An Algorithm for Computer Synthesis of Complementary Sequences

Borislav Y. Bedzhev, Zhaneta N. Tasheva, Borislav P. Stoyanov

Abstract: *The sequences with complex pseudorandom structure, ideal autocorrelation function, close to zero cross-correlation function for all possible pairs of sequences from a set have extreme importance for several practical applications, such as communications, radars and cryptanalysis. As a result, the sequences with mentioned abilities are intensively studied during the past fifty years. Despite of great efforts, at present small number of these sequences are known and they couldn't meet the fast raising requirements of the manufacturers and consumers of communication services. With regard to these reasons in our paper we prove a new algorithm for synthesis of so-named Complementary Sequences introduced by Golay, which not only have ideal ACF, but also exist for arbitrary large length. In the paper is shown also that the recently proposed generalized matrix signals are a derivative from generalized complementary sequences.*

Key words: *Computing, Computer Modelling, Complementary Sequences, Communication Systems.*

INTRODUCTION

The sequences with complex pseudorandom structure, ideal *autocorrelation function (ACF)*, similar to delta impulse, close to zero *cross-correlation function (CCF)* for all possible pairs of sequences from a set have extreme importance for several practical applications. Especially, the correlation features of the sequences are interested for the spread spectrum communication systems, radar systems, signal synchronization and cryptanalysis, as well as being of theoretical interest as measures of randomness. As a result, the sequences with mentioned abilities are intensively studied during the past fifty years. From the abundant experience in this area could be concluded that the sequences with valuable for the practice correlation features are very rare and their synthesis is a hard computation problem. In fact, at present small number of these sequences are known and they couldn't meet the fast raising requirements of the manufacturers and consumers of communication services. With regard to these reasons in our paper we prove a new algorithm for synthesis of so-named *Complementary Sequences (CSs)* introduced by Golay [3], which not only have ideal *ACF*, but also exist for arbitrary large length.

The paper is organized as follows. First, the basics of the *CSs* are recalled. Second, a new algorithm for *CS* synthesis is proposed. After then the tight connection between *CSs* and some recently proposed sequences such as matrix signals is studied. Finally, the advantages and possible areas of application of our algorithm are discussed.

AN ALGORITHM FOR COMPUTER SYNTHESIS OF COMPLEMENTARY SEQUENCES

It is known [5], that complex *phase manipulated (PM)* signals are sequences of *n* equivalent impulses and they are described with the formula:

$$v(t) = \sum_{j=1}^{n} U_j . u_0(t - t_j) . \cos[\omega_0 . (t - t_j) + \theta_j] \qquad (1)$$

where τ_0 is the duration of the elementary impulses, $\omega_0 = 2\pi f_0$, f_0 is their carrier frequency, U_j - the amplitude of the *j*th impulse and:

$$u_0(t) = \begin{cases} 1, \ if \ \ 0 \le t \le \tau_0 \\ 0, \ if \ \ t < 0, \ or \ \ t > \tau_0 \end{cases}.$$

To simplify the practical realization of the complex process of *PM* signals receiving, the following limitations in the formula (1) are made:

- $\tau_0 = const; \qquad U_j = U_0 = const; \qquad j = 1,2,...,n;$
- $\theta_j \in \{(2\pi l)/m; \qquad l = 0,1,...,m-1\}$.

In this case the *PM* signals can be described as a *sequence* of complex amplitudes of elementary signals [4]:

$$V(t) = \sum_{j=1}^{n} U_0 . \zeta(j) . u_0(t - t_j) ,$$

where $\{\zeta(j)\}_{j=0}^{n-1}$ is the set of complex amplitudes of the elementary impulses:

$$\zeta(j) \in \{\exp(2\pi i l / m); l = 0,1,...,m-1\} . \quad (2)$$

It is known that a *CS* is a set of two special *PM* signals, whose summary non-periodical *ACF* is similar to delta impulse. The classical Golay's definition of the *CS* [3] is:

Definition 1: *The sequences* $\{\mu(j)\}_{j=0}^{n-1}$, $\{\eta(j)\}_{j=0}^{n-1}$, *consisting of n elements with values +1 and -1:* $\mu(j) \in \{-1,+1\}$; $\eta(\mathrm{j}) \in \{\text{-}1,+1\}$; $\mathrm{j} = 0,1,...,\mathrm{n}\text{-}1$, *are called pair of complementary series, if:*

$$R_c(k) = R_\mu(k) + R_\eta(k) = \begin{cases} 2n; & k = 0 \\ 0; k = \pm 1, \pm 2, ..., \pm(n-1) \end{cases} . \quad (3)$$

