Journal scientific and applied research, vol. 2, 2012
Association Scientific and Applied Research
International Journal

ISSN 1314-6289

Original Contribution

METHOD FOR SYNTHESIS OF LARGE FAMILIES OF SIGNALS WITH LOW CORRELATION

Borislav Y. Bedzhev, Stoyan S. Yordanov

bedzhev@abv.bg, stoyan.yordanov1000@abv.bg

Abstract: *In the paper a new method for synthesis of large families of signals with low auto- and cross-correlation is presented. It is based on the known method for generation of Gold sets but is not related to a certain value of the decimation coefficient d. As a result it allows generating of families, consisting of p-ary M – sequences, for arbitrary values of p and the degree of their characteristic equation.*

Key words: *synthesis of signals, family of signals with low periodic correlation.*

1. Introduction

Sequences with low periodic correlation (LPC) find many applications in radars and wireless communications for synchronization and for providing the simultaneous work of multiple users with low mutual interference. With regard methods for synthesis of families of signals with LPC have been researched from many authors for the last several decades [1] – [19].

In this paper a new method for creating of large sequence sets with LPC is presented. It is based on the known method for generation of the so-named *Gold sets* [1], [19], but is more general. The main advantage of the method is that it is not related to a certain value of the decimation coefficient *d*. Therefore it is applicable for all *p*-ary *M*–sequences independently of the sen values of *p* and the degree *n* of their characteristic equation.

The paper is organized as follows. First, the basics of the synthesis of the *M*-sequences are recalled in Section 2. After that in Section 3, a new general method for synthesis of phase manipulated (PM) signals, possessing both low level of the lobes of the periodic auto- and cross-correlation is suggested. Conclusions of the paper are summarized in Section 4.

2. Basics of the synthesis of the *M*-sequences

The linear recurring sequences (LRS) find wide implementation in many fields, especially for information protection and in communications [1], [2], [3], [11], [18], [19]. Due to this reason they have been extensively studied since 50th years of the 20th century.

LRSs are created by means of a linear recursive equation (LRE), which can be expressed as [19], [20]:

(1) $$u(i) = a_{n-1}.u(i-1) + a_{n-2}.u(i-2) + ... + \\ + a_0.u(i-n)$$

where:

- $u(i)$ is the new *i*-th element of the *LRS*;

- $u(i-1), u(i-2), ..., u(i-n)$ are elements of the considered *LRS,* obtained during the previous steps of the LRE (1) (the initial elements $u(0), u(1), ..., u(n-1)$ should be known);

- $a_{n-1}, a_{n-2}, ..., a_0$ are coefficients, belonging to a finite algebraic field (named *Galois Field* (*GF*)) and all algebraic operations in (1) are performed in *GF*(p^m) (i.e. modulo *p*, where *p* can be an arbitrary prime integer).

After the substitution $u(i) = x^i,\ i = 0,1,2,...,$ (1) is transformed into the so-named *characteristic equation* (noted often as *the connection polynomial* of the linear feedback shift registers (LFSRs), which are the hardware, realizing the LRE (1)):

(2) $$x^n - d_{n-1}.x^{n-1} - d_{n-2}.x^{n-2} - \\ - ... - d_0 = 0$$

If the left side of the characteristic equation is a primitive irreducible polynomial over *GF*(p^{m}), then the period of the LRS is maximal, namely $N = (p^m)^n - 1$ and it is called *maximal length sequence* (*M – sequence*) [19], [20].

In communications the *M*-sequences are used for controlling the phase modulation of the PM signals. Due to the symmetric connection the derivative PM signals are named *M*-sequences also. The main advantage of these signals is that their periodic autocorrelation function (PACF) is almost perfect, because the level of the side-lobes is constant and equal to -1 [19], i.e.:

(3) $$P_{\zeta\zeta}(r) = \sum_{i=0}^{N-1} \zeta(i).\zeta^*\langle i+r \rangle = \\ = \begin{cases} N, & r = 0, \\ -1, & r \neq 0. \end{cases}$$

In (3) $P_{\zeta\zeta}(r)$ is the PACF of the *M*-sequence $\{\zeta(i)\}_{i=0}^{N-1}$, *r* is the time shift, the symbol "$\langle\ \rangle$" means "summing modulo *p*", and symbol "*" – "complex conjugation".

