Problems of Information Transmission, Vol. 38, No. 4, 2002, pp. 255–267. Translated from Problemy Peredachi Informatsii, No. 4, 2002, pp. 10–23.

INFORMATION THEORY AND CODING THEORY

New Sequences with Zero Autocorrelation

E. M. Gabidulin and V. V. Shorin

Received April 2, 2002

Abstract—New families of unimodular sequences of length $p = 3f+1$ with zero autocorrelation are described, p being a prime. The construction is based on employing Gauss periods. It is shown that in this case elements of the sequences are algebraic numbers defined by irreducible polynomials over $\mathbb{Z}$ of degree 12 (for the first family) and 6 (for the second family). In turn, these polynomials are factorized in some extension of the field $\mathbb{Q}$ into polynomials of degree, respectively, 4 and 2, which are written explicitly. For $p = 13$, using the exhaustive search method, full classification of unimodular sequences with zero autocorrelation is given.

1. INTRODUCTION

Let $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$ be a nonzero complex-valued sequence of length n.

Definition 1. A sequence is called delta-correlated (has zero autocorrelation) if it is orthogonal to all of its cyclic shifts:

$$R_{\boldsymbol{x}}(k) = \sum_{i=0}^{n-1} x_i x^*_{(i+k) \bmod p} = 0, \quad k = 1, 2, \ldots, n-1. \tag{1}$$

Here, x^* means complex conjugation.

Let ζ be a primitive nth root of unity, i.e., $\zeta^n = 1$, $\zeta^i \neq 1$, $0 < i < n$.

Definition 2. The unitary matrix

$$\boldsymbol{W} = \frac{1}{\sqrt{n}} \left[\zeta^{ij}\right], \quad i, j = 0, 1, \ldots, n-1,$$

is called the matrix of a (direct) nth-order discrete Fourier transform.

Definition 3. The vector

$$\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}) = \boldsymbol{x}\boldsymbol{W}$$

is called the Fourier image of vector $\boldsymbol{x}$.

The inverse Fourier transform is defined by the matrix

$$\boldsymbol{W}^H = \frac{1}{\sqrt{n}} \left[\zeta^{-ij}\right], \quad i, j = 0, 1, \ldots, n-1.$$

Theorem 1 [1]. *A sequence $\boldsymbol{x}$ is delta-correlated if and only if all components of its Fourier image are of the same magnitude:*

$$|y_j|^2 = \frac{\sum\limits_{i=0}^{n-1} |x_i|^2}{n}, \quad j = 0, 1, \ldots, n-1.$$

Theorem 1 yields a classification of the whole class of delta-correlated sequences and a method of constructing them: one takes a vector $\boldsymbol{y}$ with components of the same magnitude and applies the inverse Fourier transform.

0032-9460/02/3804-0255 $27.00

Definition 4. A sequence $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$ is called phase-modulated, or unimodular, if all elements of the sequence equal 1 in magnitude, i.e., lie on the unit circle.

Let $\boldsymbol{x}$ be a unimodular delta-correlated sequence. Then the following transformations of $\boldsymbol{x}$ give new unimodular delta-correlated sequences $\boldsymbol{x}' = (x'_0, x'_1, \ldots, x'_{n-1})$ (see [1]):

$$\begin{aligned}
&\boldsymbol{x}' = a\boldsymbol{x}, \quad |a| = 1;\\
&\boldsymbol{x}' = \{x'_i\}, \quad x'_i := x_{(i+1) \bmod n}, \quad i = 0, 1, \ldots, n-1;\\
&\boldsymbol{x}' = \{x'_i\}, \quad x'_i := x_{(di) \bmod n}, \quad i = 0, 1, \ldots, n-1, \quad \gcd(d, n) = 1;\\
&\boldsymbol{x}' = \{x'_i\}, \quad x'_i := x^*_i, \quad i = 0, 1, \ldots, n-1;\\
&\boldsymbol{x}' = \{x'_i\}, \quad x'_i := x_i\zeta^{is}, \quad i = 0, 1, \ldots, n-1, \quad s = 0, 1, \ldots, n-1;\\
&\boldsymbol{x}' = \boldsymbol{x}\boldsymbol{W}.
\end{aligned}$$

These transformations generate a group, and we can introduce the equivalence relation with respect to this group.

Delta-correlated sequences $\boldsymbol{x}$ and $\boldsymbol{x}'$ are equivalent, $\boldsymbol{x} \sim \boldsymbol{x}'$, if and only if one of them can be obtained from the other by a series of these transformations.

Thus, all unimodular delta-correlated sequences are split into equivalence classes.

Below, we only consider the case where $n = p$, p being a prime.

For the case of unimodular delta-correlated sequences of prime length, it is known that there are finitely many equivalence classes (see [1, 2]).

The problem arises to describe all equivalence classes and propose methods for constructing unimodular delta-correlated sequences.

For $p = 2$, 3, and 5, there is exactly one equivalence class.

For any prime $p \geq 7$, methods are known to construct two equivalence classes for $p \equiv 1 \pmod 4$ and one equivalence class for $p \equiv 3 \pmod 4$ (see Section 5).

As far as we know, there is no information on any other equivalence classes in the literature.

In the present paper, we propose a method for constructing equivalence classes based on using Gauss periods. In details, we consider the case where the length of the sequence is $p = 3f + 1$.

For the particular case $p = 13$, using exhaustive search, we obtain full classification, i.e., all equivalence classes are found.

2. REDUCTION TO A SYSTEM OF ALGEBRAIC EQUATIONS

In the sequel, as a representative of a class, we consider a sequence with 1 in the first position ($x_0 = 1$); in any class, such representatives exist.

