Construction Method for Infinite Families of Bent-Sequences

A.V. Sokolov, I.V. Tsevukh
Department of Radioelectronic and Telecommunication Systems,
Odessa National Polytechnic University, Ukraine.
radiosquid@gmail.com

Abstract— Bent-sequences is one of the most important classes of Boolean functions, which are widely used in modern cryptographic algorithms, and telecommunication systems that are based on CDMA and OFDM standards. The problem of synthesis of bent-sequences of large lengths is actual and widely discussed. However, in view of the high complexity and unpredictability of the class of bent-sequences, the creation of methods for their synthesis faces significant difficulties. In this paper, a recursive method for constructing infinite families of bent-sequences, based on easily synthesized bent-sequences of small length, has been developed. As the basis of this method, the operations of interleaving of elements and strings, which are widely used in the theory of synthesis of perfect binary arrays, are applied. Effective reproduction rules for bent-sequences in the time domain based on the operation of rearrangement of segments, a rotor, and dimensional changes are proposed. The method developed allows rapid acquisition of a lot of bent-sequences of any predefined length. Moreover, the obtained bent-sequences belong to different classes according to Agievich classification, which is important from the cryptographic point of view.

***Index Terms* — bent-sequence, Maiorana-McFarland construction, recursive method.**

I. Introduction

One of the most important classes of Boolean functions, which are widely used in cryptography, coding theory, extended-range communication systems, and other fields of science and technology are bent-sequences. This class, discovered in the 1960s by O. Rothaus [1], is still an object of close attention of many researchers working in the branch of communication theory and mathematics. Being maximally non-linear, bent-sequences allows to resist most effectively the attacks of linear cryptanalysis – approximation by affine functions. Bent-sequences also have a uniform distribution of the absolute values of the Walsh-Hadamard spectrum [2], which makes them indispensable in the tasks of rational use of transmitter power in digital information transmission systems. For this reason, bent-sequences are successfully applied in such modern standards of digital communication such as CDMA (Code Division Multiple Access) and OFDM (Orthogonal Frequency-Division Multiplexing), and also common cryptographic algorithms such as CAST-256 (block symmetric cipher), HAVAL (hashing algorithm), Grain (stream cipher), and many others.

Of course, such a wide use of bent-sequences in modern information transmission systems makes actual the problem of synthesis of complete classes of these signals for arbitrary length $N = 2^k$, where k is even. However, in view of the peculiarities of the class of bent-sequences, whose structure is very unpredictable, this problem, in the general case, has not yet been solved. Moreover, currently, in the literature, there are not even asymptotic estimates of the bent-sequences class cardinality for values $k > 8$. Existing estimates of the cardinalities of bent-functions classes are mainly based on the well-known Maiorana-McFarland construction [3], which uses the recursive algorithm for constructing Hadamard matrices for the construction of bent-sequences. Anyhow, it turns out that the Maiorana-McFarland construction allows acquisition of only a very small part of the bent-sequences in comparison with their full class, which certainly significantly hampers the full use of their beneficial properties in modern information technology.

The purpose of this article is to develop a new effective method for constructing infinite families of bent-sequences based on existing small-length bent-sequences that can be easily found in accordance with known regular methods [4,5].

II. Maiorana-McFarland and Dvornikov Constructions

In accordance with the definition [4], the binary sequence $\mathbf{B} = [b_0, b_1, \ldots, b_i, \ldots, b_{N-1}]$, where $b_i \in \{\pm 1\}$ are coefficients, of even length $N = 2^k$, $k = 2, 4, 6...$ is called a bent-sequence if it has a uniform absolute value of Walsh-Hadamard spectrum, which is representable in matrix form

$$\mathbf{W}_{\mathbf{B}}(\omega) = \mathbf{BA}, \quad \omega = 0, 1, ..., 2^{k-1}, \tag{1}$$

where $\mathbf{A}$ is the Walsh-Hadamard matrix of order N. We note, that bent-sequence is considered as a truth table of corresponding bent-function.

Based on the definition of the bent-function, each spectral coefficient of the sequence $\mathbf{W}_{\mathbf{B}}(\omega = 0), \mathbf{W}_{\mathbf{B}}(\omega = 1), ..., \mathbf{W}_{\mathbf{B}}(\omega = N-1)$ takes values from the set $\left\{\pm\sqrt{N}\right\}$.