The complex envelopes of the elementary phase impulses (chips) of the PM signal are described with the following equation (or *coding rule*):

(4) $$\zeta(i) = \exp\left[j\frac{2\pi m}{p} u(i) \right],\ j = \sqrt{-1}, \\ 1 \le m \le p-1,\ i = 0,1,2,...,N-1,...$$

Here $u(i)$ are the elements of the *M*-sequence, controlling the phase modulation [18], [19].

Another important advantage of the PM signals, which are *M*-sequences, is that their length can be arbitrary long even though the size of the signal alphabet is small. This feature is essential if longer sequences are required.

3. Method for synthesis of large families of signals with low correlation

Key feature of the methods for synthesis of signals for the present communication systems is the possibility for synthesis of families (sets) of signals, possessing both periodic auto- and cross-correlation functions with small level of the side-lobes. These conditions can be mathematically described as follows. Let Φ (K, N, C) be a set of *K* signals with period *N* and with maximal level *C* of the auto- and cross-correlation lobes:

$$C \le \eta\sqrt{N} \tag{5}$$

Here η is a coefficient with relatively low value. In this case Φ (K, N, C) is named *family of signals with low periodic correlation (LPC)* [19], [20], [21].

The known methods for generation of *M* - sequences with low cross-correlation are based on the principle of the permutation of a *M*-sequence or the so – named *decimation* [1]-[19]. Let we have a sequence $\{\xi(i)\}_{i=0}^{N-1}$ with ideal PACF, similar to a delta pulse. Then the derivative signals $\{\xi_k(i)\}_{i=0}^{N-1}$, obtained by the rule:

$$\begin{gathered}\xi_k(i) = \xi\langle d_k.i\rangle_{\mathrm{mod}\,N}, \\ i = 0,1,2,\ldots,N-1,\ldots\end{gathered} \tag{6}$$

have also ideal PACF [1] - [19]. Here the decimation coefficients $d_k, k = 1,2,\ldots,N_t$ are the all possible positive integers smaller than ***N*** and co-prime to ***N***, and the symbol " $\langle d_k.i\rangle_{\mathrm{mod}\,N}$ " means "multiplication modulo *p*".

In the sequel we shall suggest a new method for synthesis of families of signals with LPC. It is a generalization of the so-named *Gold method* [1], [19], which can be described as follows. For $0 \le l < 2^n - 1$ and *n* an arbitrary odd integer, let $s_l = \{s_l(i)\}_{i=0}^{2^n-2}$ be a binary sequence, whose elements are evaluated by the rule:

$$\begin{gathered}s_l(i) = Tr(\alpha^j\alpha^i + \alpha^{di}), \\ i = 0,1,\ldots,2^n - 2.\end{gathered} \tag{7}$$

Then s_l is called a *Gold-pair sequence* [19]. Here α is an arbitrary primitive element of *GF*(*2*^{n}), *d*, $d = 2^k + 1,\ \gcd(k,n) = 1,\ k \le (n-1)/2$ is an integer co-prime with $N = 2^n - 1$ and $Tr(\alpha^l.\alpha^i + \alpha^{di})$ denotes the trace function of the elements $\alpha^l.\alpha^i + \alpha^{di}$ of *GF*(*2*^{n}) to *GF*(2). In this situation, the set, given by [19]:

$$S(d) = \{s_l \,|\, 0 \le l \le 2^n\}, \tag{8}$$

is said to be a *Gold-pair (signal) set*. Note, that $a = s_{2^n-1} = \{Tr(\alpha^i)\}_{i=0}^{2^n-2}$ and $b = s_{2^n} = \{Tr(\alpha^{di})\}_{i=0}^{2^n-2}$, are *M*-sequences [19] and, consequently, they possess an almost ideal PACF, according to (3). Besides, it is easy to see that the set (family) (8) is generated by the pair-wise summing modulo 2 of the sequences ***a*** and ***b***:

$$(9) \qquad s_l = L^l a + b,\ 0 \le l < N-1.$$

Here $L^l a$ means “right rotation of the sequence ***a*** at *l* steps”.

It is proven [1], [19] that the signal set (8) is a family Φ (K, N, C) of signals with LPC with parameters:

$$(10) \qquad \begin{array}{l} K = 2^n + 1 = N + 1,\ N = 2^n - 1, \\ C = 2^{(n+1)/2} + 1 \end{array}$$

With regard to the described Gold method, since 1968 many authors (for example Kasami, Welch, No, Kumar, Niho, Helleseth, Müller) have proposed different values of the decimation coefficients *d* that can be used in the construction (7) [2], [4], [5], [6], [7], [8], [10], [11], [13], [14], [15], [16], [17], [19]. It should be pointed out that despite of the all efforts there is no any general method, applicable for all values of *n* and *p*.

