Journal scientific and applied research, vol. 4, 2013
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

AN ALGORITHM FOR SYNTHESIS OF PHASE MANIPULATED SIGNALS WITH HIGH STRUCTURAL COMPLEXITY

Tsvetoslav Tsankov, Tihomir Trifonov, Lilia Staneva

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR.

e-mail: hitar@abv.bg, trif.69@abv.bg, anest_bg@bitex.bg

Abstract: *In the paper an algorithm for synthesis of pseudo-noise signals with high structural complexity is presented. It is based on the possibility the elements of the finite algebraic fields to be generated by means of a linear recurring sequence with maximal length. The algorithm can be used in the development of communication systems with high resistance to hostile radio-electronic environment.*

Key words*: synthesis of signals, phase manipulated signals with high structural complexity.*

1. **Introduction**

Today the radio-electronic warfare plays a very important role in the local military conflicts and in the fight against terroristic and criminal groups. As a consequence, the present communication systems should possess a very high resistance to the radio-electronic counter-measurements. The general method for providing of anti-jamming capabilities is the usage of pseudo-noise signals with high structural complexity (HSC), which are hard both to detect and to imitate. With regard methods for synthesis of signals with HSC have been researched from many authors for the last several decades [1] – [9].

In this paper an algorithm for synthesis of phase manipulated (PM) signals with HSC is presented. It is based on the peculiarities of the non-linear polynomial functions, which are the most resistive to the present crypto-attacks. The main advantage of the algorithm is that it can be easily realized by any specialized computer software for modeling of communication systems.

The paper is organized as follows. First, the present algebraic methods for modeling of PM signals are analyzed in Section 2. After that in Section 3, an algorithm for synthesis of PM signals with HSC is suggested. Conclusions of the paper are summarized in Section 4.

2. Algebraic methods for modeling of phase manipulated signals

The algebraic methods for modeling are a very effective tool in the process of research and development of PM signals for the perspective communication systems. They are based on the fact that any PM signal can be presented as a sequence of complex numbers [2]-[7], [10], [11]

$$\{\zeta(i)\}_{i=0}^{N-1} = \\ = \{\zeta(0), \zeta(1), \ldots, \zeta(N-1)\} \quad (1)$$

called *signal sequence* or simply *PM signal*.

In (1) the length N denotes the quantity of the consecutive elementary phase pulses (chips), forming the PM signal.

The complex number

$$\zeta(i) = U_{mi}.e^{j\psi_i}, \; j = \sqrt{-1} \quad (2)$$

is the so-named *complex envelope* of the i-th chip. It presents the amplitude U_{mi} and the phase angle ψ_i of the i-th chip.

Today the so-named *uniform PM signals*, which satisfy simultaneously the following conditions

$$U_{mi} = U_{m0} = const, i = 1 \div N-1 \quad (3)$$

$$\psi_i \in \left\{ \frac{2\pi}{p} l, \; l = 0 \div p-1 \right\} \quad (4)$$

are preferred due to the following reasons [2]-[9]. First, the condition (3) minimizes the probability of detection of the PM signal by the enemy radio-electronic intelligence as the signal spectrum is uniformly distributed. Second, the observation of the condition (4) leads to simplification and reduction the cost of the communication devices.

In case of uniform PM signals the complex envelopes of the chips become the form [2]-[7], [10]

$$\zeta(i) = U_{m0}.e^{j\frac{2\pi}{p}s(i)} \quad (5)$$

where the integer sequence

$$S = \{s(0), s(1), \ldots, s(N-1)\}, \\ s(i) \in \{0, 1, \ldots, p-1\} = Z_p \quad (6)$$

is called *the power sequence of the uniform PM signal* or simply *the power sequence*.

From (5) we see that the features of the uniform PM signals can be explored on the base of their power sequences. With regard to this conclusion in the rest part of this section we shall focus our attention over the algebraic methods for modeling of the power sequences of uniform PM signals.