To determine equivalence classes, we have to find all unimodular solutions of system (1) with $x_0 = 1$ and then select nonequivalent solutions.

Note that, for unimodular sequences, we have

$$x^*_i = \frac{1}{x_i};$$

therefore, system (1) can be rewritten as the system of equations

$$\sum_{i=0}^{p-1} \frac{x_i}{x_{(i+k) \bmod p}} = 0, \quad k = 1, 2, \ldots, p-1. \tag{2}$$

If we multiply each equation in (2) by the product $\prod_{i=0}^{p-1} x_i$, we get the system of algebraic equations

$$\sum_{i=0}^{p-1}\left(x_i \prod_{\substack{j=0 \\ j\neq(i+k) \bmod p}}^{j=p-1} x_j\right) = 0, \quad k = 1, 2, \ldots, p-1. \tag{3}$$

The polynomial ideal defined by this system is a union of irreducible components. For prime p, the dimension of each component is zero [2]. In other words, there are finitely many equivalence classes.

Unimodular solutions ($|x_i| = 1$, $\forall i$) of this system form a unimodular delta-correlated sequence.

Generally, all components of a solution of system (3) can be found by methods of exclusion theory [3–5]. In one of its possible versions, the Gröbner basis of the polynomial ideal generated by system (3) is used.

Then, for this system, the last polynomial in the Gröbner basis (with respect to the lexicographic order) is a polynomial in one variable, the previous polynomial is (or polynomials are) in two variables, etc.

In this case, solving system (3) reduces to finding the roots of a one-variable polynomial with integer coefficients; hence, all roots are *algebraic* numbers.

When we find a unimodular root (if it exists), we pass to the previous equation and substitute the value found. Thus, we obtain an equation with algebraic coefficients. If it has a unimodular root, we again pass to the previous step, etc. If we find a unimodular root at each step, the sequence obtained is precisely a unimodular delta-correlated sequence.

Remark. All x_i, $i = 1, \ldots, p-1$, are algebraic numbers.

In the general case, eliminating variables is very difficult. For instance, for $p = 13$, at the last step we obtain a polynomial of degree of the order of $2^{2^{12}}$. Sometimes, the problem is greatly simplified if one considers sequences of a special form. We suggest sequences composed of several groups of equal numbers. The set of indices $[0, 1, 2, \ldots, p-1]$ is divided into disjoint subsets, one of them consisting solely of zero. Coordinates with indices from the same subset are assumed to be equal. As such subsets, we suggest to use *Gauss cyclotomic* classes.

3. GAUSS CYCLOTOMIC CLASSES AND GAUSS PERIODS

Let a prime p be represented as $p - 1 = ef$ and let g be a primitive element modulo p.

The set of indices $[0, 1, 2, \ldots, p-1]$ is divided into the Gauss cyclotomic classes as follows: the zero cyclotomic class

$$0 = \{0\}$$

and cyclotomic classes

$$G_i = \left\{g^{e+i}, g^{2e+i}, \ldots, g^{ef+i} = g^i\right\}, \quad i = 0, 1, \ldots, e-1.$$

Define the algebraic numbers $\eta_0, \eta_1, \ldots, \eta_{e-1}$, called the Gauss f-periods [3, 6]:

$$\eta_i = \sum_{s\in G_i} \zeta^s = \sum_{k=1}^{f} \zeta^{g^{ek+i}}, \quad i = 0, 1, \ldots, e-1. \tag{4}$$

Let us state some necessary properties of the Gauss periods:

1. The sequence $(\eta_0, \eta_1, \ldots, \eta_{e-1})$ has the same periodic autocorrelation coefficients:

$$\sum_{j=0}^{e-1} \eta_j \eta^*_{(j+s) \bmod e} = \begin{cases} p-f, & s=0; \\ -f, & s=1,2,\ldots,p-1. \end{cases} \tag{5}$$

2. If f is even, the product $\eta_s \eta_{(s+j) \bmod e}$, $s=0,1,\ldots,e-1$, $j=0,1,\ldots,e-1$, can be represented in the form

$$\eta_s \eta_{(s+j) \bmod e} = c_j + a_{0,j}\eta_s + a_{1,j}\eta_{s+1} + \ldots + a_{e-1,j}\eta_{(s+e-1) \bmod e}, \tag{6}$$

where $c_j = 0$ and $a_{0,j} + a_{1,j} + \ldots + a_{e-1,j} = f$ for all j except for $j=0$. In the latter case, $c_0 = f$ and $a_{0,0} + a_{1,0} + \ldots + a_{e-1,0} = f-1$.

4. SEQUENCES BASED ON GAUSS PERIODS

As new variables, we take e numbers $z_0, z_1, \ldots, z_{e-1}$ of magnitude 1. We will construct sequences $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$ as follows: define their coordinates to be

$$\begin{aligned} &x_0 = 1, \\ &x_j = z_s, \quad j \in G_s, \quad s = 0,1,\ldots,e-1. \end{aligned} \tag{7}$$

In this case, we obtain only e different equations in system (2) in e unknowns z_s. Different equations are, for instance, those in rows $1, g, g^2 \bmod p, \ldots, g^{e-1} \bmod p$ of system (2). Any other equation coincides with one of them.

It is not too difficult to write the resulting system for any particular p, but the general form strongly depends on the structure of Gauss cyclotomic classes. We will obtain another system in an explicit form, which will be equivalent to (2).

