УДК 621.396.946

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 5-14

EFFECT OF BINARY ORTHOGONAL TRANSFORM TYPE ON THE CARDINALITY AND STRUCTURE OF CONSTANT AMPLITUDE CODES FOR THE MC-CDMA TECHNOLOGY

A.V. Sokolov

Odesa National Polytechnic University,
Shevchenko ave. 1, Odesa, 65044, Ukraine; e-mail: radiosquid@gmail.com

One of the most important multiple access technologies used in modern mobile telecommunication systems is MC-CDMA technology, in which Walsh-Hadamard transform coefficients are used as transmitted signals. Despite the significant advantages of MC-CDMA technology, its significant disadvantage is the high PAPR (Peak-to-Average Power Ratio) values of the transmitted signals. One of the most effective methods to overcome this disadvantage is the use of C-codes, each codeword of which has a strictly defined PAPR value. This paper is devoted to the research of the influence of the type of binary orthogonal transform on the structure and cardinality of C-codes, which can be built on its basis. It is established that the class of classical bent-sequences with respect to the Walsh-Hadamard matrix constructed using the Sylvester construction is only a special case of the class of binary bent-sequences. It was established that similar classes of bent-sequences exist for two other nonequivalent classes of Hadamard matrices, as well as for Hadamard matrices constructed on the basis of other perfect algebraic constructions: perfect binary arrays and, in fact, classical bent-sequences. So, in the paper, algebraic normal forms of bent-sequences constructed with respect to the second and third nonequivalent Hadamard matrices of order n=16 are listed. The structure and cardinality of classes of bent-sequences constructed with respect to Hadamard matrices synthesized based on perfect binary arrays and classical bent-sequences were researched. Using the found new classes of bent-sequences, as well as the concept of operative changing of the working orthogonal transform matrix, it will be possible to reduce the redundancy of C-codes used in MC-CDMA technology while maintaining the PAPR of the transmitted signals at a minimal level.

Keywords: Peak-to-Average Power Ratio, C-code, MC-CDMA, bent-sequence, perfect binary array.

Introduction and problem statement

The key technology used to build new generation mobile communication systems is Multi-Code Code Division Multiple Access (MC-CDMA) technology, in which communication channels have the same frequency band, but different code manipulation [1]. MC-CDMA technology has many advantages, such as high noise immunity, flexible distribution of resources among subscribers, high security level, and greater energy efficiency.

MC-CDMA technology is based on the coding model of the transmitted information using an orthogonal transform to implement the concept of code division of channels (Fig. 1).

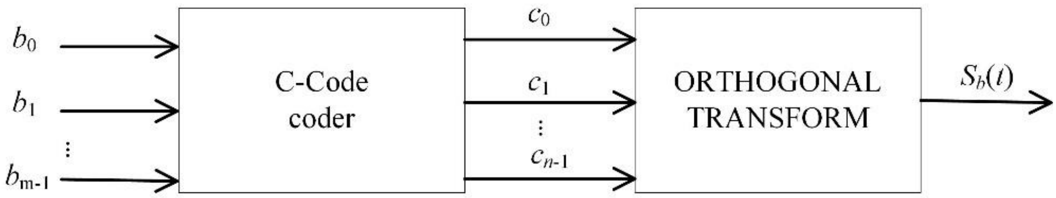

Fig. 1. Information coding model based on orthogonal transform

Thus, the original message d_i is encoded using a set of codewords c_j of the C-code, which are fed to the input of the Walsh-Hadamard orthogonal transform unit, and further to the transmitter.

One of the most significant requirements for the C-code is its ability to form output signals with an optimal PAPR value

$$\kappa = \frac{P_{\max}}{P_{av}} = \frac{1}{n} \max_t \left\{ \left| S_c(t) \right|^2 \right\}, \tag{1}$$

where $P_{\max}$ is the peak power of $S_c(t)$ signal; P_{av} is the average power of signal $S_c(t)$; n is the length of signal $S_c(t)$.

Achieving the optimal value of the PAPR can significantly increase the energy and spectral efficiency of the communication system, reduce the levels of out-of-band emissions, nonlinear distortion, and facilitate the reception and demodulation of the transmitted signal.