With regard below we shall prove a different approach for finding of decimation coefficients *d* for *M*-sequences over an arbitrary finite field *GF*(*p*) so that the requirement (5) to be satisfied. The new method consists of the following steps.

1) For given *p* and *n* with a computer program all possible values of the decimation coefficients *d*, $\gcd(d, N = p^n - 1) = 1$, are calculated. Note that these decimation coefficients *d*, applied in (6), transform every *M*-sequence over *GF*(*p*) with a characteristic equation of degree *n* in a *M*-sequence of the same type [19], [20]. In this way an initial family (set) of *M*-sequences is obtained.

2) With the above computer program the initial set is filtered in order to retain only these pairs of *M*-sequences which periodic cross-correlation function (PCCF) satisfies the restriction (5).

3) The *M*-sequences from the all selected pairs are used in the Gold construction (7), which provides a large number of different families of signals with LPC.

The correctness of the proposed method is a consequence of the following facts. First of all, let ***a*** be an arbitrary *M*-sequence over *GF*(*p*) with characteristic equation of degree *n*. As known, it can be presented in the form [19]:

$$(11) \qquad a = \left\{ Tr(\gamma\alpha^i) \right\}_{i=0}^{N-1},\ N = p^n - 1,$$

where α is a primitive element of *GF*(*p*^n^), $\gamma = \alpha^u$ for some *u*, $0 \le u < N$ and $Tr(z)$ is the so-named trace function, which maps the elements of $GF(p^n)$ to *GF*(*p*) [19], [20]:

$$(12) \qquad Tr(z) = z^{p^0} + z^{p^1} + ..z^{p^{n-1}}.$$

According to the above method, let ***b*** be another *M*-sequence, obtained by a decimation of ***a***, so that the maximal absolute level *C* of the lobes of PCCF of the sequences ***a*** and ***b*** does not exceed the restriction (5). Consequently, ***a*** and ***b*** form a family V (K, N, C) of signals with LPC, which parameters are:

(13) $K = 2,\ N = p^n - 1,\ C = \eta\sqrt{N}$.

(Note that ***a*** and ***b*** are *M*-sequences and as a result the maximal level of the side-lobes of theirs PACF do not exceed -1).

It should be pointed out that ***b*** can be presented in the form [19]:

(14) $b = \left\{Tr(\delta\beta^i)\right\}_{i=0}^{N-1},\ N = p^n - 1,$

where $\beta = \alpha^d$, $\gcd(d, N) = 1$ is also a primitive element of $GF(p^n)$, $\delta = \beta^v$ for some v, $0 \le v < N$.

Now, let this initial family be enlarged by the all sequences, generated by the rule (9). We shall show that the maximal absolute level of the lobes of the PACFs and PCCFs of the new family, consisting of $K = p^n + 1 = N + 2$ sequences, satisfy (5).

In order to prove the above proposition it is necessary to consider the following cases.

Case 1. The PACFs of the sequences ***a*** and ***b*** and their PCCF satisfy (5) due to the peculiarities of the initial family V (K, N, C).

Case 2. Let $\omega = \exp(j\dfrac{2\pi m}{p})$, $1 \le m \le p - 1$ be an arbitrary *p*-th root of unity. Then the PCCF of an arbitrary pair s_l, s_k, $0 \le l < k \le N - 1$ is:

(15)
$$\begin{aligned} &P_{s_l s_k}(r) = \\ &= \sum_{i=0}^{N-1}\Big[\omega^{Tr(\gamma\alpha^l\alpha^i + \delta\beta^i)} \times \\ &\times \omega^{Tr(\gamma\alpha^k\alpha^{i+r} + \delta\beta^{i+r})}\Big] = \\ &= \sum_{i=0}^{N-1}\Big[\omega^{Tr[\gamma(\alpha^l - \alpha^{k+r})\alpha^i]} \times \\ &\times \omega^{Tr[\delta(1-\beta^r)\beta^i)}\Big] = \\ &= P_{ab}(u' - v') \end{aligned}$$

Here $\alpha^{u'} = \alpha^l - \alpha^{k+r}$, $\beta^{v'} = 1 - \beta^r$ and *u'* and *v'* show the steps of the right rotations of ***a*** and ***b*** respectively.

