PACS numbers: 03.67.Dd; 03.67.Lx
DOI: 10.1070/QE2005v035n08ABEH009164

Algebraic solution of the synthesis problem for coded sequences

A.N. Leukhin

***Abstract*. The algebraic solution of a 'complex' problem of synthesis of phase-coded (PC) sequences with the zero level of side lobes of the cyclic autocorrelation function (ACF) is proposed. It is shown that the solution of the synthesis problem is connected with the existence of difference sets for a given code dimension. The problem of estimating the number of possible code combinations for a given code dimension is solved. It is pointed out that the problem of synthesis of PC sequences is related to the fundamental problems of discrete mathematics and, first of all, to a number of combinatorial problems, which can be solved, as the number factorisation problem, by algebraic methods by using the theory of Galois fields and groups.**

Keywords: *phase-coded sequences, quasi-uniform energy spectrum, Galois group of a system of equations, difference set.*

1. Introduction

The problem of separation of the fields of application of quantum and classical calculations appeared from the very beginning of the development of the theory of quantum calculations [1]. A number of problems of classical discrete mathematics have not been solved so far first of all due to the difficulties involved in solving algebraic problems based on the theory of finite groups and fields. The problems whose solution is of great practical interest include: (i) the problem of number factorisation; (ii) the problem of existence of difference sets with given parameters; (iii) the problem of partition of the coefficient set specifying sets, which are automorphic to the initial difference set, into nonintersecting classes of coefficients without specifying the code method; (iv) synthesis of all the finite projective block schemes whose incidence matrices are circulant; (v) synthesis of all the finite projective planes and projective geometries of a given dimensionality; (vi) analytic expression for irreducible polynomials over a given Galois field $GF(q^s)$.

Note that this list is far from being complete, and the above-mentioned problems have much in common, being related to practical applications in cryptographic schemes, synthesis of the codes correcting errors, and in synthesis of noise-like signals [2]. All these problems have been solved in some particular cases, but as a whole the classical complexity of the algorithms for solving these problems was not proved. However, there exist quantum algorithms which can be used for solving many so-called difficult problems by employing the polynomial number of iterations. The main argument in the favour of their application is the absence at present of the classical algorithm for solving these problems.

In this paper, the solution of one of such difficult problems is presented – the synthesis of phase-code (PC) sequences with the zero level of side lobes of the cyclic autocorrelation function (ACF), and the classical algorithm for its solution is given.

A.N. Leukhin Mari State Technical University, pl. Lenina 3, 424000 Ioshkar-Ola, Russia; e-mail: inf@marstu.mari.ru, fun_man@list.ru

Received 2 June 2005
Kvantovaya Elektronika **35** (8) 688 – 692 (2005)
Translated by M.N. Sapozhnikov

2. Formulation of the problem of synthesis of phase-code sequences

At present, codes with the zero side lobes of the cyclic ACF, which have, as the white noise, a uniform energy spectrum, have found wide applications in radio-engineering systems. Therefore, the problems of synthesis of noise-like code sequences, their practical realisation and processing are of current interest. In the case of large phase gradations, a number of sequences are known which have the one-level ACF with the zero side lobes [3]: Franc codes, class p codes, and codes associated with a linear frequency-modulated (LFM) signal. In [4], a code in the form of a composition contour was considered, which was synthesised based on the theoretical concepts of contour analysis described in monograph [5].

To date the problem of synthesis of all the possible PC sequences with the zero level of side lobes for a given dimensionality N is not solved. Numerous methods and approaches have been developed for the synthesis of codes with good correlation properties. In this paper, a new approach, based on the Galois theory, is proposed for solving the problem of synthesis of PC sequences with the zero level of side lobes of the cyclic ACF. Some aspects of the problem, related to the so-called basis solution, were discussed earlier [6].

Let us write the discrete PC sequence $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$ as

$$\gamma_n = \exp(\mathrm{i}\varphi_n), \quad n = 0, ..., N-1, \tag{1}$$

where the phase value in each nth code interval is determined from the range $\varphi_n \in [0, 2\pi]$; N is the number of code elements in the code, and the modulus of each code element is $|\gamma_n| = 1$.

