VOL. 11, NO. 10, MAY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ABOUT A FAMILY OF ALMOST FOUR-PHASED SEQUENCES WITH PERFECT PERIODIC AUTOCORRELATION FUNCTION

M. V. Zaleshin and V. E. Gantmakher
Yaroslav-the-Wise Novgorod State University, Velikiy Novgorod, Russian Federation
E-Mail: mikhailzaleshin@gmail.com

ABSTRACT

A new family of almost four-phased sequences with perfect periodic autocorrelation function is proposed. It extends the array of the known almost four-phased sequences both for the periods' grid and for the structure via a slight increase of the peak-factor, the value of which is not greater than two. The generation algorithm for the sequences of this family is developed and can be easily implemented on any standard configuration computer.

Keywords: almost four-phased sequence, perfect periodic autocorrelation function, synthesis, generation.

INTRODUCTION

Today the operational principle of the greatest part of information technology complexes is based on the periodic sequences (hereafter the sequences) with specific sets of numerical characteristics. Among these characteristics, very important are the following [1]: periodic autocorrelation functions (PACF), alphabet, period, weight (the number of non-zero symbols on the period), and peak-factor (a ratio of the period to the weight of a sequence).

The sequences with perfect PACF are in great demand [2]. PACF is usually called perfect if the values of its sidelobes are constant and equal to zero [3]. However, the condition for the PACF to be perfect brings some severe constraints for the problem of the synthesis of sequences which satisfy this condition. For example, only one binary sequence with perfect PACF is known and it is supposed that no other one exists [4].

The first solution for the problem of the synthesis of the sequences with perfect PACF is the usage of the multiphase alphabets. The following papers are ones of the most known in this direction: [5]-[7]. A considerable limitation of these families of the sequences is the linear dependence of the quantity of the phases on the periods of the synthesized sequences. Also there exists the paper [8], where the generalized method for the synthesis of the sequences with perfect PACF is proposed. The main drawback of this case is the limited number of the multiphase sequences with perfect PACF.

The most popular method to eliminate the mentioned drawback is the switching from the multiphase sequences to the almost multiphase ones. The examples of such sequences are:

- almost four-phased Lee sequences with one zero symbol [9];
- almost eight-phased Lüke sequences with two zero symbols [10];
- almost multiphase Krengel sequences [11][12];
- ternary Ipatov sequences [13];
- besides, several families of the almost multiphase sequences are synthesized by the authors [14]-[15].

However, the known families cannot satisfy the continually growing demand on the sequences with such characteristics. Thus, the aim of this paper is the synthesis of a new family of the sequences with perfect PACF over the almost four-phased alphabet.

PRELIMINARIES

Let $GF(q^m)$ be the extended Galois field with a characteristic $q = p^x$ where p - a prime number, and s – an arbitrary natural number. Now over $GF(q^m)$ we define q-adic M-sequence denoted by $\{d_n\}$. Its period equals $q^m - 1$ that coincides with the number of non-zero elements of the field.

If θ – is a primitive element of the fields $GF(q)$ then for each devisor $b|(q - 1)$ there exists the set of residue classes H_r, which consist of $(q - 1)/b$ elements and are defined as follows:

$$H_r = \left\{ \theta^{r+jb} \mid j = 0,1,\ldots,\frac{q-1}{b}-1 \right\},$$

where $r = 0,1,\ldots,b-1$.

Let us associate some symbol of the ternary alphabet with each r-th class H_r according to the following coding rule:

$$y_n = i^n \begin{cases} 1, & d_n \in \bigcup\limits_{0,8,9,12} H_r; \\ -1, & d_n \in \bigcup\limits_{1,2,5,7} H_r; \\ 0, & \text{else.} \end{cases} \quad (1)$$

The sequence $\{y_n\}$. defined in Equation. (1), is generated in such way that its n-th position value is i^n, if the corresponding n-th symbol of the M-sequence d_n is owned by classes H_0, H_8, H_9, *or* H_{12}; - i^n, if d_n is owned by H_1, H_2, H_5, *or* H_7 else y_n equals zero.