Let us find the Fourier image of a sequence $\boldsymbol{x}$ from (7):

$$y_0 = \frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} x_s = \frac{1}{\sqrt{p}}(1 + fz_0 + fz_1 + \ldots + fz_{e-1}),$$

$$y_j = \frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} x_s \zeta^{sj} = \frac{1}{\sqrt{p}} \left(1 + \left(\sum_{s \in G_0} \zeta^{sj}\right) z_0 + \left(\sum_{s \in G_1} \zeta^{sj}\right) z_1 + \ldots + \left(\sum_{s \in G_{e-1}} \zeta^{sj}\right) z_{e-1}\right),$$

where $j = 1,2,\ldots,p-1$.

Taking definition (4) into account, one easily sees that

$$y_0,\ y_g,\ \ldots,\ y_{g^{e-1} \bmod p}$$

are different Fourier components, and the coefficients of unknowns z_s are the Gauss periods (4):

$$\begin{aligned} \sqrt{p}\, y_0 &= 1 + fz_0 + fz_1 + fz_2 + \ldots + fz_{e-1}, \\ \sqrt{p}\, y_g &= 1 + \eta_0 z_0 + \eta_1 z_1 + \eta_2 z_2 + \ldots + \eta_{e-1} z_{e-1}, \\ \sqrt{p}\, y_{g^2 \bmod p} &= 1 + \eta_1 z_0 + \eta_2 z_1 + \eta_3 z_2 + \ldots + \eta_0 z_{e-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sqrt{p}\, y_{g^{e-1} \bmod p} &= 1 + \eta_{e-1} z_0 + \eta_0 z_1 + \eta_1 z_2 + \ldots + \eta_{e-2} z_{e-1}. \end{aligned}$$

Since all y and z are of magnitude 1 by the condition and since $z^* = 1/z$, after passing to squared magnitudes on either sides of the equations, using relation (5), and making algebraic

transformations, for an even f we get

$$\psi = \sum_{s=0}^{e-1}\left(z_s + \frac{1}{z_s}\right) + \sum_{0\le s<m\le e-1} f\left(\frac{z_s}{z_m} + \frac{z_m}{z_s}\right) + e(f-1) = 0,$$
$$\varphi_k = \sum_{s=0}^{e-1}\eta_{s+k}\left(z_s + \frac{1}{z_s}\right) + \sum_{0\le s<m\le e-1}\eta_{s+k}\eta_{s+m}\left(\frac{z_s}{z_m} + \frac{z_m}{z_s}\right) - (f-1) = 0, \qquad (8)$$
$$k = 0, 1, \ldots, e-1.$$

In fact, the equation $\psi = 0$ can be omitted since it is a linear combination of the others.

Similarly, we can obtain a system for odd f.

System (8) can further be simplified if we replace the products $\eta_{s+k}\eta_{m+k}$ using relations (6).

After eliminating variables, a solution is obtained in the form of a product of irreducible polynomials over $\mathbb{Q}(\eta_0)$. Of these polynomials, we may discard those without roots of magnitude 1.

5. KNOWN SEQUENCES

All sequences of prime length known to the authors can be described using Gauss periods.

5.1. Case $e = 2$

In this case, two equivalence classes are known if $p \equiv 1 \pmod 4$ and one equivalence class if $p \equiv 3 \pmod 4$ (see, e.g., [1, 7]).

In terms of the Gauss periods, the set G_0 precisely consists of quadratic residues modulo p and G_1 consists of quadratic nonresidues.

5.1.1. Case $p \equiv 1 \pmod 4$. In this case, we have

$$e = 2, \qquad f = (p-1)/2 \quad \text{even},$$
$$\eta_0 = \sum_{i\in G_0}\zeta^i = (\sqrt{p}-1)/2,$$
$$\eta_1 = \sum_{i\in G_1}\zeta^i = (-\sqrt{p}-1)/2.$$

System (8) has the following form:

$$\psi = \left(z_0 + \frac{1}{z_0}\right) + \left(z_1 + \frac{1}{z_1}\right) + f\left(\frac{z_0}{z_1} + \frac{z_1}{z_0}\right) + e(f-1) = 0,$$
$$\varphi_0 = \eta_0\left(z_0 + \frac{1}{z_0}\right) + \eta_1\left(z_1 + \frac{1}{z_1}\right) + \eta_0\eta_1\left(\frac{z_0}{z_1} + \frac{z_1}{z_0}\right) - (f-1) = 0,$$
$$\varphi_1 = \eta_1\left(z_0 + \frac{1}{z_0}\right) + \eta_0\left(z_1 + \frac{1}{z_1}\right) + \eta_0\eta_1\left(\frac{z_0}{z_1} + \frac{z_1}{z_0}\right) - (f-1) = 0.$$

Eliminating the variable z_1 leads to the following relations:

1. $z_1 = z_0$. In this case, z_0 is a root of the irreducible polynomial over $\mathbb{Z}$

$$g(x) = x^2 + (2f-1)x + 1.$$

This polynomial has no unimodular roots and should be discarded.