Now it should be seen that the PCCF ($P_{ab}(u' - v')$) of the *M*-sequences ***a*** and ***b*** satisfy (5), according to their choice. Besides, if $r \equiv 0 \bmod N$ then

(16) $P_{s_l s_k}(0) = P_{aa}(l - k) = -1$.

Case 3. The PACF of an arbitrary sequence s_l, $0 \le l \le N - 1$ can be evaluated from (15) after the substitution $l = k$. The result is

(17) $P_{s_l s_l}(r) = \begin{cases} P_{ab}(u' - v'), & r \ne 0; \\ N, & r = 0. \end{cases}$

Here $\alpha^{u'} = \alpha^l(1 - \alpha^r)$, $\beta^{v'} = 1 - \beta^r$.

Case 4. The PCCF of an arbitrary pair s_l, a, $0 \le l \le N - 1$ is:

(18) $P_{s_l a}(r) = \begin{cases} P_{ab}(u' - v'), & r \ne 0; \\ -1, & r = 0. \end{cases}$

Here $\alpha^{u'} = \alpha^{l} - \alpha^{r}$, $\beta^{v'} = -\beta^{r}$. In (18) it is accounted that if $r = 0$, then $P_{s_l a}(0) = \sum_{i=0}^{N-1} \omega^{Tr(\delta\beta^{i})}$ and the sequence $\left\{Tr(\delta\beta^{i})\right\}_{i=0}^{N-1}$ contains p^{n-1} times the elements $1, 2, \ldots, p-1$ and $p^{n-1}-1$ times the element 0 [19], [20].

Case 5. The PCCF of an arbitrary pair $s_l, b,\ 0 \le l \le N-1$ is:

$$(19) \quad P_{s_l b}(r) = \begin{cases} P_{ab}(u'-v'), & r \ne 0; \\ -1, & r = 0. \end{cases}$$

Here $\alpha^{u'} = \alpha^{l}$, $\beta^{v'} = \beta^{r} - 1$. In (19) it is accounted that if $r = 0$, then $P_{s_l b}(0) = \sum_{i=0}^{N-1} \omega^{Tr(\gamma\alpha^{i})}$ and the sequence $\left\{Tr(\gamma\alpha^{i})\right\}_{i=0}^{N-1}$ contains p^{n-1} times the elements $1, 2, \ldots, p-1$ and $p^{n-1}-1$ times the element 0.

This finishes the all possible variants.

The new method for synthesis of families of signals with LPC will be illustrated by the following examples.

Example 1: Let we consider a *M*-sequence over *GF*(2^5) with length $N = 2^5 - 1 = 31$. The results of a survey of the all possible decimation coefficients *d* and the maximal absolute level of the PCCFs of the initial *M*-sequence and the decimated *M*-sequences, are shown in table 1.

Table 1: A Survey of the maximal values of the cross-correlation functions of the initial and the decimated *M*-sequences with length *N* = 31

d	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C	31	9	31	9	9	9	31	9	9	9	9	9	9	11	31

d	17	18	19	20	21	22	23	24	25	26	27	28	29	30
C	9	9	9	9	9	9	11	9	9	9	11	9	11	11

In table 2, a comparison of the known at present methods for synthesis of families of signals with low LPC is presented for the *M*-sequences over GF(2^5) with length $N = 2^5 - 1 = 31$, [2], [4], [5], [6], [7], [8], [10], [11], [13], [14], [15], [16], [17], [19].

Table 2: Comparison of the known methods for synthesis of families of signals with low LPC for N = 31

	Gold decimation $d=2^{k}+1$, $k\le(n-1)/2$	Kasami decimation $d=2^{2k}-2^{k}+1$, $k\le(n-1)/2$	Welch decimation $d=2^{(n-1)/2}+3$	Niho decimation $d=2^{2k}+2^{k}-1$, $k=(n-1)/4$ or $(3n-1)/4$	Decimations, according to the new method
C=9	5	13	7	5	3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 24, 25, 26, 28
C=11	-	-	-	-	15, 23, 27, 29, 30

Example 2: Let we consider a ternary (i.e. $p=3$) M - sequence with length $N=3^3-1=26$. The results of a survey of the all possible decimation coefficients d and the corresponding *M*-sequences, are shown in table 3.

Table 3 A Survey of the maximal absolute values of the cross-correlation functions of the initial and the decimated *M*-sequences with length *N* = 26

d	3	5	7	9	11	15	17	19	21	23	25
C	26	10	10	26	10	10	10	10	10	10	10

As can be seen the decimation coefficients 5, 7, 11, 15, 17, 19, 21, 23 and 25 can be used in order to generate families of signals with maximal absolute level $C=10$ of the lobes of the PCCFs.