Now we find necessary and sufficient conditions for the parameters of the extended Galois field $GF(q^m)$ for

which the generated almost four-phased sequences $\{y_n\}$ have perfect PACF if the following condition is met:

NECESSARY AND SUFFICIENT CONDITIONS OF EXISTENCE

Based on the results, provided by the paper [16] of the authors, the sequence $\{y_n\}$ has perfect PACF if the following condition is met:

$$7h \equiv 2 \pmod 4, \tag{2}$$

where $h = \frac{q^m - 1}{q - 1}$.

Let us use the Equation. (2) to find the necessary condition of existence for the sequences which are generated by Equation. (1).

THEOREM 1

In order for the almost four-phased sequence $\{y_n\}$ to have perfect PACF, it is necessary that the extension m of the Galois field is congruent: $m \equiv 2 \pmod 4$.

PROOF

For the characteristic of the field q the following condition must be satisfied: $q - 1 \equiv 0 \pmod{14}$. That is q can be represented as follows: $q=14c+1$ where c – such a natural number that q is the prime power. As a result:

$$7h = 7\frac{q^m - 1}{q - 1} = \frac{(14c+1)^m - 1}{2c} = \\ = 7m + \sum_{k=2}^{m} \binom{k}{m} (2c)^{k-1} 7^k \equiv 2 \pmod 4. \tag{3}$$

The necessary condition for Equation. (3) to be hold is the solubility of the following congruence for the extension: $m \equiv 2 \pmod 4$. That completes the proof.

For convenience, let us assume the value of the extension: $m \equiv 2$. Hence, we obtain the corresponding value of $h = q+1 = 14c+2$ where c -a natural number. Now we find the sufficient condition of existence for the almost four-phased sequences with perfect PACF over $GF(q^2)$.

THEOREM 2

In order for PACF of $\{y_n\}$ $\{y_n\}$ over $GF(q^2)$ to be perfect, it is sufficient that the value of c in equation $h = 14c+2$ is an even integer.

PROOF

It follows from Equation. (3) that:

$$7h = 2 \cdot 7(7c+1) \equiv 2 \pmod 4.$$

If d – an odd number, then the equation in the brackets $(7c+1)$ is even, and the left part of the congruence $2.7(7c+1)$ becomes a multiple of four, that is:

$$2 \cdot 7(7c+1) \equiv 0 \pmod 4,$$

that contradicts the necessary condition of existence. Thus, the solubility of the presented congruence requires the equation $(7c+1)$ to have odd value, that is c must be an even number. This completes the proof.

PROPERTIES OF THE FAMILIY'S SEQUENCES

Now we enumerate the basic properties of the obtained almost four-phased sequences with perfect periodic autocorrelation function.

PROPERTY 1

The period of sequence $\{y_n\}$ equals $7(q+1)$.

PROPERTY 2

The weight of sequence $\{y_n\}$ equals $4q$.

PROPERTY 3

The peak-factor pf of sequence $\{y_n\}$ approaches 1.75 with the growth of the period.

Considering these properties, we obtained Table-1 where the values of some parameters that satisfy the necessary and sufficient conditions of existence are presented.

The proposed family of the sequences considerably expands the periods' grid of Lee-sequences. But even for those cases, where the periods are the same, the sequences of the proposed family have different structure.

THE GENERATION ALGORITHM

Thus, the generation algorithm of the obtained almost four-phased sequences with perfect PACF over the extended Galois fields $GF(q^2)$ is determined by the following sequence of operations:

1. Choose such a natural number c that $q = 14c+1$ can be represented as $q=p^s$ where p – a prime number and s – a natural number;
2. Find the first $4q$ symbols of the M-sequence over $GF(q^2)$
3. Construct 14 residue classes over $GF(q)$
4. Generate the desired sequence $\{y^n\}$ via the coding rule (1).

Let us demonstrate how the algorithm operates with the following example.

EXAMPLE

We generate the first almost four-phased sequence with perfect PACF from Table-1:

Table-1. The examples of the parameters of the synthesized sequences with perfect PACF.