The most effective of the known methods of recursive construction of bent-sequences of length N is the Maiorana-McFarland construction [3], which is based on the concatenation of rows of the Hadamard matrix $\mathbf{A}$ of order $L = \sqrt{N}$, as well as all possible $L!$ permutations of its rows and 2^L of their sign encodings. Then, in turn, the Hadamard matrix of each successive order is constructed in accordance with the well-known recurrence rule [6]

$$\mathbf{A}_{2^k} = \begin{bmatrix} \mathbf{A}_{2^{k-1}} & \mathbf{A}_{2^{k-1}} \\ \mathbf{A}_{2^{k-1}} & -\mathbf{A}_{2^{k-1}} \end{bmatrix}, \qquad (2)$$

where $\mathbf{A}_1 = 1$.

For example, in accordance with (2) we construct the Hadamard matrix $\mathbf{A}_8$ (where, for brevity, $+1$ are designated as "$+$", and -1 as "$-$")

$$\mathbf{A}_8 = \begin{bmatrix} +\,+\,+\,+\,+\,+\,+\,+ \\ +\,-\,+\,-\,+\,-\,+\,- \\ +\,+\,-\,-\,+\,+\,-\,- \\ +\,-\,-\,+\,+\,-\,-\,+ \\ +\,+\,+\,+\,-\,-\,-\,- \\ +\,-\,+\,-\,-\,+\,-\,+ \\ +\,+\,-\,-\,-\,-\,+\,+ \\ +\,-\,-\,+\,-\,+\,+\,- \end{bmatrix}, \qquad (3)$$

and applying sequential concatenation of its rows, we obtain a bent-sequence of length $N = 64$ and, in accordance with (1), its Walsh-Hadamard spectrum

$$\begin{aligned} \mathbf{B} = [&+ + + + + + + + + - + - + - + - + + - - + + - - \\ &+ - - + + - - + + + + + - - - - + - + - - + - + \\ &+ + - - - - + + + - - + - + + -]; \\ \mathbf{W_B}(\omega) = [&8\;\; 8\;\; 8\;\; 8\;\; 8\;\; 8\;\; 8\;\; 8\;\; 8\; -8\;\; 8\; -8\;\; 8\; -8\;\; 8\; -8 \\ &8\;\; 8\; -8\; -8\;\; 8\;\; 8\; -8\; -8\;\; 8\; -8\; -8\;\; 8\;\; 8\; -8\; -8\;\; 8 \\ &8\;\; 8\;\; 8\;\; 8\; -8\; -8\; -8\; -8\;\; 8\; -8\;\; 8\; -8\; -8\;\; 8\; -8\;\; 8 \\ &8\;\; 8\; -8\; -8\; -8\; -8\;\; 8\;\; 8\;\; 8\; -8\; -8\;\; 8\; -8\;\; 8\;\; 8\; -8], \end{aligned} \qquad (4)$$

which shows that sequence (4) does satisfy the definition of a bent-sequence.

It was shown in [7] that the full class $\mathbf{M}$ of Maiorana-McFarland bent-functions can be written in matrix form as

$$\mathbf{M} = \mathbf{B} \cdot (\mathbf{I} \otimes \mathbf{PC}), \qquad (5)$$

where $\otimes$ is the symbol of Kronecker's product, $\mathbf{B}$ is some initial bent-sequence, for example (4); $\mathbf{I}$ is the identity matrix of order k; $\mathbf{P}$ is the matrix of permutations of order k, the total number of which is $L!$; $\mathbf{C}$ is matrix of sign encodings of order k, the total number of which is 2^L.

Thus, the cardinality of the Maiorana-McFarland class is defined as $J = L! \cdot 2^L$. In [7] it was proposed by Dvornikov to extend the Maiorana-McFarland class by using a new construction

$$\mathbf{M}' = \mathbf{B} \cdot (\mathbf{PC} \otimes \mathbf{I}). \qquad (6)$$

Due to the noncommutativity of the Kronecker product, it is possible to obtain new bent-sequences, some of which however coincides with the original Maiorana-McFarland class (5).

For example, we choose matrices and the original bent-function

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad \mathbf{C} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad \mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \qquad (7)$$

$$\mathbf{B} = [+ \; + \; + \; + \; + \; - \; + \; - \; + \; + \; - \; - \; + \; - \; - \; +],$$

for which, in accordance with (5) and (6), we obtain respectively new bent-sequences

$$\begin{aligned} \mathbf{M} &= [- \; + \; + \; + \; - \; + \; - \; - \; - \; - \; + \; - \; - \; - \; - \; +]; \\ \mathbf{M}' &= [- \; - \; - \; - \; + \; + \; - \; - \; + \; - \; + \; - \; + \; - \; - \; +], \end{aligned} \qquad (8)$$

which, as we see, are different in structure.