The researches [2] led to the conclusion that the optimal value of the PAPR $\kappa = 1$ can be achieved only by the use of such perfect algebraic constructions as bent-sequences [3], which have uniform absolute values of the Walsh-Hadamard transform coefficients. However, the number of bent-sequences is small, for example, for the length $N = 16$ their class cardinality is equal to $J_{16} = 896$ [4], which leads to significant redundancy of code, which is spent only on reducing the PAPR of the output signal. The possibility of increasing the cardinality of classes of available signals with an optimal value of the PAPR may lie in the consideration of new types of orthogonal transforms, but this issue has not been considered well in the literature.

The purpose of this paper is to research new classes of orthogonal transform matrices of order $\lambda = 16$ in terms of the possibility of the constructing the C-codes with an optimal PAPR value κ.

Definition 1 [5]. The Hadamard matrix A of order λ is a such matrix that all its elements take values from the set $\{\pm 1\}$ and the following identity is valid

$$A \cdot A^T = \lambda E,$$

where T is the transpose operator, E is the identity matrix.

As an orthogonal transform in communication systems with MC-CDMA technology, the well-known Hadamard matrices of order $\lambda = 2^k$ obtained using the recurrent rule are often used

$$A_{2^k} = \begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix}, \tag{2}$$

where $A_1 = 1$.

Equivalent classes of Hadamard matrices of order $N = 16$

Definition 2 [6]. The Hadamard matrices obtained from each other by repeated using of the operations of inversion and permutation of rows or columns are called as equivalent.

It was shown in [6] that for the orders of Hadamard matrices $\lambda = 1; 2; 4; 8$ there is only one class of equivalent Hadamard matrices, whose representative matrix can be obtained by using the recurrent rule (2). For the order $\lambda = 16$, there are 5 equivalent classes of Hadamard matrices, whose representatives are shown in Fig. 2.

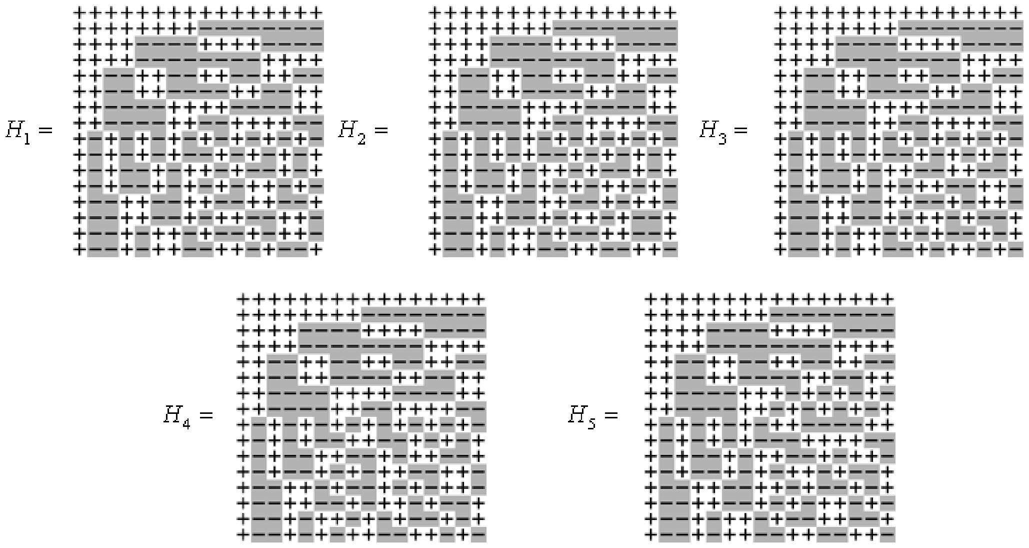

Fig. 2. Equivalent classes of Hadamard matrices

Using each of the Hadamard matrices shown in Fig. 2 as an orthogonal transform in the model (Fig. 1) and the full code as the C-code, we construct (Table 1) the PAPR distribution tables calculated in accordance with (1) [7].

Table 1.