The algebraic methods for modeling of the uniform PM signals use some *polynomial function* (or *simply polynomial*) for evaluating the elements of their power sequences:

$$f(x) = \sum_{i=0}^{M} a_i.x_{n-1}^{c_{n-1,i}}.x_{n-2}^{c_{n-2,i}}..x_1^{c_{1,i}}x_0^{c_{0,i}} \quad (7)$$

The polynomial function (7) maps the elements of the extended finite algebraic field GF(p^n), p

prime, to the elements of the prime finite algebraic field GF(p). Here the abbreviation GF means *Galois Field*.

As known [10], all elements of GF(p) are $\{0,1,\ldots,p-1\}$, which can be added and multiplied modulo p. GF(p^n) is obtained by joining to GF(p) an arbitrary zero (root) α of an irreducible over GF(p) polynomial $g(y)$ of n-th degree. The polynomial $g(y)$ is called *the generator polynomial* of GF(p^n). As a result every element of GF(p^n) is viewed as an n-dimensional vector $x=(x_{n-1},x_{n-2},\ldots,x_0)$, which coordinates are defined by the sum

$$x = x_{n-1}.\alpha^{n-1} + x_{n-2}.\alpha^{n-2} + \\ + \ldots + x_1.\alpha + x_0 . \quad (8)$$

If the argument $x=(x_{n-1},x_{n-2},\ldots,x_0)$, $\forall x_i \in GF(p)$ of the polynomial (7) runs through all the vectors (elements) of GF(p^n), following an preliminarily defined order, then a sequence S_f

$$S_f = \{s(i)\}_{i=0}^{L-1} = \\ = \{s(0), s(1),\ldots,s(L-1)\}, L = p^n \quad (9)$$

is obtained. As in (7) the coefficients a_i, $i=0,1,\ldots,M$ and the coordinates x_i, $i=0,1,\ldots,n-1$ of the argument (vector) x are elements of GF(p) and all additions and multiplications are performed modulo p, the elements of the generated sequence S_f are elements of GF(p) also.

From all above stated it follows that the polynomial function (7) describes mathematically an algorithm for synthesis of power sequences of uniform FM signals with length

$$L = p^k, k = 0,1,\ldots,n . \quad (10)$$

This conclusion will be clarified by an example in which $p=2, n=3$ and the polynomial (7) has the following concrete form:

$$f(x) = x_2.x_1.x_0 + x_0 + 1. \quad (11)$$

In this case the sequence S_f, generated by (11), has length $L=2^3=8$ and it is presented in the last column of the Table I (in (11) the coordinates of the argument $x=(x_2,x_1,x_0)$ are listed in the lexicographical order).

Table I
The variant 1 of the sequence S_f, generated by the polynomial (11)

№	(x_2,x_1,x_0)	S_f
0	(0, 0, 0)	1
1	(0, 0, 1)	0
2	(0, 1, 0)	1
3	(0, 1, 1)	0
4	(1, 0, 0)	1
5	(1, 0, 1)	0
6	(1, 1, 0)	1
7	(1, 1, 1)	1

With regard to this example it should be pointed out, that according to the small Fermat's theorem [10] $a^{n-1}=1$ for every element of GF(p). Due to this reason the powers $c_{n-1,i}, c_{n-2,i}, \dots, c_{0,i}$ in (7) can be only integers in the range $[0, p-1]$, i.e.:

(12) $\forall c_{k,i} \in Z_p = \{0, 1, \dots, p-1\}$.

Consequently, in case $p=2$ the powers $c_{n-1,i}, c_{n-2,i}, \dots, c_{0,i}$ can be only 0 or 1 and the polynomial (7) is named *Boolean function* [6], [10], [11].

It should be pointed out, that the coordinates of the argument $x=(x_{n-1}, x_{n-2}, \dots, x_0)$ in (7) can be listed in the following exponential order [6], [10]

(13) $$\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-2},$$

because the sequence (13) contains every non-zero element of GF(p^n).