№	*p*	*s*	*m*	Period	*pf~*
	29	**1**	**2**	**210**	**1.81**
	113	1	2	798	1.77
	13	2	2	1190	1.76
	197	1	2	1386	1.76
	281	1	2	1974	1.76
	337	1	2	2366	1.76
	421	1	2	2954	1.75
	449	1	2	3150	1.75
	617	1	2	4326	1.75
	673	1	2	4718	1.75
	701	1	2	4914	1.75
	3	6	2	5110	1.75
	757	1	2	5306	1.75
	29	2	2	5894	1.75
	953	1	2	6678	1.75
	1009	1	2	7070	1.75
	1093	1	2	7658	1.75
	1289	1	2	9030	1.75
	1373	1	2	9618	1.75
	1429	1	2	10010	1.75
	1597	1	2	11186	1.75
	41	2	2	11774	1.75
	1709	1	2	11970	1.75
	43	2	2	12950	1.75
	1877	1	2	13146	1.75
	1933	1	2	13538	1.75
	2017	1	2	14126	1.75
	2129	1	2	14910	1.75
	2213	1	2	15498	1.75
	2269	1	2	15890	1.75
	2297	1	2	16086	1.75
	2381	1	2	16674	1.75
	2437	1	2	17066	1.75
	2521	1	2	17654	1.75
	2549	1	2	17850	1.75
	2633	1	2	18438	1.75
	2689	1	2	18830	1.75
	2801	1	2	19614	1.75
	2857	1	2	20006	1.75
	2969	1	2	20790	1.75
	3109	1	2	21770	1.75
	3137	1	2	21966	1.75
	3221	1	2	22554	1.75
	3361	1	2	23534	1.75
	3389	1	2	23730	1.75
	3529	1	2	24710	1.75
	3557	1	2	24906	1.75
	3613	1	2	25298	1.75
	3697	1	2	25886	1.75
	4201	1	2	29414	1.75

1. We choose for which

2. We find the first 210 symbols of the M-sequence over

2, 16, 17, 13, 18, 25, 18, 12, 13, 21, 15, 7, 16, 14, 23, 0, 21, 17, 10, 28, 7, 14, 11, 11, 7, 1, 6, 20, 9, 16, 7, 27, 16, 2, 5, 15, 5, 13, 2, 1, 9, 10, 27, 20, 8, 0, 1, 16, 6, 11, 10, 20, 24, 24, 10, 18, 21, 12, 17, 27, 10, 22, 27, 7, 3, 9, 3, 2, 7,

18, 17, 6, 22, 12, 28, 0, 18, 27, 21, 24, 6, 12, 26, 26, 6, 5, 1, 13, 16, 22, 6, 19, 22, 10, 25, 17, 25, 7, 10, 5, 16, 21, 19, 13, 11, 0, 5, 22, 1, 26, 21, 13, 4, 4, 21, 3, 18, 2, 27, 19, 21, 23, 19, 6, 15, 16, 15, 10, 6, 3, 27, 1, 23, 2, 24, 0, 3, 19, 18, 4, 1, 2, 14, 14, 1, 25, 5, 7, 22, 23, 1, 8, 23, 21, 9, 27, 9, 6, 21, 25, 22, 18, 8, 7, 26, 0, 25, 23, 5, 14, 18, 7, 20, 20, 18, 15, 3, 10, 19, 8, 18, 28, 8, 1, 17, 22, 17, 21, 1, 15, 19, 5, 28, 10, 4, 0, 15, 8, 3, 20, 5, 10, 12, 12, 5, 9, 25, 6, 23, 28;
3. We construct 14 residue classes over

4. We generate the desired sequence:
+, i, +, -i, –, 0, +, i, +, 0, +, 0, +, -i, –, 0, 0, -i, 0, -i, 0, -i, +, i, 0, i, –, 0, 0, i, 0, -i, +, i, +, i, –, i, –, -i, 0, 0, –, 0, 0, 0, –, -i, +, -i, 0, 0, –, -i, 0, i, 0, -i, +, -i, 0, 0, –, 0, 0, 0, 0, -i, 0, -i, +, -i, 0, -i, –, 0, –, i, 0, i, +, -i, 0, 0, +, -i, –, -i, +, 0, –, 0, 0, 0, 0, i, 0, 0, 0, i, +, 0, 0, -i, –, 0, +, 0, +, 0, 0, -i, 0, 0, 0, 0, –, i, –, 0, 0, i, 0, -i, –, i, +, 0, +, 0, –, -i, +, i, +, 0, 0, 0, +, 0, +, i, +, i, +, 0, +, 0, 0, i, –, 0, +, 0, 0, -i, 0, i, 0, 0, 0, -i, 0, 0, 0, 0, 0, -i, –, -i, +, 0, 0, 0, +, i, 0, 0, 0, 0, –, i, 0, -i, –, 0, +, 0, +, -i, 0, i, +, 0, 0, 0, –, 0, 0, 0, –, 0, +, i, –, 0, 0, -i, +, i.