2. $z_1 = \dfrac{1}{z_0}$. In this case, z_0 is a root of the irreducible polynomial over $\mathbb{Z}$

$$g(x) = \frac{f}{2}x^4 + x^3 + (f-1)x^2 + x + \frac{f}{2}. \tag{9}$$

In turn, in the extended field $\mathbb{Q}(\eta_0)$, this polynomial is factorized into the product of polynomials of degree two:

$$g(x) = (\eta_0 x^2 - x + \eta_0)(\eta_1 x^2 - x + \eta_1).$$

The roots of the first factor are of the form

$$z_0 = \cos A_1 + \mathrm{i}\,\sin A_1, \qquad z_1 = \cos A_1 - \mathrm{i}\,\sin A_1, \tag{10}$$

where

$$\cos A_1 = 1/(2\eta_0) = \frac{1}{\sqrt{p}-1}.$$

They generate a delta-correlated sequence $\boldsymbol{x} = (x_0, \ldots, x_{p-1})$ from the first equivalence class:

$$x_0 = 1, \qquad x_i = \begin{cases} z_0, & i \in G_0, \\ z_1, & i \in G_1. \end{cases}$$

Similarly, the roots of the second equation are of the form

$$z_0 = \cos A_2 + \mathrm{i}\,\sin A_2, \qquad z_1 = \cos A_2 - \mathrm{i}\,\sin A_2, \tag{11}$$

where

$$\cos A_2 = 1/(2\eta_1) = -\frac{1}{\sqrt{p}+1}.$$

They generate a delta-correlated sequence $\boldsymbol{x} = (x_0, \ldots, x_{p-1})$ from the second equivalence class.

5.1.2. Case $p \equiv 3 \pmod 4$. In this case, we have

$$\begin{aligned} e &= 2, \qquad f = (p-1)/2 \quad \text{odd}, \\ \eta_0 &= \sum_{i \in G_0} \zeta^i = (-1 + \mathrm{i}\sqrt{p})/2, \\ \eta_1 &= \sum_{i \in G_1} \zeta^i = (-1 - \mathrm{i}\sqrt{p})/2. \end{aligned}$$

System (8) has the form

$$\begin{aligned} \psi &= \left(z_0 + \frac{1}{z_0}\right) + \left(z_1 + \frac{1}{z_1}\right) + f\left(\frac{z_0}{z_1} + \frac{z_1}{z_0}\right) + e(f-1) = 0, \\ \varphi_0 &= \eta_0 z_0 + \eta_1 \frac{1}{z_0} + \eta_1 z_1 + \eta_0 \frac{1}{z_1} + \eta_0^2 \frac{z_0}{z_1} + \eta_1^2 \frac{z_1}{z_0} - (f-1) = 0, \\ \varphi_1 &= \eta_1 z_0 + \eta_0 \frac{1}{z_0} + \eta_0 z_1 + \eta_1 \frac{1}{z_1} + \eta_1^2 \frac{z_0}{z_1} + \eta_0^2 \frac{z_1}{z_0} - (f-1) = 0. \end{aligned}$$

Elimination of the variable z_1 implies that z_0 is a root of the polynomial

$$g(x) = (x-1)\left(\frac{p+1}{4}x^2 + \frac{p-1}{2}x + \frac{p+1}{4}\right)(*),$$

where $(*)$ stands for a polynomial with no unimodular roots. One may take $z_0 = 1$. Then z_1 is a root of the polynomial

$$h(x) = \frac{p+1}{4}x^2 + \frac{p-1}{2}x + \frac{p+1}{4},$$

that is,

$$z_1 = \cos A + \mathrm{i}\,\sin A \quad \text{or} \quad z_1 = \cos A - \mathrm{i}\,\sin A, \qquad \cos A = -\frac{p-1}{p+1}.$$

The only equivalence class is formed by the delta-correlated sequence $\boldsymbol{x} = (x_0, \ldots, x_{p-1})$ with

$$x_0 = 1, \quad x_i = \begin{cases} z_0 = 1, & i \in G_0, \\ z_1 = \cos A + \mathrm{i}\,\sin A, & i \in G_1. \end{cases}$$

5.2. Case $e = (p-1)/2$, $f = 2$

In this case, two equivalence classes are known if $p \equiv 1 \pmod 4$ and one equivalence class if $p \equiv 3 \pmod 4$ (see, e.g., [7, 8]).

If $p \equiv 1 \pmod 4$, then a representative of the first class is the sequence

$$x_i = \zeta^{i^2}, \quad i = 0, 1, \ldots, p-1,$$

and that of the second class is

$$x_i = \zeta^{si^2}, \quad i = 0, 1, \ldots, p-1,$$

where s is a quadratic nonresidue modulo p.

If $p \equiv 3 \pmod 4$, then a representative of the only known equivalence class is the sequence

$$x_i = \zeta^{i^2}, \quad i = 0, 1, \ldots, p-1.$$

6. METHOD FOR CONSTRUCTING SEQUENCES FOR $e = 3$

In this section, we describe a new infinite family of unimodular sequences with zero autocorrelation.

Let a prime p have the form $p = 3f + 1$; i.e., f is even. Let g be a primitive root modulo p. In this case, the Gauss cyclotomic classes are defined as

$$\begin{aligned} 0 &= \{0\}, \\ G_0 &= (g^3, g^6, g^9, \ldots, g^{3f} = 1) && \pmod p, \\ G_1 &= (g^{3+1}, g^{6+1}, g^{9+1}, \ldots, g^{3f+1} = g) && \pmod p, \\ G_2 &= (g^{3+2}, g^{6+2}, g^{9+2}, \ldots, g^{3f+2} = g^2) && \pmod p. \end{aligned}$$

The corresponding Gauss f-periods

$$\eta_0 = \sum_{i \in G_0} \zeta^i, \qquad \eta_1 = \sum_{i \in G_1} \zeta^i, \qquad \eta_2 = \sum_{i \in G_2} \zeta^i$$

are real numbers. Moreover, the number

$$s = \eta_0 \eta_1 \eta_2$$

is integer.