This will be clarified with the above example ($p=2, n=3$ and the polynomial (7) has the concrete form (11)). In this case the argument of (11) is viewed as an element of GF(2^3), i.e.:

(14) $x = x_2.\alpha^2 + x_1.\alpha + x_0$,

where α is a zero (root) of the irreducible over GF(2) polynomial $g(y)$ of *3*-rd degree

(15) $g(y) = y^3 + y + 1$.

From (14) follows:

(16) $$\begin{aligned} \alpha^0 &= 1 = 0.\alpha^2 + 0.\alpha + 1.1 = \\ &= (0,0,1), \\ \alpha^1 &= 0.\alpha^2 + 1.\alpha + 0.1 = (0,1,0), \\ \alpha^2 &= 1.\alpha^2 + 0.\alpha + 0.1 = (1,0,0). \end{aligned}$$

Then we must have

(17) $\alpha^3 = \alpha + 1 = (0,1,1)$

because α is a zero (root) of (15), i.e.

(18) $\alpha^3 + \alpha + 1 = 0$.

From (18) we obtain

(19) $$\begin{aligned} \alpha^4 &= \alpha.\alpha^3 = \alpha(\alpha+1) = \\ &= \alpha^2 + \alpha = (1,1,0) \\ \alpha^5 &= \alpha.\alpha^4 = \alpha^3 + \alpha^2 = \\ &= \alpha^2 + \alpha + 1 = (1,1,1) \\ \alpha^6 &= \alpha.\alpha^5 = \alpha^3 + \alpha^2 + \alpha = \\ &= \alpha^2 + 1 = (1,0,1) \\ \alpha^7 &= \alpha.\alpha^6 = \alpha^3 + \alpha = \\ &= 1 = (0,0,1) \\ \alpha^8 &= \alpha.\alpha^7 = \alpha = (0,1,0) \\ &\dots\dots\dots\dots\dots\dots \end{aligned}.$$

Consequently $\alpha^0, \alpha^1, \dots, \alpha^6$ presents an exponential ordering of the non-zero elements of GF(p^n), which allows Table I to be transformed in Table II.

Table II
The variant 2 of the sequence S_f,
generated by the polynomial (11)

№	α^i	(x_2, x_1, x_0)	S_f
0		(0, 0, 0)	1
1	α^1	(0, 1, 0)	1
2	α^2	(1, 0, 0)	1
3	α^3	(0, 1, 1)	0
4	α^4	(1, 1, 0)	1
5	α^5	(1, 1, 1)	1
6	α^6	(1, 0, 1)	0
7	α^7	(0, 0, 1)	0

From the point of view of the practical realization by computers, the usage of the exponential order of the elements of GF(p^n) in the polynomial (7) has the following advantages.

First, it can be easily generated by means of *a linear recurring sequence* (LRS) *with maximal length* (*m-sequence* for short) [6], [10].

Second, the exponential order (13) can be presented in many different forms [10]

(20) $(\alpha^d)^0, (\alpha^d)^1, \ldots, (\alpha^d)^{n-2}$.

using any integer *d*, which is co-prime with $p^n - 1$. It is known that *d* can be chosen in $\varphi(p^n - 1)$ different ways. Here $\varphi(l)$ is the so-named *Euler's phi-function*, which gives the quantity of all natural numbers smaller and co-prime with ***l*** [10].

The last ability for listing the argument of the polynomial (7) according to (20) will be clarified with the above example – i.e. $p = 2, n = 3$, the polynomial (7) has the concrete form (11) and the generator polynomial of GF(2^3) is (15). As $2^n - 1 = 2^3 - 1 = 7$ is a prime number, the parameter *d* in (20), often named *coefficient of the decimation*, can be $d = 1, 2, 3, 4, 5, 6$. For simplicity let we choose $d = 2$. In this case Table I is transformed in Table III.