The PAPR distribution for full code vectors for different non-equivalent matrices

No.	Absolute peak value $P_{\max}$	PAPR value κ	The number of vectors for the matrix				
			H_1	H_2	H_3	H_4	H_5
1	16	1	896	384	128	0	0
2	36	2,25	14336	14336	14336	14336	14336
3	64	4	28000	28512	28768	28896	28896
4	100	6,25	17920	17920	17920	17920	17920
5	144	9	3840	3840	3840	3840	3840
6	196	12,25	512	512	512	512	512
7	256	16	32	32	32	32	32

It is clear that of the greatest practical interest from the point of view of construction of the C-codes are the vectors from group No. 1 (Table 1), which have the optimal value of the PAPR $\kappa = 1$. For the matrix H_1, each such codeword is a bent-sequence of length $N = 16$, a regular synthesis method of which was developed in [4].

Definition 3 [7]. A binary sequence $B = [b_0, b_1, \cdots, b_i, \cdots, b_{n-1}]$ of length n, where $b_i \in \{\pm 1\}$ are the coefficients, $i = 0,1,...,n-1$, $n = 2^k, k = 2,4,6,8,...$, is called a bent-sequence, if it has a uniform Walsh-Hadamard spectrum $W_B(\omega)$.

We call a bent-sequence as classical if Definition 3 is valid for Walsh-Hadamard matrix of classical structure (2).

Thus, the number of bent-sequences is different for each nonequivalent class of orthogonal transform (Fig. 2). However, research have shown that the codewords of the C-code formed from the vectors of group No. 1 for the orthogonal transform matrix H_1 include the vectors for the matrix H_2 and H_3. In other words, the matrices H_2 and H_3 do not allow obtaining new structures of bent-sequences.

Definition 4 [8]. The algebraic normal form (ANF) $\varphi(x_1, x_2, ..., x_k)$ of a sequence T is a polynomial of $k \le \log_2 n$ variables with coefficients $a_i \in \{0,1\}$, where the AND operation is used as the multiplication, and the XOR operation is used as the addition operation

$$\varphi\left(x_1, x_2, ..., x_k\right) = \bigoplus_{i=0}^{n-1} a_i X_i^s ,$$

where X_i^s are the terms of the ANF polynomial of degree $s = wt\{X\}$; wt is the Hamming's weight. The coefficients $a_i = \{a_0, a_1, ..., a_{n-1}\}$ can be found by performing the Reed-Muller transform [8], i.e. by multiplying the original sequence by the Reed-Muller matrix RM_v

$$\{a_i\} = TRM_v, T = \{a_i\}RM_v ,$$

where the original sequence T is represented above the alphabet {0,1} using a bijective mapping $+1 \leftrightarrow 0, -1 \leftrightarrow 1$, and the Reed-Muller matrix RM_v is determined using the following recurrent rule

$$RM_0 = [1], RM_v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes RM_{v-1} = \begin{bmatrix} RM_{v-1} & 0 \\ RM_{v-1} & RM_{v-1} \end{bmatrix},$$

where $\otimes$ is the Kronecker product.

Definition 5 [8]. Terms of ANF of the degree $s = wt\{X\} \le 1$ are called as affine.

For example, for sequence length $n = 16$ there are the following possible affine terms: $1, x_1, x_2, x_3, x_4$ on the basis of which corresponding affine codewords can be formed.

The modern approach to the classification, as well as the synthesis of bent-sequences, involves the use of the following proposition.

Proposition 1 [3]. The sum of a bent-sequence with an affine function (which is equivalent to adding one or several affine terms to the ANF coefficients sequence) leads to the formation of other bent-sequences.

The researches performed in this paper allowed us to establish that Proposition 1 is valid for bent-sequences, both on the basis of the orthogonal transform matrix H_1, and for the bent-sequences on the basis of the orthogonal transform matrices H_2 and H_3.

Thus, the full set of bent-sequences of cardinality $J = 896$ can be classified into $896/32 = 28$ affine non-equivalent classes, in each of which it is possible to distinguish a bent-sequence that does not have affine terms