The cyclic ACF can be found from the expression

$$\eta_\tau = \sum_{n=0}^{N-1} \gamma_{n+\tau \pmod N} \gamma_n^*, \quad \tau = 0, 1, ..., N-1. \tag{2}$$

It is necessary to determine the form of the code $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$ providing the zero values of all the side readings of the cyclic ACF, i.e.,

$$\eta_0 = N, \quad \eta_1 = 0, \quad \eta_2 = 0, ..., \eta_{N-1} = 0. \tag{3}$$

It is necessary to find out whether code sequences satisfying condition (3) exist for any positive integers N and also to determine the total number P of solutions in the case of the existence of solutions at a given dimensionality and to develop the algorithm for synthesis of the total family of codes with the zero level of side lobes of the cyclic ACF for a given dimensionality N of the code.

By representing the energy spectrum for the PC sequence $\boldsymbol{\Gamma} = \{\gamma_n\}_{0,N-1}$ in the form

$$|\rho_m|^2 = \left| \sum_{n=0}^{N-1} \gamma_n \exp\left(-\mathrm{i}\frac{2\pi}{N}mn\right)\right|^2, \; m = 0, ..., N-1,$$

and taking into account that $|\rho_0|^2 = |\rho_1|^2 = ... = |\rho_{N-1}|^2 = N$, we obtain the system of equations

$$\sum_{n=1}^{N-1} \left\{ \cos\left(\varphi_n - \frac{2\pi}{N}mn\right) + \sum_{l=n+1}^{N-1} \cos\left[\varphi_n - \varphi_l + \frac{2\pi}{N}m(l-n)\right]\right\} = 0, \tag{4}$$

which can be used for seeking for the angles $\varphi_1, \varphi_2, ..., \varphi_{N-1}$.

3. Solutions of the problem of synthesis of PC sequences obtained using basis solutions

Basis solutions. By analysing the system of equations (4), we can prove that the condition

$$\varphi_1 = \varphi_{N-1}, \quad \varphi_2 = \varphi_{N-2}, ..., \quad \varphi_{]N/2[} = \varphi_{]N/2[}, \tag{5}$$

should be satisfied for at least one solution, where]...[means an integer. We will call this solution *the basis solution*.

The initial basis solutions can be represented by the expressions

$$\varphi_{l,n} = \phi_l[n^2 (\mathrm{mod}\, N_1)], \tag{6}$$

where

$$N_1 = \begin{cases} 2N \text{ for } N \,(\mathrm{mod}\, 2) \equiv 0, \\ N \text{ for } N \,(\mathrm{mod}\, 2) \equiv 1; \end{cases}$$

$n = 0, ..., N-1$; $\phi_l = 2\pi\lambda_l / N_1$; λ_l is the number mutually disjoint with the number N_1; $l = 1, 2, ..., \varphi(N_1)$; $\varphi(N_1)$ is the Euler function.

If the dimensionality of the PC sequence is the square of an integer k, i.e., $N = k^2$, the initial basis solutions of the system of equations (4) will also have the form

$$\varphi_{s,n} = \phi_s k \left\{ \left[\begin{array}{l} \overbrace{0\cdot 1, 1\cdot 1, ..., (k-1)\cdot 1}^{k}; \overbrace{k\cdot 3, (k+1)\cdot 3, ..., (2k-1)\cdot 3}^{k}, ..., \\ \overbrace{(k^2-k)(2k-1), (k^2-k+1)(2k-1), ..., (k^2-1)(2k-1)}^{k} \end{array} \right] (\mathrm{mod}\, M) \right\}, \tag{7}$$

where

$$M = \begin{cases} 2k \text{ for } k \,(\mathrm{mod}\, 2) \equiv 0, \\ k \text{ for } k \,(\mathrm{mod}\, 2) \equiv 1; \end{cases}$$

$\phi_s = 2\pi\lambda_s / N_1$; λ_s is the number mutually disjoint with the number M; $s = 1, 2, ..., \varphi(M)$; and $\varphi(M)$ is the Euler function of the number M.