Let us choose the elements of a desired unimodular delta-correlated sequence as follows:

$$\begin{aligned} x_0 &= 1, \\ x_i &= z_0, \quad i \in G_0, \\ x_i &= z_1, \quad i \in G_1, \\ x_i &= z_2, \quad i \in G_2, \\ |z_0| &= |z_1| = |z_2| = 1. \end{aligned} \tag{12}$$

Then system (8) reduces to the following system of algebraic equations in three unknowns:

$$\begin{aligned} \psi &= f\left(\frac{z_0}{z_1}+\frac{z_1}{z_0}\right)+f\left(\frac{z_1}{z_2}+\frac{z_2}{z_1}\right)+f\left(\frac{z_2}{z_0}+\frac{z_0}{z_2}\right) \\ &\quad +\left(z_0+\frac{1}{z_0}\right)+\left(z_1+\frac{1}{z_1}\right)+\left(z_2+\frac{1}{z_2}\right)+e(f-1)=0, \\ \varphi_0 &= \eta_0\eta_1\left(\frac{z_0}{z_1}+\frac{z_1}{z_0}\right)+\eta_1\eta_2\left(\frac{z_1}{z_2}+\frac{z_2}{z_1}\right)+\eta_2\eta_0\left(\frac{z_2}{z_0}+\frac{z_0}{z_2}\right) \\ &\quad +\eta_0\left(z_0+\frac{1}{z_0}\right)+\eta_1\left(z_1+\frac{1}{z_1}\right)+\eta_2\left(z_2+\frac{1}{z_2}\right)-(f-1)=0, \\ \varphi_1 &= \eta_1\eta_2\left(\frac{z_0}{z_1}+\frac{z_1}{z_0}\right)+\eta_2\eta_0\left(\frac{z_1}{z_2}+\frac{z_2}{z_1}\right)+\eta_0\eta_1\left(\frac{z_2}{z_0}+\frac{z_0}{z_2}\right) \\ &\quad +\eta_1\left(z_0+\frac{1}{z_0}\right)+\eta_2\left(z_1+\frac{1}{z_1}\right)+\eta_0\left(z_2+\frac{1}{z_2}\right)-(f-1)=0, \\ \varphi_2 &= \eta_2\eta_0\left(\frac{z_0}{z_1}+\frac{z_1}{z_0}\right)+\eta_0\eta_1\left(\frac{z_1}{z_2}+\frac{z_2}{z_1}\right)+\eta_1\eta_2\left(\frac{z_2}{z_0}+\frac{z_0}{z_2}\right) \\ &\quad +\eta_2\left(z_0+\frac{1}{z_0}\right)+\eta_0\left(z_1+\frac{1}{z_1}\right)+\eta_1\left(z_2+\frac{1}{z_2}\right)-(f-1)=0, \end{aligned}$$

Elimination theory yields, for each p, two irreducible polynomials over $\mathbb{Z}$ of degree, respectively, 12 and 6. Their roots generate the delta-correlated sequence. These polynomials are found explicitly but their coefficients are expressed through p and f in a too complicated way and are not presented here.

In turn, further factorization of these polynomials into polynomials of degrees 4 and 2 in the extended field $\mathbb{Q}(\eta_0)$ is possible. Let us present the decompositions.

Polynomials of degree 12 have the following three factors of degree 4:

$$\begin{aligned} &sz^4-(2s-(f+1)(\eta_0+\eta_0^2))z^3+((2f-1)(\eta_0+\eta_0^2)-3s)z^2-(2s-(f+1)(\eta_0+\eta_0^2))z+s, \\ &sz^4-(2s-(f+1)(\eta_1+\eta_1^2))z^3+((2f-1)(\eta_1+\eta_1^2)-3s)z^2-(2s-(f+1)(\eta_1+\eta_1^2))z+s, \\ &sz^4-(2s-(f+1)(\eta_2+\eta_2^2))z^3+((2f-1)(\eta_2+\eta_2^2)-3s)z^2-(2s-(f+1)(\eta_2+\eta_2^2))z+s. \end{aligned}$$

Each of the polynomials has two conjugate unimodular roots, which are used in the sequel to construct sequences, and two nonunimodular roots, which we do not need.

Polynomials of degree 6 have the following three factors of degree 2:

$$\begin{aligned} &Az^2-(B-(f-1)(\eta_0+\eta_0^2))z+A, \\ &Az^2-(B-(f-1)(\eta_1+\eta_1^2))z+A, \\ &Az^2-(B-(f-1)(\eta_2+\eta_2^2))z+A, \end{aligned}$$

where the integer coefficients A and B are defined by the relations

$$A=\frac{f^3-s}{p}, \qquad B=3\frac{f^3-s}{p}-f+s.$$

Each of the polynomials has two conjugate unimodular roots, which are used in the sequel to construct sequences.

The first equivalence class is constructed with the help of the roots of polynomials of degree 4. The second equivalence class is constructed using the roots of polynomials of degree 2. The construction process does not depend on a class.

To compose a unimodular delta-correlated sequence, we have to take as z_0, z_1, and z_2 in (12) one unimodular root of each of the three polynomials. Some triples of such roots do not form required sequences. For instance, if a triple (z_0, z_1, z_2) is suitable, then the triples (z_1, z_2, z_0) and (z_2, z_0, z_1) are also suitable but (z_0, z_1, z_2^*) and (z_0, z_2, z_1) are not. It is possible to give a deterministic algorithm for the choice (z or z^*) and order of roots but, for the case $e = 3$, it is simpler to choose one sequence from the eight: as z_0, we may take any root; then there are two variants to choose from, either $(z_0, z_1^{(*)}, z_2^{(*)})$ or $(z_0, z_2^{(*)}, z_1^{(*)})$; and then four variants: which of the conjugate roots to take as z_1 and z_2.