The one generated in the example is almost a four-phased sequence with perfect PACF has the period 210, its weight equals 116, and peak-factor is approximately equal to 1.81.

CONCLUSIONS

In this paper we proposed a new family of almost four-phased sequences with perfect periodic autocorrelation function. The distinctive features of this family are:

1. The grid of the periods which extends the array of the known almost four-phased sequences with perfect PACF;
2. The structure which allows to increase the number of isomorphic almost four-phased sequences with perfect PACF for the known periods due to a slight growth of the peak-factor's value;
3. The generation algorithm which can be easily implemented on any standard configuration computer.

The results presented in the paper are verified by the great amount of the examples by means of computer-aided simulation with the help of the specially developed software complex. One of these examples is included in the paper.

ACKNOWLEDGEMENTS

The paper is prepared with financial support of the Ministry of Education and Science of the Russian Federation within the basic part of the government assignment.

REFERENCES

[1] P. Fan, M. Darnell. 1996. Sequence design for communications applications. Research Studies Pre. 516.

[2] S. W. Golomb, G. Gong. 2005. Signal Design for Good Correlation: for Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge. 438.

[3] D. Jungnickel, A. Pott. 1999. Perfect and almost perfect sequences. Discrete Applied Mathematics, 95(1-3): 331-359.

[4] R. J. Turyn. 1965. Character sums and difference sets. Pacific J. Math. 15: 319-346.

[5] D. C. Chu. 1972. Polyphase codes with good periodic correlation properties. IEEE Trans. Inf. Theory. 18: 531-533.

[6] R. L. Frank. 1963. Phase coded communication system, U.S. Patent 3,099,795.

[7] A. Milewski. 1983. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. IBM J. Res. Dev. 27(5): 425-431.

[8] W. H. Mow. 1996. A New Unified Construction of Perfect Root-of-Unity Sequences, Proc. Int. Symp. Spread Spectrum Techniques and its Applications, Mainz, Germany. pp. 955-959.

[9] C. E. Lee. 1992. Perfect q-ary sequences from multiplicative characters over GF (p), Electron. Lett., 3628(9): 833–835.

[10] H. D. Lüke, H. D. Schotten and H. Hadinejad-Mahram. 2003. Binary and quadriphase sequences with optimal autocorrelation properties: a survey. IEEE Trans. Inf. Theory. 49(12): 3271–3282.

[11] E. I. Krengel. 2009. A method of Construction of perfect sequences. Radiotekhnika. 11: 15–21.

[12] E. I. Krengel. 2010. Some Constructions of Almost-Perfect, Odd-Perfect and Perfect Polyphase and Almost-Polyphase Sequences. SETA, Paris, France, LNCS. 6338: 387–398.

[13] V. P. Ipatov. 1992. Periodic discrete signals with optimal correlation properties. Radio i svyaz, Moscow. 152.

[14] V. E. Gantmakher and M. V. Zaleshin. 2014. Six-phase sequences with perfect periodic autocorrelation function. SETA, Melbourne, Australia, LNCS. 8865: 97-103.

[15] V. E. Gantmakher and M. V. Zaleshin. 2015. Almost multiphase sequences based on Chu sequences. Electron. Lett. 51(2): 145-147.

[16] M. V. Zaleshin and V. E. Gantmakher. 2014. Generalized algorithm for the synthesis of the sequences with perfect periodic autocorrelation function over the extended Galois fields. DSPA, Moscow, Russian Federation. pp. 53-56.