In addition, if k is an even number, then except the solutions of types (6) and (7), there exist the initial basis solutions of system (4) of the type

$$\varphi_{s,n} = \phi_s k \left\{ \left[\begin{array}{l} 0, \overbrace{0, 0, ..., 0}^{k/2}; \overbrace{2\cdot 1, 2\cdot 2, ..., 2\cdot k}^{k}; \overbrace{4\cdot (k+1), 4\cdot (k+2), ..., 4\cdot 2k}^{k}, ..., \\ \overbrace{2\cdot (k-1)(k-1)^2, ..., 2\cdot (k-1)(k^2-k-1)}^{k}; \overbrace{0, 0, ..., 0}^{k/2} \end{array} \right] (\mathrm{mod}\, 2k) \right\}, \tag{8}$$

where $\phi_s = 2\pi\lambda_s / N_1$; λ_s is the number mutually disjoint with the number k; and $s = 1, 2, ..., \varphi(k)$.

The Galois group for the system of equations (4). We can prove that the roots $\varphi_1, \varphi_2, ..., \varphi_{N-1}$ of the system of equations (4) satisfy operations of mutual replacement – permutations that does not violate the relation between the roots of the system of equations. By multiplying the subscripts $1, 2, 3, ..., N-1$ of the roots of the system of equations (4) by the number λ mutually disjoint with the number N, we obtain that each nth root, where $n = 1, 2, 3, ..., N-1$ will pass to a new root with the subscript $\lambda \cdot n (\mathrm{mod}\, N)$. We represent such a permutation in the form

$$T_{\lambda_l} = \{[1 \to \lambda_l \cdot 1 \;(\mathrm{mod}\, N)], \; [2 \to \lambda_l \cdot 2 \,(\mathrm{mod}\, N)], ...,$$

$$[N-1 \rightarrow \lambda_l \cdot (N-1)\,(\mathrm{mod}\,N)]\}, \tag{9}$$

where $l = 1, 2, ..., \varphi(N_1)$; $\varphi(N)$ is the Euler function. A set of permutations

$$\mathrm{Gal}(\boldsymbol{T}) = \{\boldsymbol{T}_{\lambda_1}, \boldsymbol{T}_{\lambda_2}, ..., \boldsymbol{T}_{\lambda_{\varphi(N)}}\} \tag{10}$$

forms the Galois group of the $\varphi(N)$ order, where $l = 1, 2, ..., \varphi(N)$. Because any Galois group is Abelian, the system of equations (4) has the solution for any dimensionality N.

If the dimensionality of the PC sequence is $N = k^2$, the solution of the system of equations (4) can be considered in the form of the quadratic matrix $\boldsymbol{\Phi} = ||\Phi_{ij}||$, where $\Phi_{ij} = \varphi_n$, $n = 0, ..., k^2 - 1$, and the subscript n is incremented upon changing the subscripts $i = 0, ..., k-1$ and $j = 0, ..., k-1$. The permutations

$$S_{\lambda_l} = \{[1 \rightarrow \lambda_l \cdot 1(\mathrm{mod}\,k)],\ [2 \rightarrow \lambda_l \cdot 2\,(\mathrm{mod}\,k)], ...,$$

$$(k-1 \rightarrow \lambda_l \cdot (N-1)\,(\mathrm{mod}\,k)]\} \tag{11}$$

are admissible, where λ_l is the number mutually disjoint with the number k; $l = 1, 2, ..., \varphi(k)$; and $\varphi(k)$ is the Euler function. The set of permutations interchanging the lines of the matrix $\boldsymbol{\Phi}$

$$\mathrm{Gal}(\boldsymbol{S}) = \{\boldsymbol{S}_{\lambda_1}, \boldsymbol{S}_{\lambda_2}, ..., \boldsymbol{S}_{\lambda_{\varphi(k)}}\}, \tag{12}$$

forms the Galois group of the $\varphi(k)$th order of additional permutations.