$$b_1 = x_2x_3 + x_1x_4;$$
$$b_2 = x_2x_3 + x_1x_4 + x_1x_2;$$
$$b_3 = x_2x_3 + x_1x_4 + x_1x_3;$$
$$b_4 = x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2;$$
$$b_5 = x_2x_4 + x_1x_3;$$
$$b_6 = x_2x_4 + x_1x_3 + x_1x_2;$$
$$b_7 = x_2x_4 + x_1x_4 + x_1x_3;$$
$$b_8 = x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2;$$
$$b_9 = x_2x_4 + x_2x_3 + x_1x_3;$$
$$b_{10} = x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2;$$
$$b_{11} = x_2x_4 + x_2x_3 + x_1x_4;$$
$$b_{12} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2;$$
$$b_{13} = x_3x_4 + x_1x_2;$$
$$b_{14} = x_3x_4 + x_1x_3 + x_1x_2;$$
$$b_{15} = x_3x_4 + x_1x_4 + x_1x_2;$$
$$b_{16} = x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2;$$
$$b_{17} = x_3x_4 + x_2x_3 + x_1x_2;$$
$$b_{18} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2;$$
$$b_{19} = x_3x_4 + x_2x_3 + x_1x_4;$$
$$b_{20} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3;$$
$$b_{21} = x_3x_4 + x_2x_4 + x_1x_2;$$
$$b_{22} = x_3x_4 + x_2x_4 + x_1x_3;$$
$$b_{23} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_2;$$
$$b_{24} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3;$$
$$b_{25} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_2;$$
$$b_{26} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3;$$
$$b_{27} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4;$$
$$b_{28} = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2.$$

Similarly, we can represent all bent-sequences relating to the matrix H_2 up to an affine term

$$\begin{array}{ll}
b_1 = x_2x_3 + x_1x_4; & b_7 = x_2x_4 + x_2x_3 + x_1x3; \\
b_2 = x_3x_4 + x_2x_3 + x_1x_4; & b_8 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3; \\
b_3 = x_2x_4 + x_2x_3 + x_1x_4; & b_9 = x_2x_4 + x_1x_4 + x_1x_3; \\
b_4 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4; & b_{10} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3; \\
b_5 = x_2x_4 + x_1x_3; & b_{11} = x_2x_3 + x_1x_4 + x_1x_3; \\
b_6 = x_3x_4 + x_2x_4 + x_1x_3; & b_{12} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3.
\end{array}$$

We also represent a set of bent-sequences relating to the matrix H_3 up to an affine term

$$\begin{array}{ll}
b_1 = x_2x_3 + x_1x_4; & b_3 = x_2x_4 + x_2x_3 + x_1x_4; \\
b_2 = x_3x_4 + x_2x_3 + x_1x_4; & b_4 = x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4.
\end{array}$$

Let us consider the well-known regular rules for constructing matrices of orthogonal transforms on the basis of perfect algebraic constructions and research their influence on the type and cardinality of the code.

The matrices of orthogonal transforms based on perfect binary arrays

Definition 6 [9]. A perfect binary array (PBA) is a two-dimensional matrix sequence

$$H(N) = \left\| h_{i,j} \right\|, \quad i,j = \overline{0, N-1}, \quad h_{i,j} \in \{-1,1\},$$

having an ideal two-dimensional Periodic Autocorrelation Function (PACF), whose elements

$$R(m,\tau) = PACF\left(m,\tau\right) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+\tau} = \begin{cases} N^2, & for \;\; m = \tau = 0; \\ 0, \text{ for any other } m \text{ and } \tau. \end{cases}$$

It is known that the generating $P(N)$ PBA class of order $N = 4$ consists of 12 arrays [9]

$$P_1(4) = \begin{bmatrix} -+-- \\ --+- \\ +++- \\ +--- \end{bmatrix},\; P_2(4) = \begin{bmatrix} ++-+ \\ +--- \\ --+- \\ +--- \end{bmatrix},\; P_3(4) = \begin{bmatrix} -+-- \\ -+++ \\ -+-- \\ +--- \end{bmatrix},\; P_4(4) = \begin{bmatrix} +++- \\ --+- \\ -+-- \\ +--- \end{bmatrix},$$

$$P_5(4) = \begin{bmatrix} +-++ \\ +--- \\ -+-- \\ +--- \end{bmatrix},\; P_6(4) = \begin{bmatrix} --+- \\ ++-+ \\ +--- \\ +--- \end{bmatrix},\; P_7(4) = \begin{bmatrix} ++-+ \\ --+- \\ +--- \\ +--- \end{bmatrix},\; P_8(4) = \begin{bmatrix} -+++ \\ +--- \\ +--- \\ +--- \end{bmatrix}, \tag{3}$$

$$P_9(4) = \begin{bmatrix} +--+ \\ -+-+ \\ ++-- \\ ---- \end{bmatrix}, P_{10}(4) = \begin{bmatrix} -++- \\ -+-+ \\ ++-- \\ ---- \end{bmatrix}, P_{11}(4) = \begin{bmatrix} +--+ \\ +-+- \\ ++-- \\ ---- \end{bmatrix}, P_{12}(4) = \begin{bmatrix} -++- \\ +-+- \\ ++-- \\ ---- \end{bmatrix}.$$