In (3) the non-periodical *ACF* $R_\mu(k)$ and $R_\eta(k)$ are defined with the well known formula:

$$R_\varsigma(k) = \begin{cases} \sum_{j=0}^{n-1-|k|} \varsigma(j) \varsigma^*(j+|k|), & -(n-1) \le k \le 0 \\ \sum_{j=0}^{n-1-k} \varsigma^*(j) \varsigma(j+k), & 0 \le k \le n-1 \end{cases} . \quad (4)$$

The *CSs* are unique among all *PM* signals with the following their features:

- their summary *ACF* has an ideal shape, similar to delta impulse;
- if a pair of complementary series, consisting *n* elements, is known, then it is easy to create an infinite set of pairs with unlimited sequence (or code) length.

With regard to second features, it is necessary to emphasize that the most types *PM* signals with close to ideal *ACF* have limited code-length. For instance, Barker codes exist only for $n \le 13$, if *n* is an odd integer.

In the original Golay's paper are proved the so-called theorems 11 and 12 [3], which show the way we can obtain derivative *CSs* with code-length *2n.r* if two pairs with code-length *n* and *r* are known.

Complementary series with code-length $n = 2,10,26$ are known at present days. Using them and Golay's theorems, it is possible to create infinite number of complementary series with code-lengths:

$$n = 2^u . 10^v . 26^w . \quad (6)$$

The usage of only binary phase modulation, according to Definition 1, often is not appropriate due to following reasons:

- the length *n* of the *CSs* must satisfy (6);
- it is hard to regulate the information transmission rate if *CSs* are used in a communication system.

With regard to these constrains, in our previous papers [2] we:

- introduced the so-called *Generalized Complementary Sequences (GCS)*, where the phase modulation can be arbitrary (i.e. not necessarily binary);
- proved an iterative method for *GCS* synthesis, which allows obtaining a *GCS* with practically arbitrary size using some initial *GCS* with short sizes.

Especially, we have proved a theorem, which includes the Golay's theorem as a particular case. This common theorem uses the following definitions.

***Definition 2*:** *The matrix* $H_{q,p} = \{h_{k,l}(x)\}; k = 1,2,...,q; l = 1,2,...,p$ *will be called generalized column orthogonal matrix, if:*

$$\sum_{k=1}^{q} h_{k,j}(x).h^{*}_{k,s}(x^{-1}) == \begin{cases} c; & c = const, \quad if\ j = s; \\ 0, & if\ j \neq s; j = 1,2,...,p; s = 1,2,...,p. \end{cases} \tag{7}$$

The entries of the matrix $H_{p,q}$ in (7) are polynomials which maximal power of x is equivalent in every column: $\deg h_{k,j} = r_j - 1; j = 1,2,\ldots,p$.

Examples of the matrix H when $\deg h_{k,j}(x) = 0$ are:

$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}$, $\begin{bmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{bmatrix}$, where: $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$; $\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $1 + \omega + \omega^2 = 0$.

Only two sequences participate in the classical definition of the *CSs*. In some practical cases this restriction isn't appropriate. If the number of the sequences is bigger than two, then the following definition must be used.

Definition 3**:** *The set of p sequences:*

$$\{A_1 = \{\xi_1(j)\}_{j=0}^{n_1-1}; ...; A_p = \{\xi_p(j)\}_{j=0}^{n_p-1}\}; \quad \xi_k(j) \in \{\exp(2\pi i l / m_k); l = 0,1,...,m_k - 1\};\ k = 1,2,...,p \tag{8}$$

will be called generalized complementary set, if:

$$R_c(r) = \sum_{k=1}^{p} R_{A_k}(r) = \begin{cases} n = n_1 + n_2 + ... + n_p; if\ r = 0; \\ 0;\ if\ r = 1,2,...,\max\{n_k\}. \end{cases} \tag{9}$$

The common theorem is:

Theorem 1**:** *Let* $H_{q,p}$ *be generalized orthogonal column matrix, and let* $\{A_k = \{\xi_k(j)\}_{j=n_1+...+n_{k-1}}^{n_k-1}\}_{k=1}^{p}$ *be a generalized complementary set. Then the set:*

$$\{h_{11}.A_1,...,h_{1p}.A_p\}; \{h_{21}.A_1,...,h_{2p}.A_p\}; ...; \{h_{q1}.A_1,...,h_{qp}.A_p\}, \tag{10}$$

is generalized complementary set also. The multiplications in (10) mean:

$$h_{ij}.A_k = \zeta_{ij}(0).A_k, \zeta_{ij}(1).A_k, ..., \zeta_{ij}(r_j - 1).A_k,$$

where $h_{ij}(x) = \zeta_{ij}(r_j - 1).x^{r_j - 1} + \zeta_{ij}(r_j - 2).x^{r_j - 2} + \zeta_{ij}(0)$.