The number of bent-sequences from Maiorana-McFarland and Dvornikov classes, constructed with the help of (5) and (6) is defined as [7]

$$J_k = \left(2^{k/2}\right)! \cdot 2^{2^{k/2}+1} - 2^{k+1} \prod_{r=0}^{\frac{k}{2}-1} \left(2^{k/2} - 2^r\right), \qquad (9)$$

that determines a lower bound estimate of the number of bent-sequences for an arbitrary even number k.

III. The New Method for Recurrent Construction of Bent-Sequences

In this paper, we propose a fundamentally new method for bent-sequences construction based on the use of a full class of bent-sequences of smaller length and two recurrent constructions, which we describe in the following steps, illustrated by an example for a short length of source sequences $N = 16$ and generated sequences of length $N' = 64$.

Step 1. Choose two arbitrary bent-sequences $\mathbf{B}_1$ and $\mathbf{B}_2$ of length N.

For example, let the chosen bent-sequences to be

$$\begin{cases} \mathbf{B}_1 = \{+ - - + - + - + - - + + + + + +\}; \\ \mathbf{B}_2 = \{- + - + + - - + - - + + + + + +\}. \end{cases} \qquad (10)$$

Step 2. We get 2 new bent-sequences of length $N' = 64$ in accordance with the rule of horizontal concatenation

$$\begin{aligned} \mathbf{B}'_1 &= [\mathbf{B}_1 \,|\, \mathbf{B}_2 \,|\, -\mathbf{B}_1 \,|\, \mathbf{B}_2]; \\ \mathbf{B}'_2 &= [\mathbf{B}_1 \,|\, \mathbf{B}_2 \,|\, \mathbf{B}_1 \,|\, -\mathbf{B}_2], \end{aligned} \qquad (11)$$

where "$|$" is the horizontal concatenation symbol. For our example, we get the following bent-sequences

$$\begin{aligned} \mathbf{B}'_1 = \{&+ - - + - + - + - - + + + + + + \\ &- + - + + - - + - - + + + + + + \\ &- + + - + - + - + + - - - - - - \\ &- + - + + - - + - - + + + + + +\}; \\ \mathbf{B}'_2 = \{&+ - - + - + - + - - + + + + + + \\ &- + - + + - - + - - + + + + + + \\ &+ - - + - + - + - - + + + + + + \\ &+ - + - - + + - + + - - - - - -\}. \end{aligned} \qquad (12)$$

Step 3. Represent a respective original bent-sequences (10) in the form of corresponding matrices

$$\boldsymbol{\beta}_1 = \begin{bmatrix} + & - & - & + \\ - & + & - & + \\ - & - & + & + \\ + & + & + & + \end{bmatrix}, \quad \boldsymbol{\beta}_2 = \begin{bmatrix} - & + & - & + \\ + & - & - & + \\ - & - & + & + \\ + & + & + & + \end{bmatrix}. \qquad (13)$$

Step 4. To increase the length of the rows of matrices $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$ we apply the matrix element interleaving operation, introduced in [6, 8] for the recursive construction of perfect binary arrays. Schematically, the operation of interleaving the first two rows of the matrix $\boldsymbol{\beta}_1$ can be represented as the following algebraic construction

$$\left\{\begin{array}{cccccccc} + & & - & & - & & + & \\ & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ & - & & + & & - & & + \end{array}\right\} \Rightarrow \\ \Rightarrow \{+ \; - \; - \; + \; - \; - \; + \; +\}. \tag{14}$$

Similarly, by interleaving each two neighboring rows of matrices $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2$ we construct auxiliary matrices $\mathbf{Z}_1$, $\mathbf{Z}_2$ of the size $\sqrt{N}/2 \times 2\sqrt{N}$

$$\begin{cases} \mathbf{Z}_1 = \begin{bmatrix} + & - & - & + & - & - & + & + \\ - & + & - & + & + & + & + & + \end{bmatrix}; \\ \mathbf{Z}_2 = \begin{bmatrix} - & + & + & - & - & - & + & + \\ - & + & - & + & + & + & + & + \end{bmatrix}, \end{cases} \tag{15}$$