4. Conclusion

In the paper a general method for synthesis of families of signals with low periodic correlation is suggested. It is more general by the known at present methods and as a result it is applicable for all possible values of *p* and *n*. These positive features are confirmed by the results, obtained by exhaustive computer surveys, shown in tables 1-3.

The proposed method can be successfully used in the process of development of perspective wireless communication system, providing both very high rate of information transmission and data protection.

Bibliography:

[1] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions, ”IEEE Trans. Inf. Theory, vol. IT-14, no. 1, pp.154–156, Jan. 1968.

[2] T. Kasami, Weight Distribution Formula For Some Class of Cyclic Codes, Coordinated Sci. Lab., Univ. Illinois at Urbana-Champaign, Urbana, IL, 1996, Tech. Rep. R-285 (AD 632574).

[3] J.-S. No and P. V. Kumar, “A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span,” IEEE Trans. Inf. Theory, vol. 35, no. 2, pp. 371–379, Mar. 1989.

[4] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, “New family of p-ary sequences with optimal correlation property and large linear span,”IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1839–1844, Aug. 2004.

[5] H. M. Trachtenberg, “On the Cross-Correlation Functions of Maximal Recurring Sequences,” Ph.D. dissertation, Univ. of Southern California, Los Angeles, 1970.

[6] T. Helleseth, “Some results about the cross-correlation function between two maximal linear sequences,” Discr. Math., vol. 16, pp. 209–232, 1976.

[7] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, “Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type,” IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1473–1481, May 2001.

[8] G. J. Ness, T. Helleseth, and A. Kholosha, “On the correlation distribution of the Coulter–Matthews decimation,” IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2241–2247, May 2006.

[9] P. V. Kumar and O. Moreno, “Prime-phase sequences with periodic correlation properties better than binary sequences,” IEEE Trans. Inf. Theory, vol. 37, no. 3, pp. 603–616, May 1991.

[10] E. N. Müller, “On the cross-correlation of sequences over GF(p) with short periods,” IEEE Trans. Inf. Theory, vol. 45, no. 1, pp. 289–295, Jan. 1999.

[11] Z. Hu, Z. Li, D. Mills, E. N. Müller, W. Sun, W. Willems, Y. Yang, and Z. Zhang, “On the cross-correlation of sequences with the decimation factor d=((pn+1)/(p+1))-((pn-1)/2),” Applicable Algebra in Engineering, Communication and Computing, vol. 12, pp. 255–263, 2001.

[12] L. R. Welch, “Lower bounds on the maximum cross-correlation of signals,” IEEE Trans. Inf. Theory, vol. IT-20, no. 3, pp. 397–399, May 1974.

[13] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, “Cross-correlation distribution of p-ary M-sequence and its p-1 decimated sequences with shorter period,” IEICE Trans. Fund. Electron., Commun. Comp. Sci., vol. E90-A, no. 11, pp. 2568–2574, Nov. 2007

[14] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin ”Cross-Correlation Distribution of p-ary M-Sequence of Period p4k-1and Its Decimated Sequences by ((p2k+1)/2)2, IEEE Trans. Inf. Theory, vol. 54, No. 7, July 2008

[15] G. J. Ness, T. Helleseth, and A. Kholosha, ”On the correlation distribution of the Coulter-Matthews decimation,” IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2241-2247, May 2006.

[16] S.-T. Choi, J.-S. No, H. Chung, ”On the cross-correlation of a ternary m-sequence of period 34k+2 − 1 and its decimated sequence by (32k+1+1)2/8,” ISIT 2010, Austin, Texas, U.S.A., June 13-18, 2010.

[17] Y. Sun, Z. Wang, H. Li, “On the Cross-Correlation of a Ternary m-sequence of Period 34k − 1 and Its Decimated Sequence by (32k+1)2 /20

[18] B. Y. Bedzhev, S. Yordanov, An Algorithm for synthesis of system of signals with optimum correlation properties, International Scientific Conference of the University of Ruse “Angel Kanchev”, Ruse, 26-27.10.2012 (In Bulgarian)

[19] Golomb S., G. Gong, Signal design for good correlation for wireless communications, cryptography and radar, Cambridge University Press, 2005, 455 pp.

[20] Zierler N., Linear recurring sequences, J. Soc. Ind. Appl. Math., 7 (1959), №1, pp. 31 – 48