Theorem 1 utilizes the problem of complementary sequences synthesis to two steps: first, finding of an arbitrary "*beginning*" complementary set $\{A_k\}_{k=1}^{p}$, and, second, constructing of an appropriate "*creative*" column orthogonal matrix $H_{p,q}$. Having in mind that the well known Hadamar matrices are column orthogonal matrices, which may exist for every size $n \equiv 0 (\mathrm{mod}\, 4)$, our attention shall be focused on the first step. Namely, we shall prove an algorithm for Computer synthesis of *GCSs* when the number of sequences in the generalized complementary set is $p = 2$ and quadric-phase manipulation is used (i.e. $m = 4$ in (2)). In this case the elements of the beginning complementary set $\{A_k\}_{k=1}^{2}$ are the numbers $(\pm 1, \pm i)$. Appearing of the numbers $\pm i$ complicates the *GCS* computer synthesis. Due to this reason we shall transform the synthesis of *GCS* with $p = 2$ and $m = 4$ in synthesis of generalized complementary sets with $p = 4$ and $m = 2$.

Let $A(x)$ and $B(x)$ be the polynomials which coefficients are the elements of desirable *GCS* with $p = 2$ and $m = 4$. Then their real and imaginary parts will be:

$$\mathrm{Re}\, A(x) = C(x);\ \mathrm{Im}\, A(x) = D(x);\ \mathrm{Re}\, B(x) = E(x);\ \mathrm{Im}\, B(x) = F(x) \tag{11}.$$

It is obvious that $C(x)$ $D(x)$, $E(x)$ and $F(x)$ are polynomials which coefficients are only ± 1 or 0 and:

- if the coefficient of x^j in $C(x)$ (respectively in $E(x)$) is ± 1, then the coefficient of x^j in $D(x)$ (respectively in $F(x)$) is 0 ($j = 0,1,....,n-1$);

- if the coefficient of x^j in $C(x)$ (respectively in $E(x)$) is 0, then the coefficient of x^j in $D(x)$ (respectively in $F(x)$) is ± 1 ($j = 0,1,....,n-1$).

The necessary condition for existing of *GCS* with $p = 2$ and $m = 4$ has the following polynomial form:

$$A(x).A^*(x^{-1}) + B(x)B^*(x^{-1}) = 2n \qquad (12).$$

From (11) and (12) follows:

$$[C(x) + iD(x)][C(x^{-1}) - iD(x^{-1})] + [E(x) + iF(x)][E(x^{-1}) - iF(x^{-1})] = 2n. \qquad (13).$$

After opening of the parenthesis in (13) and taking in account the equivalence of real and imaginary parts of the left and right sides, the result is:

$$C(x).C(x^{-1}) + D(x).D(x^{-1}) + E(x).E(x^{-1}) + F(x).F(x^{-1}) = 2n \qquad (14),$$

$$-i[C(x).D(x^{-1}) + C(x^{-1}).D(x) + E(x).F(x^{-1}) + E(x^{-1}).F(x)] = -i.0 \qquad (15).$$

The formula (14) can be transformed as follows:

$$\begin{aligned} &2C(x).C(x^{-1}) + 2D(x).D(x^{-1}) + 2E(x).E(x^{-1}) + 2F(x).F(x^{-1}) = \\ &= [C(x) + D(x)][C(x^{-1}) + D(x^{-1})] + [C(x) - D(x)][C(x^{-1}) - D(x^{-1})] + \\ &+ [E(x) + F(x)][E(x^{-1}) + F(x^{-1})] + [E(x) - F(x)][E(x^{-1}) - F(x^{-1})] = 4n \end{aligned} \qquad (16).$$

After substitutions:

$$\begin{aligned} &C(x) + D(x) = K(x); \quad C(x) - D(x) = L(x); \\ &E(x) + F(x) = M(x); \quad E(x) - F(x) = N(x), \end{aligned} \qquad (17),$$

formula (16) obtains the form:

$$K(x).K(x^{-1}) + L(x).L(x^{-1}) + M(x).M(x^{-1}) + N(x).N(x^{-1}) = 4n. \qquad (18).$$

The polynomials (18), according to (11), have only coefficients ± 1. Hence, the following Corollary is true.