Table III
The variant 3 of the sequence S_f,
generated by the polynomial (11)

№	$(\alpha^2)^i$	(x_2, x_1, x_0)	S_f
0		(0, 0, 0)	1
1	$(\alpha^2)^1 = \alpha^2$	(1, 0, 0)	1
2	$(\alpha^2)^2 = \alpha^4$	(1, 1, 0)	1
3	$(\alpha^2)^3 = \alpha^6$	(1, 0, 1)	0
4	$(\alpha^2)^4 = \alpha^1$	(0, 1, 0)	1
5	$(\alpha^2)^5 = \alpha^3$	(0, 1, 1)	0
6	$(\alpha^2)^6 = \alpha^5$	(1, 1, 1)	1
7	$(\alpha^2)^7 = \alpha^0$	(0, 0, 1)	0

3. Algorithm for synthesis of phase manipulated signals with high structural complexity

The algorithm for synthesis of phase manipulated signals with HSC, which will be presented later in this section, is based on the fact, that the exponential order (20) of the elements of GF(p^n) can be easily generated by means of a LRS with maximal length (m-sequence for short).

The LRSs find a wide application in many areas of the science and techniques [1] - [10], [12]. They are generated by means of a *linear recurrence equation* (LRE) [6], [10], [12]:

$$u(i) = a_{n-1}.u(i-1) + \\ + a_{n-2}.u(i-2) + \ldots + a_0.u(i-n) \quad (21)$$

In (21) the new *i*-th element $u(i)$ of the LRS is evaluated on the base of the elements $u(i-1), u(i-2), \ldots, u(i-n)$ of the LRS, obtained in the previous time moments (it is necessary the initial elements $u(0), u(1), \ldots, u(n-1)$ to be given). Besides, the arithmetic operations in (21) and the coefficients $a_{n-1}, a_{n-2}, \ldots, a_0$ are defined in a preliminary given algebraic field, which can be infinite (i.e. number field) or finite (i.e. Galois Field).

Beginning from the known initial elements $u(0), u(1), \ldots, u(n-1)$ of the LRS, all other elements $u(n), u(n+1), \ldots,$ can be recursively (i.e. step-by-step) evaluated by (21). This method is not always appropriate. Due to this reason a mathematical method for direct evaluating of the elements of a LRS has been developed [10], [12]. This method uses the substitution $u(i) = z^i$, which transforms (21) in the equation:

$$z^{i-n}(z^n - a_{n-1}.z^{n-1} - \\ - a_{n-2}.z^{n-2} - \ldots - a_1.z - a_0) = 0 \quad (22)$$

If $z = 0$, then LRS will consist only of zeros and, obviously, this is the trivial case. Hence, in the non-trivial case $z \neq 0$ and then the both sides of (22) can be reduced by the factor z^{i-n}. This transforms (22) into the so-named *characteristic equation* of the LRS:

$$z^n - a_{n-1}.z^{n-1} - \\ a_{n-2}.z^{n-2} - \ldots - a_1.z - a_0 = 0 \quad (23)$$

Let we suppose, that all the roots $z_1, z_2, \ldots z_n$ of (23) are distinct. In this situation it is not hard to be proven, that the *i*-th element of the LRS can be directly evaluated by the formulae:

$$u(i) = c_1.z_1^i + c_2.z_2^i + \ldots + c_n.z_n^i, \\ i = n, n+1, n+2, \ldots \quad (24)$$

In (24) the coefficients $c_1, c_2, \ldots c_n$ are determined from the following system of linear equations:

$$\left| \begin{array}{l} c_1 z_1^0 + c_2 z_2^0 + \ldots + c_n z_n^0 = u(0) \\ c_1 z_1^1 + c_2 z_2^1 + \ldots + c_n z_n^1 = u(1) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_1 z_1^{n-1} + \ldots\ldots + c_n z_n^{n-1} = u(n-1) \end{array} \right. \quad (25)$$

It must be outlined that (24) is valid in all cases of fields (infinite or finite), used for generating of the LRS.

On the base of (24) and (25) the following proposition will be proven.