Step 5. We build new bent-sequences in the form of matrices $\boldsymbol{\beta}_1'$ and $\boldsymbol{\beta}_2'$ of size $2\sqrt{N} \times 2\sqrt{N}$ by the rules

$$\boldsymbol{\beta}_1' = \begin{bmatrix} \begin{bmatrix} \mathbf{Z}_1 \\ \cup \\ \mathbf{Z}_2 \end{bmatrix} \\ cat \\ \begin{bmatrix} \mathbf{Z}_1 \\ \cup \\ -\mathbf{Z}_2 \end{bmatrix} \end{bmatrix}, \boldsymbol{\beta}_2' = \begin{bmatrix} \begin{bmatrix} \mathbf{Z}_1 \\ \cup \\ \mathbf{Z}_2 \end{bmatrix} \\ cat \\ \begin{bmatrix} -\mathbf{Z}_1 \\ \cup \\ \mathbf{Z}_2 \end{bmatrix} \end{bmatrix}, \tag{16}$$

where the operator $\cup$ means the interleaving of lines — a consecutive line spacing of the rows of the lower matrix between the rows of the upper matrix;

cat is the operation of vertical concatenation (union) of two submatrices.

For our example, we obtain matrices $\boldsymbol{\beta}_1'$ and $\boldsymbol{\beta}_2'$, of size 8×8 corresponding to bents-sequences of length $N' = \left(2\sqrt{N}\right)^2 = 4N = 64$

$$\boldsymbol{\beta}_1' = \begin{bmatrix} + & - & - & + & - & - & + & + \\ - & + & + & - & - & - & + & + \\ - & + & - & + & + & + & + & + \\ - & + & - & + & + & + & + & + \\ + & - & - & + & - & - & + & + \\ + & - & - & + & + & + & - & - \\ - & + & - & + & + & + & + & + \\ + & - & + & - & - & - & - & - \end{bmatrix}, \\ \boldsymbol{\beta}_2' = \begin{bmatrix} + & - & - & + & - & - & + & + \\ - & + & + & - & - & - & + & + \\ - & + & - & + & + & + & + & + \\ - & + & - & + & + & + & + & + \\ - & + & + & - & + & + & - & - \\ - & + & + & - & - & - & + & + \\ + & - & + & - & - & - & - & - \\ - & + & - & + & + & + & + & + \end{bmatrix}. \tag{17}$$

As the next step we increase the cardinality of obtained bent-sequences by using the following Rules:

Rule R1. We represent matrices $\boldsymbol{\beta}_1'$ and $\boldsymbol{\beta}_2'$ in the following form

$$\boldsymbol{\beta} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{18}$$

by simply dividing the original matrix of the size $\sqrt{N'} \times \sqrt{N'}$ into 4 parts of size $\sqrt{N'}/2 \times \sqrt{N'}/2$, as, for example, is shown for the matrix $\boldsymbol{\beta}_1'$

$$\boldsymbol{\beta}_1' = \begin{bmatrix} +--+--++ \\ -++---++ \\ -+-+++++ \\ -+-+++++ \\ +--+--++ \\ +--+++-- \\ -+-+++++ \\ +-+----- \end{bmatrix} = \begin{bmatrix} A = \begin{bmatrix} +--+ \\ -++- \\ -+-+ \\ -+-+ \end{bmatrix} B = \begin{bmatrix} --++ \\ --++ \\ ++++ \\ ++++ \end{bmatrix} \\ \\ C = \begin{bmatrix} +--+ \\ +--+ \\ -+-+ \\ +-+- \end{bmatrix} D = \begin{bmatrix} --++ \\ ++-- \\ ++++ \\ ---- \end{bmatrix} \end{bmatrix}. \tag{19}$$

Performing $4! = 24$ permutations of the blocks $A, B, C, D,$ we obtain from the original matrix $J_1 = 24$ new matrices corresponding to the bent-sequences.