***Corollary 1**:* If *GCSs* with $p = 2$ and $m = 4$ exist then they can be derived from a generalized complementary set with $p = 4$ and $m = 2$.

With regard to Corollary 1 it is necessary to find the sufficient conditions, which allow the transforming of a generalized complementary set with elements ± 1 in *GCSs* with elements ± 1 and $\pm i$. Due to this reason from (17) $C(x)$, $D(x)$, $E(x)$ and $F(x)$ will be expressed by means of $K(x)$, $L(x)$, $M(x)$ and $N(x)$:

$$\begin{aligned} &C(x) = \frac{1}{2}[K(x) + L(x)]; \quad D(x) = \frac{1}{2}[K(x) - L(x)]; \\ &E(x) = \frac{1}{2}[M(x) + N(x)]; \quad F(x) = \frac{1}{2}[M(x) - N(x)]. \end{aligned} \qquad (19).$$

According to (19) the condition (15) obtains the form:

$$\begin{aligned} &[K(x) + L(x)][K(x^{-1}) - L(x^{-1})] - [K(x^{-1}) + L(x^{-1})][K(x) - L(x)] + \\ &+ [M(x) + N(x)][M(x^{-1}) - N(x^{-1})] - [M(x^{-1}) + N(x^{-1})][M(x) - N(x)] = 0. \end{aligned} \qquad (20).$$

The up and low rows of the formula (20) can be expanded to:

$$\begin{aligned} &K(x).K(x^{-1}) - K(x).L(x^{-1}) + K(x^{-1}).L(x) - L(x).L(x^{-1}) - K(x).K(x^{-1}) - \\ &- K(x).L(x^{-1}) + K(x^{-1}).L(x) + L(x).L(x^{-1}) = -2K(x).L(x^{-1}) + 2K(x^{-1}).L(x) \end{aligned} \qquad (21).$$

$$\begin{aligned} &[M(x) + N(x)][M(x^{-1}) - N(x^{-1})] - [M(x^{-1}) + N(x^{-1})][M(x) - N(x)] = \\ &= -2M(x).N(x^{-1}) + 2M(x^{-1}).N(x) \end{aligned} \qquad (22).$$

The taking into account (21) and (22) in (20) leads to:

$$K(x).L(x^{-1}) - K(x^{-1}).L(x) + M(x).N(x^{-1}) - M(x^{-1}).N(x) = 0, \qquad (23)$$

which must be found.

The Corollary 1 and sufficient condition (23) allowed us to develop the following algorithm for synthesis of GCSs with $p = 2$ *and* $m = 4$*:*

1) on the base of possible expressions of the integer *4n* as sum of four quadrates (i.e. $a^2 + b^2 + c^2 + d^2 = 4n$) the quantities of plus and minus ones in the generalized complementary set $\{\zeta_k(j)\}_{j=0}^{n-1};\ k = 1,2,3,4$ with elements ± 1 is determined;

2) our common algorithm [2] for synthesis of complementary sets $\{\zeta_k(j)\}_{j=0}^{n-1};\ k = 1,2,3,4$ with elements ± 1 is applied;

3) every found at the previous step complementary set $\{\zeta_k(j)\}_{j=0}^{n-1};\ k = 1,2,3,4$ with elements ± 1 is tested whether it satisfies the sufficient condition (23);

4) using formulas (19), all complementary sets $\{\zeta_k(j)\}_{j=0}^{n-1};\ k = 1,2,3,4$, passed the third step, are transformed in *GCSs* with elements ± 1 and $\pm i$.

On the base of above algorithm a computer program for automated synthesis of *GCSs* with elements ± 1 and $\pm i$ was created. With it an exhaustive searching of *GCSs* with elements ± 1 and $\pm i$ was executed. Taking into account that *CSs* with lengths $n = 2^u.10^v.26^w$ exist, our attention was focused on *GCSs* with elements ± 1, $\pm i$ and lengths $n = 3,5,7,9,11$. As a result, the following unknown till now *GCSs* were found:

$$A(2,3,4) = \{1,i,1\};\ B(2,3,4) = \{1,-1,1\};$$
$$A(2,5,4) = \{-i,i,1,1,1\};\ B(2,5,4) = \{1,i,-1,1,-i\}. \quad (24)$$

The usage of these *GCSs* and the common Theorem 1 allows creating of infinite number of generalised complementary sets with arbitrary *p* and *GCSs* with lengths $n = 2^u.3^s.5^t.10^v.26^w$.

Now we shall show the tight connection between generalised complementary sets and recently proposed *matrix signals* [4].