On the basis of each of the arrays (3) of the generating $P(N)$-class, an orthogonal matrix can be constructed by successively concatenating (joining) the rows of the original array and all its cyclic shifts in rows and columns. As an example, we give an orthogonal matrix constructed on the basis of the PBA $P_1(4)$

$$\psi_1 = \begin{bmatrix}
- & + & - & - & - & - & + & - & + & + & + & - & + & - & - & - \\
- & - & + & - & - & - & - & + & - & + & + & + & - & + & - & - \\
- & - & - & + & + & - & - & - & + & - & + & + & - & - & + & - \\
+ & - & - & - & - & + & - & - & + & + & - & + & - & - & - & + \\
+ & - & - & - & - & + & - & - & - & - & + & - & + & + & + & - \\
- & + & - & - & - & - & + & - & - & - & - & + & - & + & + & + \\
- & - & + & - & - & - & - & + & + & - & - & - & + & - & + & + \\
- & - & - & + & + & - & - & - & - & + & - & - & + & + & - & + \\
+ & + & + & - & + & - & - & - & - & + & - & - & - & - & + & - \\
- & + & + & + & - & + & - & - & - & - & + & - & - & - & - & + \\
+ & - & + & + & - & - & + & - & - & - & - & + & + & - & - & - \\
+ & + & - & + & - & - & - & + & + & - & - & - & - & + & - & - \\
- & - & + & - & + & + & + & - & + & - & - & - & - & + & - & - \\
- & - & - & + & - & + & + & + & - & + & - & - & - & - & + & - \\
+ & - & - & - & + & - & + & + & - & - & + & - & - & - & - & + \\
- & + & - & - & + & + & - & + & - & - & - & + & + & - & - & -
\end{bmatrix}.$$

Our experiments show that if the full code is used as a C-code each matrix $\psi_1,...,\psi_{12}$ gives the same PAPR value distribution as the matrix H_1 (Table 1).

So, if using the orthogonal transform based on the PBA it is possible to construct 896 sequences that have uniform absolute values of the Walsh-Hadamard transform coefficients.

Thus, the matrices $\psi_1,...,\psi_{12}$ produce $12 \cdot 896 = 10752$ bent-sequences. Considering each of them in comparison with the classical definition of a bent-sequence it was established that from the set of 10752 bent-sequences there are only 5120 unique ones, and there are $5120 - 896 = 4224$ ones that do not coincide with the class of classical bent-sequences. Let us give a classification of all newly discovered bent-sequences classes (Table 2).

Table 2.

Classes of bent-sequences based on PBA $P(N)$ class

Class Number	1	2	3	4	5	6
The orthogonal transform matrix	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6
Cardinality of the bent-sequences class	896	896	896	896	896	896
The number of bent-sequences, that coincide with the classical bent-sequences	128	384	128	128	128	128
The number of bent-sequences, that do not coincide with the classical bent-sequences	768	512	768	768	768	768
Class Number	7	8	9	10	11	12
The orthogonal transform matrix	ψ_7	ψ_8	ψ_9	ψ_{10}	ψ_{11}	ψ_{12}
Cardinality of the bent-sequences class	896	896	896	896	896	896
The number of bent-sequences, that coincide with the classical bent-sequences	128	384	128	128	128	128
The number of bent-sequences, that do not coincide with the classical bent-sequences	768	512	768	768	768	768

As an example, let us consider Class 1 of bent-sequences constructed on the basis of the matrix ψ_1 (Fig. 3). Based on this matrix, it is possible to build 768 new structures of bent-sequences that do not coincide with classical bent-sequences.

The performed researches have also shown that Proposition 1 is not valid in this class of bent-sequences. Thus, the sum of a bent-sequence with an affine codeword does not necessarily form a bent-sequence. However, in this paper, the following property of the class of bent-sequences relating to the matrix ψ_1 was established:

Property 1. The sum of a bent-sequence relating to matrix ψ_1 with an affine terms $1, x_4, x_2, x_1$ leads to the formation of other bent-sequences.