When the values of the number k are even, the Galois group of permutations of the roots of the system of equations (4) formed with the help of (10), (12), can be added. The expression $n = s - k/2\,(\mathrm{mod}\,N)$ determines the subscript s. Taking this cyclic shift from the matrix $\boldsymbol{\Phi}$ into account, we obtain the matrix $\boldsymbol{\Psi} = ||\Psi_{ij}||$, where $i = 0, ..., k-1$, $j = 0, ..., k-1$, $\Psi_{ij} = \varphi_n$, $n = k^2 - k/2 + 1$; and the subscript n is incremented upon changing the subscripts i, j. The permutations

$$V_{\lambda_1} = \{[1 \rightarrow \lambda_l \cdot 1(\mathrm{mod}\,k)],\ [2 \rightarrow \lambda_l \cdot 2\,(\mathrm{mod}\,k)], ...,$$

$$[k-1 \rightarrow \lambda_l \cdot (N-1)\,(\mathrm{mod}\,k)]\} \tag{13}$$

are admissible, where λ_l is the the number mutually disjoint with the number k; $l = 1, 2, ..., \varphi(k)$; and $\varphi(k)$ is the Euler function. The set of permutations interchanging the lines of the matrix $\boldsymbol{\Psi}$,

$$\mathrm{Gal}(\boldsymbol{V}) = \{\boldsymbol{V}_{\lambda_1}, \boldsymbol{V}_{\lambda_2}, ..., \boldsymbol{V}_{\lambda_{\varphi(k)}}\}, \tag{14}$$

forms the Galois group of the $\varphi(k)$th order of additional permutations.

After the application of permutations (14) for solving the system of equations (4) represented by the matrix $\boldsymbol{\Psi}$, it is necessary to perform the inverse transition from the matrix $\boldsymbol{\Psi}$ to the matrix $\boldsymbol{\Phi}$ by using the expression $n = s - k/2$ (mod N).

Solutions of the system of equations (4) obtained from basis solutions. By applying admissible permutations of the roots of the system of equations (4) in the form (10), (12), (14) to the initial basis solutions in the form (6)–(8), we obtain all possible basis solutions. We denote the total number of basis solutions of the system of equations (4) of dimensionality N by L. For each basis solution obtained, we can also obtain N non-basis solutions:

$$\Psi_{n+l\cdot N, N-n+m\,(\mathrm{mod}\ N)} = \varphi_{l,m} - \varphi_{l,n}\,(\mathrm{mod}\,360^\circ), \tag{15}$$

where $l = 0, ..., L-1$; $n = 0, ..., N-1$; $m = 0, ..., N-1$.

We denote by P the *total number of possible solutions of the system of equations (4)*. It was shown above that the three cases of solutions should be distinguished:

(i) For arbitrary N, where $N \neq k^2$, and k is a positive integer, we determine the total number of possible solutions as

$$P = \varphi(N)N, \tag{16}$$

the number of basis solutions for *odd* N being $L = \varphi(N)$ and for *even* N, $L = \varphi(2N)$.

(ii) For $N^2 = k$, where k is an odd number, the number of possible solutions is

$$P = [\varphi(N)\varphi(k) + \varphi(N)\varphi(k)/2]N$$

$$= \frac{3}{2}\varphi(N)\varphi(k)N, \tag{17}$$

in this case, $L = \frac{3}{2}\varphi(N)\varphi(k)$.

(iii) For $N = k^2$, where k is an even number, the number of possible solutions is:

for *even* k/2,

$$P = \left[\varphi(2N)\varphi(k) + \frac{\varphi(N)}{4}\varphi(2k)\varphi(k)\right.$$

$$\left. + \frac{\varphi(N)}{2}\varphi(k)\right]\frac{N}{2} = \frac{\varphi(N)\varphi(k)}{4}[5 + \varphi(k)]N, \tag{18a}$$

and $L = \varphi(N)\varphi(k)[5 + \varphi(k)]/2$;

for *odd* $k/2$

$$P = \left[\varphi(2N)\varphi(k) + \frac{\varphi(N)}{4}\varphi(2k)\varphi(k)\right.$$

$$\left. + \frac{\varphi(N)}{2}\varphi(k)\right]\frac{N}{2} = \frac{\varphi(N)\varphi(k)}{8}[9 + 2\varphi(k)]N, \tag{18b}$$

and $L = \{[\varphi(N)\varphi(k)]/4\}[9 + 2\varphi(k)]$.