Referring to [1], *the generalized matrix signals* are set of *n* matrices $A_k,\ k = 1,2,...,n$, which entries $a_{lj}^k,\ \left|a_{lj}^k\right| = 1,\ k = 1,2,...,n;\ l = 1,2,...,n;\ j = 1,2,...,n$ are only m^{th} roots of unity:

$$a_{lj}^k \in \{\exp(2\pi si/m);\ m = 0,1,...,m-1\} \quad (25)$$

and *the cross-correlation function (CCF)* of two arbitrary matrices in the set is:

$$R_{ks}(r) = \sum_{l=1}^{n}\sum_{j=1}^{n-r} a_{lj}^k.\tilde{a}_{lj+r}^s = \begin{cases} n^2\delta(r), & if\ k = s; \\ 0, & if\ k \neq s, \end{cases}. \quad (26)$$

In Eq. (26):

- $r = 0,1,2,...n-1$ is the horizontal shift of the matrix A_s relatively to matrix A_k;
- $\delta(r)$ is the Kronecker symbol:

$$\delta(r) = \begin{cases} 1, & if\ r = 0; \\ 0, & if\ r \neq 0; \end{cases} \quad (27)$$

- the symbol "~" means "*complex conjugation*".

Every matrix A_k describes mathematically the complex frequency and phase manipulated signal assigned to the k^{th} communication system user. Namely:

- the system frequency band *F* is divided into *n* subbands;
- every complex signal consists of *n* distinct frequency signals with carriers $f_l,\ l = 1,2,...n$, which are the central frequencies of the subbands;
- the phase of every carrier frequency is manipulated according to the elements of the rows of the k^{th} matrix A_k;
- the duration of an elementary phase impulse is τ.

It is necessary to underline two facts:

- amplitude modulation isn't used and hence the amplitudes of the carrier frequencies f_l are equivalent to U_m;

- the Eq. (26) shows that *the auto-correlation function (ACF)* of every signal has ideal shape, similar to a delta-pulse, and the *CCF* of every possible pair of signals is zero.

From these remarks can be concluded that *the generalized matrix signals* are a derivative from generalized complementary sets structure with parameters $p = n$. This is the reason, *the generalized matrix signals* to be called *generalised orthogonal complementary codes (GOCC)* in [1].

CONCLUSIONS AND FUTURE WORK

From all the above stated, it is easy to see that our algorithm for computer synthesis of complementary sequences can be successfully used in the following areas:

- the modern radar systems, because the complex signals increase the maximal detection range without suffering the range resolution ability;

- in the new generation communication systems, due to possibility to control the transmitted information rate by varying the value of *m*.

In a future work we intend to prove method for synthesis of *GOCC* using as a base the sets of generalized complementary sequences.

REFERENCES

[1] B. Y. Bedzhev, Zh. St. Zhekov, P. K. Prodanova, "A method for synthesis of orthogonal complementary codes", Proceedings of the Scientific Conference CERC2004, Bucharest, Romania (under printing)

[2] B. Y. Bedzhev, O. M. Fetfov, Y. I. Tzonev, "An Algorithm for Synthesis of Discrete Frequency Manipulated Radar Signal", Proceedings of "P. Volov" AADMA Scientific Conference, Part II, Shoumen, 2001, pp. 143 – 150

[3] Golay M. Y. E., Complementary series, IRE Trans. on Information Theory, 1961, vol. IT – 7, №2, pp. 82 – 87

[4] V. V. Ignatov, S. A. Dobrovolskiy, A. Yu. Guzhva, "Matrix signal systems used in CDMA systems", Electrosviaz, 2003, № 9, c. 41-42 (in Russian)

[5] Варакин Л. Е., Системы связи с шумоподобными сигналами - М.: Радио и связь,1985. – 384 с.

ABOUT THE AUTHORS

Assoc. Prof. Eng. DSc. Borislav Y. Bedzhev, NMU "V. Levski", Faculty of Artillery and Air Defense, Shoumen, Bulgaria, Phone: +359 5446438, e-mail: bedzhev@mail.pv-ma.bg.

Prof. Eng. PhD. Zhaneta N. Tasheva, NMU "V. Levski", Faculty of Artillery and Air Defense, Shoumen, Bulgaria, Phone: +359 5452371, e-mail: tashevi86@yahoo.com.

Assistant Prof. Mag. PhD Student Borislav P. Stoyanov, Shoumen University, Shoumen, Bulgaria, Phone: +359 5447848, e-mail: bpstoyanov@abv.bg.