math. and Phys.* 12, 1933, pp.311-320.

[12] J.M. Pollard, **"Theorems of Factorization and Primality Testing"**, *Proceedings of the Cambridge Philosophical Society* 76, 1974, pp.521-528.

[13] Silverman, Joseph H., **"The Arithmetic of Elliptic Curves"**, *Graduate Texts in Mathematics*, No. 106, Princeton University Press, 1992.

[14] Bernhard Schmidt **"Circulant Hadamard Matrices: Overcoming Non-Self-Conjugacy"**, - *submitted (≈1997).*

[15] S. V. Sizij, **"Lectures on number theory"**, *The textbook for the mathematical specialties*, Ekaterinburg: Ural university 'A. M. Gorkij', 1999, pp.35-38. (In russian)

[16] L. Smith, **"Polynomial Invariants of Finite Groups"**. *Wellesley*, MA, USA 1995.

[17] Lawrence Somer, **"Primes Having an Incomplete System of Residues for a Class of Second-Order Recurrences"**, *in Proc. Applications of Fibonacci Numbers*, 1988, pp.113-141.

[18] Z.H. Sun, **"On the theory of cubic residues and nonresidues"**, *Acta Arith.* 84, 1998, pp.291-335.

[19] R.J. Turyn **"Character sums and difference sets"**, *Pacific J. Math.* 15 (1965), pp.319-346.

[20] H.C. Williams, **"A $p+1$ method of factoring"**, *Math. Comp.*, 39, 1982, pp.225-234.

[21] Vavrek, V. and Zanten, A.J. van. **"Generating functions for finite fields and their applications to Paley type conference matrices I"**. *Technical Reports in Computer Science*, CS 04-02, IKAT, Maastricht, The Netherlands. ISSN 0922-8721, 2004.