Rule R2. The operation of the rotor to $90^{\circ}, 180^{\circ}, 270^{\circ}$ preserves the properties of the bent-sequence generating matrix and allows to obtain $J_2 = 4$ new bent-sequences on the basis of one initial matrix. For example, a matrix $\boldsymbol{\beta}_1'$ rotor leads to the appearance of the following new structures

$$\boldsymbol{\beta}_1' = \begin{bmatrix} + & - & - & + & - & - & + & + \\ - & + & + & - & - & - & + & + \\ - & + & - & + & + & + & + & + \\ - & + & - & + & + & + & + & + \\ + & - & - & + & - & - & + & + \\ + & - & - & + & + & + & - & - \\ - & + & - & + & + & + & + & + \\ + & - & + & - & - & - & - & - \end{bmatrix}, \\ rot_{90}(\boldsymbol{\beta}_1') = \begin{bmatrix} + & + & + & + & + & - & + & - \\ + & + & + & + & + & - & + & - \\ - & - & + & + & - & + & + & - \\ - & - & + & + & - & + & + & - \\ + & - & + & + & + & + & + & - \\ - & + & - & - & - & - & - & + \\ - & + & + & + & - & - & + & - \\ + & - & - & - & + & + & - & + \end{bmatrix}, \\ rot_{180}(\boldsymbol{\beta}_1') = \begin{bmatrix} - & - & - & - & - & + & - & + \\ + & + & + & + & + & - & + & - \\ - & - & + & + & + & - & - & + \\ + & + & - & - & + & - & - & + \\ + & + & + & + & + & - & + & - \\ + & + & + & + & + & - & + & - \\ + & + & - & - & - & + & + & - \\ + & + & - & - & + & - & - & + \end{bmatrix}, \\ rot_{270}(\boldsymbol{\beta}_1') = \begin{bmatrix} + & - & + & + & - & - & - & + \\ - & + & - & - & + & + & + & - \\ + & - & - & - & - & - & + & - \\ - & + & + & + & + & + & - & + \\ - & + & + & - & + & + & - & - \\ - & + & + & - & + & + & - & - \\ - & + & - & + & + & + & + & + \\ - & + & - & + & + & + & + & + \end{bmatrix}. \tag{20}$$

Rule R3. Representation of the original matrix in the form of rectangles of dimensions $L/_{2\lambda} \times 2\lambda L, \quad \lambda = 2^0, 2^1, ..., 2^{\log_2 k - 1}$ and selection of elements by columns. For example, for the size of the original matrix 8×8, these are rectangles 2×32 and 4×16, which for the matrix $\boldsymbol{\beta}_1'$ have the following form

$$\left(\boldsymbol{\beta}_1'\right)_{2\times32} = \Big[\begin{matrix} +--+-+-+--++--++ \\ -+-++--+++++++++ \end{matrix} \\ \begin{matrix} +--++-+---++++-- \\ -+-+-++-++++---- \end{matrix} \Big]; \\ \left(\boldsymbol{\beta}_1'\right)_{4\times16} = \begin{bmatrix} +----+-++-++-++- \\ --+-++++---+++-- \\ -+++-+-+-+---++- \\ ++-++++++++-++-- \end{bmatrix}. \tag{21}$$

Next, we again change the dimension of each of these rectangles into the bent-sequence, thus getting new bent-sequences, according to the number of rectangles

$$\begin{aligned}\mathbf{B}_{2\times 32} = [&+--+-+-+--++--++\\ &+--++-+---++++--\\ &-+-++--+++++++++\\ &-+-+-++-++++----]\\ \mathbf{B}_{4\times 16} = [&+----+-++-++-++-\\ &--+-++++---+++--\\ &-+++-+-+-+---++-\\ &++-++++++++-++--]\end{aligned} \quad (22)$$

This rule for matrices size 8×8 makes it possible to obtain $J_3 = 3$ structures from the original matrix, whereas for the matrices size 16×16, it is possible to obtain 4 new structures.

Let us give in Fig. 1 the schematic representation of the method presented above for constructing infinite families of bent-sequences

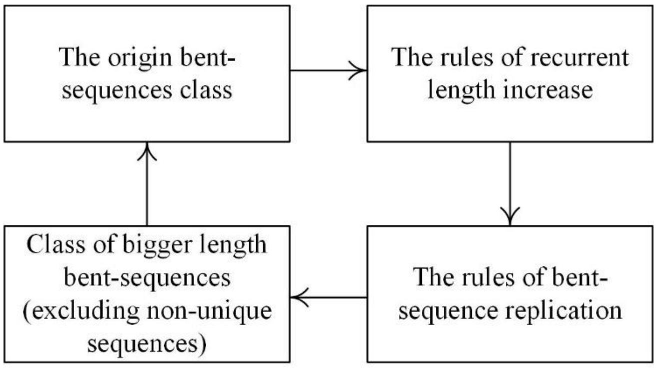
The origin bent-sequences class
The rules of recurrent length increase
The rules of bent-sequence replication
Class of bigger length bent-sequences (excluding non-unique sequences)