Using *Property 1* we can represent this set of bent-sequences relating to matrix ψ_1 in the 896/16=56 ANF up to affine terms $1, x_4, x_2, x_1$

$$\begin{array}{ll}
b_1 = 0; & b_{29} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_2 = x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{30} = x_3 + x_1x_3 + x_1x_2x_4; \\
b_3 = x_1x_4 + x_1x_2; & b_{31} = x_3 + x_1x_4 + x_1x_2; \\
b_4 = x_1x_4 + x_1x_3 + x_1x_2x_4; & b_{32} = x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_5 = x_2x_3 + x_1x_2; & b_{33} = x_3 + x_2x_3 + x_1x_2; \\
b_6 = x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{34} = x_3 + x_2x_3 + x_1x_3 + x_1x_2x_4; \\
b_7 = x_2x_3 + x_1x_4 + x_1x_2; & b_{35} = x_3 + x_2x_3 + x_1x_4 + x_1x_2; \\
b_8 = x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{36} = x_3 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4; \\
b_9 = x_2x_4; & b_{37} = x_3 + x_2x_4; \\
b_{10} = x_2x_4 + x_1x_3 + x_1x_2x_4; & b_{38} = x_3 + x_2x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{11} = x_2x_4 + x_1x_4 + x_1x_2; & b_{39} = x_3 + x_2x_4 + x_1x_4 + x_1x_2; \\
b_{12} = x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{40} = x_3 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4; \\
b_{13} = x_2x_4 + x_2x_3 + x_1x_2; & b_{41} = x_3 + x_2x_4 + x_2x_3 + x_1x_2; \\
b_{14} = x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4; & b_{42} = x_3 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{15} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2; & b_{43} = x_3 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_2; \\
b_{16} = x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4; & b_{44} = x_3 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{17} = x_3x_4; & b_{45} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{18} = x_3x_4 + x_1x_2; & b_{46} = x_3 + x_3x_4 + x_1x_2; \\
b_{19} = x_3x_4 + x_1x_3 + x_1x_2x_4; & b_{47} = x_3 + x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4; \\
b_{20} = x_3x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{48} = x_3 + x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{21} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4; & b_{49} = x_3 + x_3x_4 + x_2x_4; \\
b_{22} = x_3x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4; & b_{50} = x_3 + x_3x_4 + x_2x_4 + x_1x_2; \\
b_{23} = x_3x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4; & b_{51} = x_3 + x_3x_4 + x_2x_4 + x_1x_3 + x_1x_2x_4; \\
b_{24} = x_3 + x_3x_4; & b_{52} = x_3 + x_3x_4 + x_2x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{25} = x_3x_4 + x_2x_4; & b_{53} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2x_4; \\
b_{26} = x_3x_4 + x_2x_4 + x_1x_2; & b_{54} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_3 + x_1x_2 + x_1x_2x_4; \\
b_{27} = x_3x_4 + x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2x_4; & b_{55} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2x_4; \\
b_{28} = x_3; & b_{56} = x_3 + x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 + x_1x_2x_4.
\end{array}$$

Orthogonal transform matrices based on the full class of classical bent-sequences

In [10] it was shown that the construction of orthogonal transform matrices is also possible on the basis of the classical bent-sequences themselves by applying a regular dyadic shift operator

$$Dyad(N) = \begin{bmatrix} Dyad(N/2), & Dyad(N/2) + N/2 \\ Dyad(N/2) + N/2, & Dyad(N/2) \end{bmatrix},$$

where $Dyad(2) = \begin{bmatrix} 1,2 \\ 2,1 \end{bmatrix}$. For example, for a value $N = 16$, we get

$$Dyad(16) = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\
3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\
4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\
5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\
6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\
7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\
8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
10 & 9 & 12 & 11 & 14 & 3 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\
11 & 12 & 9 & 10 & 15 & 16 & 3 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\
12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\
13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\
14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\
15 & 16 & 13 & 14 & 11 & 2 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\
16 & 15 & 14 & 13 & 12 & 1 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}. \qquad (4)$$

Performing the permutation of the elements of the bent-sequence in accordance with the rules (lines) of the dyadic shift matrix, we obtain a binary matrix γ of the orthogonal transform.