7. CASE $p = 13$

In this case, *all* equivalence classes of unimodular delta-correlated sequences of length 13 are found. Both the above-described and numerical methods are used. The following results are obtained.

7.1. Case $e = 2$

Previously known sequences of the form

$$\boldsymbol{x} = \{1, z_0, z_1, z_0, z_0, z_1, z_1, z_1, z_1, z_0, z_0, z_1, z_0\},$$

belong to two equivalence classes, both consisting of 338 solutions. The solutions are defined by the roots of the polynomial (see (9))

$$g(x) = 3x^4 + x^3 + 5x^2 + x + 3.$$

The sequence that defines the first class (see (10)) is

$$z_0 = \exp(\mathrm{i}\, 4.931261595868),$$
$$z_1 = \exp(\mathrm{i}\, 1.351923711311).$$

The sequence that defines the second class (see (11)) is

$$z_0 = \exp(\mathrm{i}\, 4.318485428757),$$
$$z_1 = \exp(\mathrm{i}\, 1.964699878422).$$

7.2. Case $e = 3$

There are two equivalence classes, consisting of 1014 solutions of the form

$$\boldsymbol{x} = \{1, z_0, z_1, z_1, z_2, z_0, z_2, z_2, z_0, z_2, z_1, z_1, z_0\}.$$

The solutions are defined by the roots of the polynomials

$$g_{3,1}(x) = x^{12} + 14x^{11} - 12x^{10} - 38x^9 + x^8 - 25x^7 - 51x^6 - 25x^5 + x^4 - 38x^3 - 12x^2 + 14x + 1,$$
$$g_{3,2}(x) = 25x^6 + 45x^5 + 63x^4 + 59x^3 + 63x^2 + 45x + 25.$$

The sequence that defines the first class is

$$z_0 = \exp(\mathrm{i}\,4.961837311319),$$
$$z_1 = \exp(\mathrm{i}\,3.829123080261),$$
$$z_2 = \exp(\mathrm{i}\,0.887313301823).$$

The sequence that defines the second class is

$$z_0 = \exp(\mathrm{i}\,2.520358681774),$$
$$z_1 = \exp(\mathrm{i}\,4.209262236495),$$
$$z_2 = \exp(\mathrm{i}\,1.164371390059).$$

7.3. Case $e = 4$

There are two equivalence classes, consisting of 1352 solutions of the form

$$\boldsymbol{x} = \{1, z_0, z_1, z_0, z_2, z_1, z_1, z_3, z_3, z_0, z_2, z_3, z_2\}.$$

The solutions are defined by the roots of the polynomial

$$\begin{aligned} g_{4,1}(x) = {} & 1839267x^{48} + 14319504x^{47} + 134248644x^{46} + 155077527x^{45} \\ & - 1190920748x^{44} - 5275988402x^{43} - 8760573556x^{42} + 3926331880x^{41} \\ & + 58467147254x^{40} + 167525956116x^{39} + 339395597762x^{38} + 581186642764x^{37} \\ & + 663905335340x^{36} + 1026847512558x^{35} + 1910401463504x^{34} - 93533381127x^{33} \\ & - 2228273627848x^{32} - 1341693048892x^{31} + 270433926621x^{30} - 3520114694036x^{29} \\ & - 2499519303004x^{28} + 939973661496x^{27} + 2445009600764x^{26} + 1502961402072x^{25} \\ & + 1781778818664x^{24} + 1502961402072x^{23} + 2445009600764x^{22} + 939973661496x^{21} \\ & - 2499519303004x^{20} - 3520114694036x^{19} + 270433926621x^{18} - 1341693048892x^{17} \\ & - 2228273627848x^{16} - 93533381127x^{15} + 1910401463504x^{14} + 1026847512558x^{13} \\ & + 663905335340x^{12} + 581186642764x^{11} + 339395597762x^{10} + 167525956116x^{9} \\ & + 58467147254x^{8} + 3926331880x^{7} - 8760573556x^{6} - 5275988402x^{5} \\ & - 1190920748x^{4} + 155077527x^{3} + 134248644x^{2} + 14319504x + 1839267. \end{aligned}$$

The sequence that defines the first class is

$$z_0 = \exp(\mathrm{i}\,0.828308747773),$$
$$z_1 = \exp(\mathrm{i}\,2.309890279894),$$
$$z_2 = \exp(\mathrm{i}\,4.511268307248),$$
$$z_3 = \exp(\mathrm{i}\,6.191224200386).$$

The sequence that defines the second class is

$$z_0 = \exp(\mathrm{i}\,5.227849017149),$$
$$z_1 = \exp(\mathrm{i}\,2.854075020893),$$
$$z_2 = \exp(\mathrm{i}\,1.198259222271),$$
$$z_3 = \exp(\mathrm{i}\,6.026082413871).$$

7.4. Case $e = 6$

In this case, there are:

1. Two previously known classes, both consisting of 78 solutions. The solutions are defined by the roots of the polynomial

$$g_{6,1}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Representatives of the equivalence classes are

$$\boldsymbol{x} = \{\zeta^{i^2}\}, \qquad \boldsymbol{x} = \{\zeta^{2i^2}\}.$$

2. A class consisting of 1014 solutions. The solutions are defined by the roots of the polynomial

$$g_{6,2}(x) = x^{12} + x^{11} - 12x^{10} - 12x^9 + 14x^8 + x^7 + x^6 + x^5 + 14x^4 - 12x^3 - 12x^2 + x + 1.$$