Proposition: Let the LRS is defined over arbitrary finite algebraic field GF(q), $q = p^l$, p prime and l is an arbitrary positive integer. Besides, let the characteristic polynomial (23) of the LRS is irreducible and primitive over GF(q). Then the LRS will produce the elements of the extended field GF(q^n) in an exponential order if the initial elements of the LRS are chosen to be:

$$u(0) = (0,\ldots,0,1); \\ u(1) = (0,\ldots,1,0); \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ u(n-1) = (1,\ldots,0,0). \quad (26)$$

Proof: As the polynomial (23) is irreducible over GF(q), it has n distinct roots

$$\alpha^{q^0} = \alpha, \alpha^{q^1}, \ldots, \alpha^{q^{n-1}} \quad (27)$$

in the extended field GF(q^n), formed by the joining of any root (27) to the field GF(q) [6], [10]. Without loss of generality it can be supposed that the root, joined to GF(q), is exactly α and that

$$z_1 = \alpha, z_2 = \alpha^{q^1}, \ldots, z_n = \alpha^{q^{n-1}}. \quad (28)$$

In this situation the initial elements of the LRS can be viewed as the following elements (vectors) of GF(q^n):

$$u(0) = (0,\ldots,0,1) = \alpha^0 = 1; \\ u(1) = (0,\ldots,1,0) = \alpha^1; \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ u(n-1) = (1,\ldots,0,0) = \alpha^{n-1}. \quad (29)$$

After plugging (28) and (29) in (25) we see that

$$c_1 = 1, c_2 = c_3 = \ldots = c_n = 0. \quad (30)$$

Consequently (24) reduces to

$$u(i) = z_1^i = \alpha^i,\ i = n, n+1, \ldots. \quad (31)$$

The equations (29) and (31) prove the proposition.

With regard to all the above stated, the following algorithm for synthesis of PM signals with HSC can be suggested.

First, some appropriate non-linear polynomial function (7) is chosen for generating of the power sequence of the uniform PM signal. Here it should be taken into account that the level of the structural complexity of the uniform PM signals directly depends on the non-linearity of the polynomial functions (7), defined by its algebraic degree (deg f) [1]-[12]:

$$\deg f = \max_i (c_{n-1,i} + c_{n-2,i} + \\ + \ldots + c_{1,i} + c_{0,i}) \quad (32)$$

Second, the listing of the argument of the polynomial function (7) is obtained by means of a LRS with characteristic polynomial, which is irreducible and primitive over GF(p). In this case the LRS is easily generated step-by-step by a computer with matrix processors.

For example, by the above algorithm uniform PM signals, based on the so-named *bent* or *maximal non-linear functions*, which have a very high resistance to the crypto-attacks [2]-[7], [11], can be easily generated.

4. Conclusion

In the paper a general algorithm for synthesis of uniform PM signals with HSC is suggested. Its positive features are:

1) high effectiveness from the point of view of the realization of the computing process;

2) ability for synthesis of uniform PM signals with HSC for infinity and dense sets of signal lengths and types of phase manipulation.

The proposed algorithm 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.

References:

[1] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732-736, Nov. 1976.

[2] J. D. Olsen, R. A. Scholtz and L. R. Welch, "Bent-function sequences," *IEEE Trans. Infirm. Theory*, vol. IT-28, pp. 858-864, Nov. 1982.

[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] 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.

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

[7] F. Chen, J. Hua, C. Zhau and S. Shou, "Fast generation of bent sequence family," *Inform. Technology J.*, 9, 2010, pp. 1397 – 1402

[8] L. Tong, J. Hua, L. Meng and S. Shou, "Correlation analysis and realization of Gordon-Mills-Welch sequences in advanced system," *Inform. Technology J.*, 10, 2011, pp. 908 – 913

[9] S. S. Yudachev, "Sequences on the base of bent-functions for wide-band systems with code-division of channels", *Engineers' gazette*, №1, Jan. 2013, pp. 1 – 11 (in Russian)

[10] R. Lidl and H. Niederreiter, *Finite Fields, vol. 20, Encyclopedia of Mathematics and its Applications.* Amsterdam: Addison-Wesley, 1983.

[11] O. S. Rothaus, "On 'bent' functions," *J. Comb. Theory*, Series A20, pp. 300-305, 1976.

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