It is known [3] that the cardinality of the class of classical bent-sequences of length $n=16$ is $J_{16}=896$. Thus, based on the dyadic shift operator (4), it is possible to construct the same number of orthogonal transform matrices $\gamma_1, \gamma_2, ..., \gamma_{896}$. It is clear that with respect to each of these orthogonal matrices there are their own bent-sequences classes — binary vectors with uniform absolute values of transform coefficients. Researches have shown that the number of such bent-sequences relating to each of the orthogonal transform matrices is also 896. Thus, there was constructed $896*896=802816$ bent-sequences.

It was discovered that just 1152 of these differs in structure from the classical bent-sequences [3].

Conclusion

Let us summarize the main results achieved in this paper:

- the method of synthesis of C-codes classes with uniform Walsh-Hadamard transform coefficients was further developed, it was established that the cardinality and the specific type of C-code strongly depends on the type of selected orthogonal transform.
- the using of methods for the synthesis of orthogonal matrices based on perfect binary arrays, a dyadic shift operator and classical bent-sequences allowed us to construct new families of bent-sequences that can be used as C-codes, and each of the sets of bent-sequences possesses optimal error correction ability.
- it was found that the existence of various structures of bent-sequences relating to orthogonal matrices based on perfect binary arrays, a regular dyadic shift operator and classical bent-sequences, allows to improve the MC-CDMA technology in the following aspects: by combining the found classes of bent-sequences and dynamically changing the orthogonal transform matrix depending on the data vectors arriving to its input, it is possible to reduce redundancy of the code that is spent on achieving the optimal PAPR value; by dynamically changing the orthogonal transform matrices using a pseudo-random sequence, which is unknown to the third party, it is possible to implement a secret communication system with a minimal computational cost for data encryption and decryption.

We also note that, in the case of other values of n, the problem of finding existing full classes of bent-sequences relating to the all regularly constructed orthogonal transforms, which is relevant from the point of view of MC-CDMA technology, remains unresolved and may be continued in the future.

References

1. Paterson, K.G. On codes with low peak-to-average power ratio for multicode CDMA / K.G. Paterson // IEEE Transactions on Information Theory. – 2004. – Vol. 50, No. 3. – Pp. 550 -559.
2. Paterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory / K.G. Paterson // Sequences and their applications, Seta 2001: Second Int. Conference, May 13–17 2001 : proceedings. – Bergen, Norway : Springer, 2002. – Pp. 46-71.
3. Tokareva, N. Bent Functions: Results and Applications to Cryptography / N. Tokareva. – Academic Press, 2015. – 220 p.
4. Mazurkov, M.I. The regular rules of constructing the complete class of bent-sequences of length 16 / M.I. Mazurkov, A.V. Sokolov // Proceedings of ONPU. – 2013. – No. 2(41). – Pp. 231-237.
5. Mazurkov, M.I. Broadband radio communication systems / M.I. Mazurkov. – Odessa: Science and Technology, 2010. – 340 p.
6. Hadamard matrices of order 16: Research Summary: Vol I, No. 36–10 / Jet Propulsion Laboratory; M.Jr. Hall. – 1961. – Pp. 21-26.

7. Mazurkov, M.I. On the effect of the type of orthogonal transform on PAPR of signal spectrum in CDMA systems / M.I. Mazurkov, A.V. Sokolov, N.A. Barabanov // Informatics and Mathematical Methods in Modeling. – 2015. – Vol. 5, No. 1. – Pp. 28-37.
8. Logachev, O.A. Boolean Functions in Coding Theory and Cryptography / O.A. Logachev, A.A. Salnikov, V.V. Yashchenko. – Amer Mathematical Society, 2012. – 334 p.
9. Mazurkov, M.I. Classes of equivalent and generating perfect binary arrays for CDMA technologies / M.I. Mazurkov, V.Ya. Chechelnitsky // Proceedings of the universities. Radioelectronics. – 2003. – Vol. 46, No. 5. – Pp. 54-63.
10. Mazurkov, M.I. Fast orthogonal transforms based on bent-sequences / M.I. Mazurkov, A.V. Sokolov // Informatics and mathematical methods in modeling. – 2014. – No. 1. – P. 5 -13.