The sequence that defines the class is

$$\boldsymbol{x} = \{1, z_0, z_1, z_4, z_2, z_3, z_5, z_5, z_3, z_2, z_4, z_1, z_0\},$$

$$\begin{aligned} z_0 &= \exp(\mathrm{i}\,0.276669071806850), & z_3 &= z_0^* = \exp(-\mathrm{i}\,0.276669071806850)\\ z_1 &= \exp(-\mathrm{i}\,1.220721809284420), & z_4 &= z_1^* = \exp(\mathrm{i}\,1.220721809284420),\\ z_2 &= \exp(\mathrm{i}\,2.283062308094460), & z_5 &= z_2^* = \exp(-\mathrm{i}\,2.283062308094460). \end{aligned}$$

3. Nine equivalence classes consisting of 2028 solutions (polynomials are not presented). Elements of the sequences that generate the classes are as follows:

Number of the class	z_0	z_1	z_2	z_3	z_4	z_5
1	$e^{\mathrm{i}\,0.1902604}$	$e^{\mathrm{i}\,6.0532874}$	$e^{\mathrm{i}\,5.3301520}$	$e^{\mathrm{i}\,4.1247946}$	$e^{\mathrm{i}\,2.7896177}$	$e^{\mathrm{i}\,1.3456171}$
2	$e^{\mathrm{i}\,6.2572071}$	$e^{\mathrm{i}\,3.1069136}$	$e^{\mathrm{i}\,4.3142758}$	$e^{\mathrm{i}\,2.5337532}$	$e^{\mathrm{i}\,1.6095226}$	$e^{\mathrm{i}\,1.5348747}$
3	$e^{\mathrm{i}\,1.5145681}$	$e^{\mathrm{i}\,5.6230253}$	$e^{\mathrm{i}\,1.8186436}$	$e^{\mathrm{i}\,4.3012373}$	$e^{\mathrm{i}\,1.3507833}$	$e^{\mathrm{i}\,5.5295501}$
4	$e^{\mathrm{i}\,0.7098655}$	$e^{\mathrm{i}\,0.3563601}$	$e^{\mathrm{i}\,1.2761141}$	$e^{\mathrm{i}\,2.4965890}$	$e^{\mathrm{i}\,3.5264757}$	$e^{\mathrm{i}\,5.2149488}$
5	$e^{\mathrm{i}\,2.8195396}$	$e^{\mathrm{i}\,4.7919876}$	$e^{\mathrm{i}\,1.2202988}$	$e^{\mathrm{i}\,5.7462645}$	$e^{\mathrm{i}\,1.3012538}$	$e^{\mathrm{i}\,5.4918629}$
6	$e^{\mathrm{i}\,0.0360641}$	$e^{\mathrm{i}\,0.5036032}$	$e^{\mathrm{i}\,1.5060156}$	$e^{\mathrm{i}\,2.7899674}$	$e^{\mathrm{i}\,4.2286812}$	$e^{\mathrm{i}\,5.5467868}$
7	$e^{\mathrm{i}\,1.9322243}$	$e^{\mathrm{i}\,5.2951804}$	$e^{\mathrm{i}\,3.3498223}$	$e^{\mathrm{i}\,1.6479544}$	$e^{\mathrm{i}\,4.2375937}$	$e^{\mathrm{i}\,3.3816830}$
8	$e^{\mathrm{i}\,0.0300385}$	$e^{\mathrm{i}\,4.8160574}$	$e^{\mathrm{i}\,4.3715523}$	$e^{\mathrm{i}\,1.1462748}$	$e^{\mathrm{i}\,3.2148048}$	$e^{\mathrm{i}\,3.9654735}$
9	$e^{\mathrm{i}\,3.2573498}$	$e^{\mathrm{i}\,1.5620823}$	$e^{\mathrm{i}\,4.1066677}$	$e^{\mathrm{i}\,3.2922886}$	$e^{\mathrm{i}\,1.8740567}$	$e^{\mathrm{i}\,5.2812042}$

7.5. Case $e = 12$

In this case, there are seven equivalence classes, consisting of 4056 solutions of the form

$$\boldsymbol{x} = \{1, z_0, z_1, z_4, z_2, z_9, z_5, z_{11}, z_3, z_8, z_{10}, z_7, z_6\}$$

(polynomials are not presented). Elements of the sequences that generate the classes are as follows:

Number of the class	z_0 z_6	z_1 z_7	z_2 z_8	z_3 z_9	z_4 z_{10}	z_5 z_{11}
1	$e^{\mathrm{i}\,0.3644155}$ $e^{\mathrm{i}\,0.6959709}$	$e^{\mathrm{i}\,1.8544445}$ $e^{\mathrm{i}\,2.9987740}$	$e^{\mathrm{i}\,0.2119998}$ $e^{\mathrm{i}\,1.0141209}$	$e^{\mathrm{i}\,4.9720469}$ $e^{\mathrm{i}\,1.6192549}$	$e^{\mathrm{i}\,2.6024911}$ $e^{\mathrm{i}\,4.6885398}$	$e^{\mathrm{i}\,4.9544333}$ $e^{\mathrm{i}\,5.7812423}$
2	$e^{\mathrm{i}\,5.2994829}$ $e^{\mathrm{i}\,5.3280634}$	$e^{\mathrm{i}\,5.5349134}$ $e^{\mathrm{i}\,3.6895083}$	$e^{\mathrm{i}\,4.2517683}$ $e^{\mathrm{i}\,1.2821841}$	$e^{\mathrm{i}\,3.9078690}$ $e^{\mathrm{i}\,0.6130970}$	$e^{\mathrm{i}\,2.9651940}$ $e^{\mathrm{i}\,5.4055142}$	$e^{\mathrm{i}\,0.8406314}$ $e^{\mathrm{i}\,0.7926259}$
3	$e^{\mathrm{i}\,5.4648352}$ $e^{\mathrm{i}\,4.6674996}$	$e^{\mathrm{i}\,1.4102819}$ $e^{\mathrm{i}\,1.3308366}$	$e^{\mathrm{i}\,1.8284688}$ $e^{\mathrm{i}\,3.2227988}$	$e^{\mathrm{i}\,1.5169011}$ $e^{\mathrm{i}\,5.0244945}$	$e^{\mathrm{i}\,0.8084470}$ $e^{\mathrm{i}\,0.6539394}$	$e^{\mathrm{i}\,3.3618472}$ $e^{\mathrm{i}\,1.6996524}$
4	$e^{\mathrm{i}\,3.1421864}$ $e^{\mathrm{i}\,4.9889886}$	$e^{\mathrm{i}\,5.8682974}$ $e^{\mathrm{i}\,0.2742489}$	$e^{\mathrm{i}\,1.1475184}$ $e^{\mathrm{i}\,1.3089282}$	$e^{\mathrm{i}\,3.1934900}$ $e^{\mathrm{i}\,2.6927908}$	$e^{\mathrm{i}\,0.8015527}$ $e^{\mathrm{i}\,0.2996878}$	$e^{\mathrm{i}\,2.5261989}$ $e^{\mathrm{i}\,5.9201145}$
5	$e^{\mathrm{i}\,6.1299932}$ $e^{\mathrm{i}\,5.3933545}$	$e^{\mathrm{i}\,4.9103682}$ $e^{\mathrm{i}\,4.3714754}$	$e^{\mathrm{i}\,4.0871216}$ $e^{\mathrm{i}\,3.3750358}$	$e^{\mathrm{i}\,5.9363385}$ $e^{\mathrm{i}\,3.4959996}$	$e^{\mathrm{i}\,0.2631024}$ $e^{\mathrm{i}\,2.1537000}$	$e^{\mathrm{i}\,1.4894551}$ $e^{\mathrm{i}\,4.3802490}$
6	$e^{\mathrm{i}\,4.0081830}$ $e^{\mathrm{i}\,1.4528517}$	$e^{\mathrm{i}\,4.2306731}$ $e^{\mathrm{i}\,0.7048406}$	$e^{\mathrm{i}\,1.1255238}$ $e^{\mathrm{i}\,3.4903468}$	$e^{\mathrm{i}\,0.3005833}$ $e^{\mathrm{i}\,4.4028238}$	$e^{\mathrm{i}\,5.2414217}$ $e^{\mathrm{i}\,0.5291664}$	$e^{\mathrm{i}\,1.1096142}$ $e^{\mathrm{i}\,0.8061093}$
7	$e^{\mathrm{i}\,4.5781731}$ $e^{\mathrm{i}\,4.7957505}$	$e^{\mathrm{i}\,5.0348707}$ $e^{\mathrm{i}\,5.6982482}$	$e^{\mathrm{i}\,1.1102887}$ $e^{\mathrm{i}\,5.8941121}$	$e^{\mathrm{i}\,3.6339907}$ $e^{\mathrm{i}\,1.0270072}$	$e^{\mathrm{i}\,4.6511132}$ $e^{\mathrm{i}\,2.0018328}$	$e^{\mathrm{i}\,4.3997922}$ $e^{\mathrm{i}\,2.8455874}$

There are no other equivalence classes.

8. CONCLUSIONS

A method to construct sequences with zero autocorrelation is described, which is based on Gauss periods. For the case $p = 3f + 1$, explicit formulas defining unimodular delta-correlated sequences are found.

All equivalence classes for unimodular delta-correlated sequences of lengths $p = 3, 5, 7, 13$ are found.

In the cases where full classification of solutions is possible, all equivalence classes are found to be based on Gauss periods.

Conjecture. Our conjecture is that this is true for any p.

As an example, classification of unimodular δ-correlated sequences of length $p = 13$ is given.

REFERENCES

1. Gabidulin, E.M., On Classification of Sequences with the Perfect Periodic Auto-Correlation Function, in *Proc. 3rd Int. Colloq. on Coding Theory, Dilijan, Armenia, 1990*, Yerevan, 1991, pp. 24–30.

2. Gabidulin, E.M., There Are Only Finitely Many Perfect Auto-Correlation Polyphase Sequences of Prime Length, in *Proc. 1994 IEEE Int. Sympos. on Information Theory*, Trondheim, Norway, 1994, pp. 282.

3. van der Waerden, B.L., *Algebra*, Berlin: Springer, 1971, 8 ed. Translated under the title *Algebra*, Moscow: Nauka, 1976.

4. Prasolov, V.V., *Mnogochleny* (Polynomials), Moscow: Mos. Tsentr Nepreryvnogo Mat. Obrazovaniya, 2001.

5. Cox, D.A., Little, J., and O'Shea, D., *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, New York: Springer, 1997, 2nd ed. Translated under the title *Idealy, mnogoobraziya i algoritmy: Vvedenie v vychislitel'nye aspekty algebraicheskoi geometrii i kommutativnoi algebry*, Moscow: Mir, 2000.

6. Edwards, H.M., *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, New York: Springer, 1977. Translated under the title *Poslednyaya teorema Ferma*, Moscow: Mir, 1980.

7. Fan, P. and Darnell, M., *Sequences Design for Communications Applications*, Taunton: RSP; New York: Wiley, 1996.

8. Frank, R.L., Polyphase Codes with Good Nonperiodic Correlation Properties, *IEEE Trans. Inf. Theory*, 1963, vol. 9, no. 1, pp. 43–45.