Special case of $N = 4$. Consider now a special case when the code sequence length is $N = 4$. Taking into account the existence of the basis solution, the system of equations (4) can be represented in the form

$$2\cos\varphi_1 + \cos\varphi_2 + 1 + 2\cos(\varphi_1 - \varphi_2) = 0,$$
$$\cos\varphi_2 + 1 = 0. \tag{19}$$

It follows from (19) that $\varphi_2 = 180^\circ$, while φ_1 and, therefore, φ_3 can take any value in the range $[0^\circ, 360^\circ]$, i.e., $\varphi_1 = \varphi_3 \in [0^\circ, 360]^\circ$. Therefore, there exist an infinite number of basis solutions of the form

$$0^\circ, \varphi_1, 180^\circ, \varphi_1, \tag{20a}$$

where φ_1 can take any value in the range $[0^\circ, 360^\circ]$. Taking transformations (17) into account, solutions of the type

$$0^\circ, \varphi_1, 0^\circ, \varphi_1 + 180^\circ \tag{20b}$$

will be also the solutions of the system of equations (21).

Let us emphasise that only in the special case of $N = 4$, an arbitrary large number of code sequences with the zero side lobes of the ACF can be synthesised. In this case, $P = \infty$ and the number of basis solutions $L = \infty$. In the rest of the cases, taking the restriction $\varphi = 0^\circ$ into account, the number of code sequences will be finite.

4. Solutions obtained based on difference sets

The sufficient condition for the existence of a code with the one-level ACF is the existence of the difference set $D(N, K^+, \lambda)$ (where $K^\pm$ is the number of elements of the difference set of dimensionality N, and λ is the number of repetitions of the difference of elements of the difference set) and, vice versa, if the difference set exists, a code with the one-level ACF should certainly exist [1]. To date, the problem of synthesis of all possible difference sets for a given dimensionality N is not solved. The known difference sets are classified in [7]. They include:

(1) The difference set obtained based on quadratic residues:

$$D(N = 4x + 3 = p, K^+ = 2x, \lambda = x),$$

$$x = 0, 1, 2, ..., \quad p \text{ is a prime number.} \tag{21}$$

To this difference set, the Legendre code corresponds. The power of the code method (the number of non-inversion-isomorphic coefficients) is

$$M_c = 1. \tag{22}$$

(2) The difference Singer set:

$$D\left(N = \frac{q^s - 1}{q - 1},\ K^+ = \frac{q^{s-1} - 1}{q - 1},\ \lambda = \frac{q^{s-2} - 1}{q - 1}\right),$$

$$q = p^n. \tag{23}$$

To this difference set, the Singer code corresponds. The power of the code method is determined from the expression

$$M_c = \frac{\varphi(p^n - 1)}{(p - 1)n}. \tag{24}$$

Of interest is a particular case of the difference Singer set $q = 2^n$, $s = 1$:

$$D(N = 2^n - 1,\ K^+ = 2^{n-1} - 1,\ \lambda = 2^{n-2} - 1). \tag{25}$$

To this difference set, the m-sequence corresponds. The power of the code method is

$$M_c = \frac{\varphi(2^n - 1)}{2n}. \tag{26}$$

(3) The difference Jacobi set:

$$D(N = 4x + 3 = p(p + 2),\ K^+ = 2x + 1,\ \lambda = x). \tag{27}$$

To this difference set, the Jacobi code corresponds. The power of the code method, as in the case of the Legendre code, is $M_c = 1$.

(4) The difference Hall set:

$$D(N = 4x + 3 = 4y^2 + 27 = p,\ K^+ = 2x + 1,\ \lambda = x),$$

$$y = 1, ... \tag{28}$$

To this difference set, the Hall code corresponds. The power of the code method is

$$M_c = 3. \tag{29}$$

Note that in previous papers, for example, [1] the difference sets were used only for synthesis of phase-manipulated sequences (in each code interval, $\varphi_n = 0$ or $\varphi_n = \pi$) with the one-level ACF. It is shown in this paper that the difference sets can be used to synthesise PC sequences. In each code interval of the PC sequence, the phase values are