ВПЛИВ ТИПУ ДВІЙКОВОГО ОРТОГОНАЛЬНОГО ПЕРЕТВОРЕННЯ НА ПОТУЖНІСТЬ І СТРУКТУРУ КОДІВ ПОСТІЙНОЇ АМПЛІТУДИ ДЛЯ ТЕХНОЛОГІЇ MC-CDMA

А.В. Соколов

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Однією з найважливіших технологій множинного доступу, яка використовується в сучасних мобільних телекомунікаційних системах є технологія MC-CDMA, в якій в якості сигналів, що передаються використовуються коефіцієнти перетворення Адамара. Незважаючи на істотні переваги технології MC-CDMA, її значним недоліком є високий пік-фактор сигналів, що передаються. Одним з найбільш ефективних методів подолання даного недоліку є використання C-кодів, кожне кодове слово яких має строго визначене значення пік-фактора. Ця стаття присвячена дослідженню впливу виду бінарного ортогонального перетворення на структуру і потужність C-кодів, які можуть бути побудовані на його основі. У статті встановлено, що клас класичних бент-послідовностей щодо матриці Адамара, побудованої за допомогою конструкції Сильвестра, є лише окремим випадком класу бінарних бент-послідовностей. Встановлено, що подібні класи бент-послідовностей існують для двох інших нееквівалентних класів матриць Адамара, а також для матриць Адамара, побудованих на основі інших досконалих алгебраїчних конструкцій: досконалих двійкових решіток і, власне, класичних бент-послідовностей. Так, в статті виписані алгебраїчні нормальні форми бент-послідовностей, побудованих щодо другої і третьої нееквівалентних матриць Адамара порядку n=16. Проведено дослідження структури і потужностей класів бент-послідовностей, побудованих відносно матриць Адамара, синтезованих на основі досконалих двійкових решіток і класичних бент-послідовностей. Використання знайдених нових класів бент-послідовностей, а також концепції оперативної зміни робочої матриці ортогонального перетворення, дозволить отримати зменшення надмірності C-кодів, що застосовуються в технології MC-CDMA при збереженні пік-фактора сигналів, що передаються на мінімальному рівні.

Ключові слова: пік-фактор, C-код, MC-CDMA, бент-послідовність, досконала двійкова решітка.

ВЛИЯНИЕ ТИПА ДВОИЧНЫХ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ НА МОЩНОСТЬ И СТРУКТУРУ КОДОВ ПОСТОЯННОЙ АМПЛИТУДЫ ДЛЯ ТЕХНОЛОГИИ MC-CDMA

А.В. Соколов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Одной из важнейших технологий множественного доступа, используемой в современных мобильных телекоммуникационных системах является технология MC-CDMA, в которой в качестве передаваемых сигналов используются коэффициенты преобразования Уолша-Адамара. Несмотря на существенные преимущества технологии MC-CDMA, её значительным недостатком является высокий пик-фактор передаваемых сигналов. Одним из наиболее эффективных методов преодоления данного недостатка является использование C-кодов, каждое кодовое слово которых имеет строго определенное значение пик-фактора. Настоящая статья посвящена исследованию влияния вида бинарного ортогонального преобразования на структуру и мощность C-кодов, которые могут быть построены на его основе. В статье установлено, что класс классических бент-последовательностей относительно матрицы Уолша-Адамара, построенной с помощью конструкции Сильвестра, является лишь частным случаем класса бинарных бент-последовательностей. Установлено, что подобные классы бент-последовательностей существуют для двух других неэквивалентных классов матриц Уолша-Адамара, а также для матриц Уолша-Адамара, построенных на основе других совершенных алгебраических конструкций: совершенных двоичных решеток и, собственно, классических бент-последовательностей. Так, в статье выписаны алгебраические нормальные формы бент-последовательностей, построенных относительно второй и третей неэквивалентных матриц Адамара порядка n=16. Проведены исследования структуры и мощности классов бент-последовательностей, построенных относительно матриц Адамара, синтезированных на основе совершенных двоичных решеток и классических бент-последовательностей. Использование найденных новых классов бент-последовательностей, а также концепции оперативной смены рабочей матрицы ортогонального преобразования, позволит получить уменьшение избыточности C-кодов, которые применяются в технологии MC-CDMA при сохранении пик-фактора передаваемых сигналов на минимальном уровне.

Ключевые слова: пик-фактор, C-код, MC-CDMA, бент-последовательность, совершенная двоичная решетка.