Figure 1: Bent-sequences infinite families construction method

Thus, let us to calculate the number of bent-sequences of length $N' = 64$ that can be recursively constructed using the proposed method from regularly obtained bent-sequences of length $N = 16$. While it is 896 bent-sequence of length $N = 16$, by using recurrent constructions proposed in Section III we can obtain $J'_{64} = 2\cdot 2\cdot (J_{16})^2 = 3\,211\,264$ new bent-sequences of length $N' = 64$. And then using reproduction *Rules R1…R3* we obtain the total number of bent-sequences of length $N' = 64$

$$\begin{aligned} J_{64} = J'_{64}\cdot J_1\cdot J_2\cdot J_3 = 3211264\cdot 24\cdot 4\cdot 3 = \\ = 924\,844\,032, \end{aligned} \quad (23)$$

Nevertheless, computational experiments show that in this set there are repetitive sequences. The total number of unique bent-sequences of length $N = 64$ obtained is $J_{64\,unique} = 54\,065\,920$, that exceeds the number of bent-sequences of length $N' = 64$ in the Maiorana-McFarland class by 5,238 times, as well as exceeding the number of bent-sequences obtained with the help of Maiorana-McFarland and Dvornikov constructions by 2.6217 times. Moreover, these bent-sequences belong to different inequivalent classes of bent-squares according to the Agievich classification [9], which is important in cryptographic applications. We also note, that obtaining different inequivalent classes of bent-squares according to the Agievich classification may be useful for construction of constant amplitude error-correcting codes by the algorithm, proposed in [10].

IV. Conclusion

In this paper, we propose two constructions for building bent-sequences of length $4N$ on the basis of bent-sequences of length N. Application of the developed constructions allows generation of 4 new bent-sequences of length $4N$ on the basis of two initial bent-sequences of length N.

Effective rules for the reproduction of bent-sequences based on the operation of permutation of blocks are proposed (this increases the power of the class by $\sqrt{N}/2$ times), on the basis of the operator $rot()$ (this increases the power of the class by 4 times) and on the basis of a change in the dimension (this increases the power of the class by up to 3 times).

The joint application of the length-extension constructions and the bent-sequence reproduction rules made it possible to form a method for recurrent synthesis of infinite families of bent-sequences by increasing their length and the cardinality of their class at each iteration of the method application.

The proposed method can be used to generate bent-sequences of large lengths for cryptographic and telecommunication applications.

Acknowledgment

This paper is dedicated to the memory of Prof. M.I. Mazurkov.

References

[1] O.S. Rothaus “On “bent” functions”, J. Comb. Theory Ser. A, USA, Academic Press Inc, 1976, No. 20(3), pp. 300–305.

[2] K.G. Peterson “Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory”, Sequences and their applications. Seta 2001. Second Int. Conference, Bergen, Norway, May 13–17, 2001, Proc. Berlin: Springer, 2002. pp. 46–71.

[3] N.N. Tokareva “Bent functions: results and applications. Review of papers [Original text in Russian]”, Applied. discrete. mathematics, Tomsk, 2009, Ser. No. 1 (3), pp. 15–37.

[4] M.I. Mazurkov, A.V. Sokolov “The regular rules of constructing the complete class of bent-sequences of length 16 [Original text in Russian]”, Odessa, Proceedings of ONPU, 2013, pp. 227–230.

[5] A.V. Sokolov “Synthesis method of a complete class of bent-functions of six variables [Original text in Russian]”, Problems of physics, mathematics and technics, No. 4 (29), pp. 94–102.

[6] M.I. Mazurkov “Broadband radio communication systems [Original text in Russian]”, Odessa: Science and Technology, 2010, p. 340.

[7] V.D. Dvornikov. “Method for the formation of bent-sequences [Original text in Russian]”, Reports of BSUIR, Minsk, 2003, pp. 106–109.

[8] Wild, P. Infinite families of perfect binary arrays, Electronics Letters, United Kingdom, Vol. 24, Issue 14, 1988, P. 845—847.

[9] Agievich S.V. On the representation of bent functions by bent rectangles. — Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000). Utrecht, Boston: VSP, 2002, P. 121—135.

[10] M. I. Mazurkov, A.V. Sokolov, I.V. Tsevukh, Synthesis Method for Families of Constant Amplitude Correcting Codes Based on an Arbitrary Bent-Square. Journal of Telecommunication, Electronic and Computer Engineering, Vol. 9, No. 2, 2017, pp. 99—103.