$$\varphi = \{0, 0, \phi, 0, 0, \phi, ..., 0, \phi, 0\}, \tag{30}$$

where the positions of non-zero phase values are determined by the corresponding difference set. For the zero level of the side lobes, the phase gradation is determined from the expression

$$\phi = \pi - \arccos\left(\frac{N - 1}{N + 1}\right). \tag{31}$$

Except the solutions found above, we can obtain in the general case N solutions by applying to solution (30) the transformations (15). For the solutions obtained based on the difference sets, the total Galois group of the system of equations (4) will give solutions of the type

$$\varphi_{l,n} = \psi_n - 2\pi ln/N, \quad l = 0, 1, ..., N - 1,$$

$$n = 0, 1, ..., N - 1. \tag{32}$$

Taking the above consideration into account, the total number of possible solutions obtained based on the difference sets is

$$P = 2M_c N^2. \tag{33}$$

5. Example of synthesis of PC sequences

For the dimensionality $N = 7$, we have the total number $P' = 42$ of solutions obtained from basis solutions, of which six solutions are basis ones:

$$\varphi = \left\{0, \frac{2\pi}{7}, 4\frac{2\pi}{7}, 2\frac{2\pi}{7}, 2\frac{2\pi}{7}, 4\frac{2\pi}{7}, \frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0, 2\frac{2\pi}{7}, \frac{2\pi}{7}, 4\frac{2\pi}{7}, 4\frac{2\pi}{7}, \frac{2\pi}{7}, 2\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0, 3\frac{2\pi}{7}, 5\frac{2\pi}{7}, 6\frac{2\pi}{7}, 6\frac{2\pi}{7}, 5\frac{2\pi}{7}, 3\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0, 4\frac{2\pi}{7}, 2\frac{2\pi}{7}, \frac{2\pi}{7}, \frac{2\pi}{7}, 2\frac{2\pi}{7}, 4\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 5\frac{2\pi}{7},\ 6\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 3\frac{2\pi}{7},6\frac{2\pi}{7},\ 5\frac{2\pi}{7}\right\},$$

$$\varphi = \left\{0,\ 6\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 5\frac{2\pi}{7},\ 5\frac{2\pi}{7},\ 3\frac{2\pi}{7},\ 6\frac{2\pi}{7}\right\}.$$

By using transformations (15), we can obtain from these solutions $6 \times 6 = 36$ new solutions.

For the dimensionality $N = 7$, there exists one non-inversion isomorphic difference set of quadratic residues, which gives the solution

$$\varphi = \{0, 0, \phi, 0, \phi, \phi, 0\},$$

where $\phi = 138.59^\circ$.

Taking into account transformations (15) and (33), the total number of solutions obtained based on difference sets is $P'' = 98$. Then, for $N = 7$, the total number of possible solutions of the system of equations (4) is $P = P' + P'' = 42 + 98 = 140$.

6. Conclusions

The total number P of possible solutions was determined and the algebraic algorithm was developed for synthesis of PC sequences with the zero level of side lobes of the cyclic ACF for a given code dimensionality. It was shown that the difference sets can be obtained based on the solution of the problem of synthesis of code sequences.

Acknowledgements. This work was supported by the Russian Foundation for Basic Research (Grant Nos 03-02-17276 and 04-01-00243).

References

1. Klyshko D.N. *Phys. Lett. A*, **1**, 227 (1997).
2. Sverdlik M.B. *Optimal'nye diskretnye signaly* (Optimal Discrete Signals) (Moscow: Sov. Radio, 1975).
3. Varakin L.E. *Sistemy svyazi s shuopodobnymi signalami* (Commumication Systems with Noise-like Signals) (Moscow: Radio i Svyaz', 1985).
4. Furman Ya.A., Rozhentsov A.A. *Radiotekhn.*, **8**, 5 (2000).
5. Leukhin A.N. et al. *Vvedenie v konturnyi analiz; prilozheniya k obrabotke izobrazhenii i signalov* (Introduction to Contour Analysis: Applications to Image and Signal Processing) (Moscow: Fizmatlit, 2003).
6. Leukhin A.N. *Vestnik KGTU*, **5**, 3 (2004).
7. Hall M. *Combinatorial Theory* (New York: John Wiley, 1986; Moscow: Mir, 1970).