Synthesis Method for Families of Constant Amplitude Correcting Codes Based on an Arbitrary Bent-Square

Michael I. Mazurkov, Artem V. Sokolov, Igor V. Tsevukh
Department of Radioelectronic and Telecommunication Systems,
Odessa National Polytechnic University, Ukraine.
phdsquid@mail.ru

***Abstract*—One of the significant disadvantages of MC-CDMA (Multi Code-Code Division Multiple Access) technology is a high PAPR (Peak-to-Average Power Ratio) values of used signals in such telecommunication systems. The most modern and effective solution to this problem is the C-codes based on bent-sequences. However, C-codes introduce significant redundancy in communication systems, which consumes only to reduce the signals PAPR value. In this paper, we developed a method for the synthesis of C-codes with error-correction properties on the basis of an arbitrary Agievich bent-square. To build a C-code with the specified distance properties, we used the proposed sets of semidyadic permutations. Structural properties of built C-codes allow the use of simplified procedures for coding and decoding. In this case, for length $N = 256$ and PAPR value $\kappa = 1$, the cardinalities of constructed C-codes are in the range $J = 512...10321920$ for the code distances $d = 128...64$.**

***Index Terms*—Constant Amplitude Code; MC-CDMA; Bent-Sequence; Bent-Square.**

I. INTRODUCTION

Further development in 4G mobile data transmission systems and the promising LTE technology are largely based on improving the CDMA technology (Code Division Multiple Access). In recent years, researchers have been focusing on one of the most promising CDMA technology modifications — MC-CDMA (Multi Code - Code Division Multiple Access).

According to the MC-CDMA technology, the binary data vector $D = \{d_i\}, i = 0,1,...,N-1$ is subjected to the orthogonal transform [1]. Each data bit d_i changes the sign of one of N orthogonal functions of discrete time $a_i(t)$, and the output is the sum of these N modulated functions. The transmitted signal is a Walsh-Hadamard spectrum coefficients of sequence D.

$$S_D(t) = \sum_{i=0}^{N-1} d_i a_i(t) = D \cdot A, \qquad (1)$$

where A is the Hadamard matrix of order $N = 2^k$, which is constructed in accordance with the following recurrent relation:

$$A_{2^k} = \begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix}, \quad A_1 = 1. \qquad (2)$$

Although it has numerous advantages, such as high noise immunity, flexibility of system bandwidth distribution among subscribers, efficiency and good electromagnetic compatibility, MC-CDMA technology still has some disadvantages. One of the most significant disadvantages of MC-CDMA technology is the high PAPR (Peak-to-Average Power Ratio) values of signals. This fact leads to an inefficient use of the transmitter power, non-linear distortions. Consequently, the rise in the cost of the equipment used reduces the potentially achievable noise immunity.

The PAPR of the signals in the system is determined by the peak of Walsh-Hadamard transform coefficients [2].

$$\kappa = P_{\max} \Big/ P_{av} = \frac{1}{N} \max_t \left\{ \left| S_D(t) \right|^2 \right\} \qquad (3)$$

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

One of the most effective solutions to this problem is using the C-codes (constant amplitude codes) to reduce the PAPR in the system signals. The main results on C-codes are represented in [3].

Definition 1: C-code or constant amplitude code is a set of codewords that have a predetermined, fixed codeword for each PAPR value [3].

Application of C-code suggests the replacement of encoder input vectors $\{d_j\}$ of length m to such codeword vectors $\{c_i\}$ of length n, which have the lowest value of PAPR as shown in Figure 1.

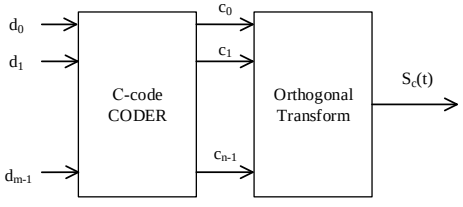

Figure 1: C-code application scheme

It is clear that in practice $n > m$, thus, C-code introduces redundancy into the transmitted messages, which is used only to reduce the PAPR, thereby reducing data transmission rate in time of $R = m/n$. Note, that the redundancy introduced by the C-code can be used not only to reduce the PAPR, but also to give the C-code some correcting properties. This fact makes it necessary to develop such a C-code, which would have the corrective properties [4].

The purpose of this article is to develop a synthesis method of the families of constant amplitude correction codes based on an arbitrary bent-square.

The optimal algebraic constructions to generate the C-code codewords of the length $N = 2^k$, $k = 2,4,6,...$ are bent-sequences. They have a uniform Walsh-Hadamard spectrum, and accordingly, the value of the PAPR $\kappa = 1$ [5].

Definition 2: A binary sequence $B = [b_0, b_1, \cdots, b_i, \cdots, b_{N-1}]$ $b_i \in \{\pm 1\}$, of the length $N = 2^k = n^2$, $k = 2,4,6,...$ is called a bent-sequence, if it has a uniform modulo of the Walsh-Hadamard spectrum, which can be represented in the matrix from [5].

$$W_B(\omega) = BA_N, \ \omega = \overline{0, N-1}. \quad (4)$$

Further, we consider in detail the main types of representation and methods of constructing the bent-sequences.

II. Representation of Bent-Functions by Bent-Squares, and a Method for Construction of Semidyadic Permutations Set

The theory of synthesizing the bent-functions is complex, multifaceted and has a highly developed mathematical apparatus [6]. One of the most valuable achievements of this theory is a form of representation of bent-functions by the bent-squares proposed by S. Agievich [7].

Definition 3: Bent-square is a matrix, in which each row and each column is the spectral vector of the Walsh-Hadamard transform.

In [8] an algorithm for the synthesis of Agievich bent-squares of arbitrary order on the basis of a given spectral vector and regular operator of dyadic shift is presented. We briefly explain the essence of this algorithm, which is based on a few definitions.

Definition 4: The elementary structure of the spectral vector is said to be a set of absolute values of its spectral components [9].

Definition 5: The parameter $\gamma_{\max} = \max\{|W_i|\}$ of spectral vector W_i is defined as the maximum absolute value.

Definition 6: The equivalent class of spectral vectors $\{W_j\}$ is the set of vectors, each of which has the same elementary structure but different position structures and/or sign coding.

Thus, when $N = 16$, the set of vectors $\{W_i\}$ is divided into 8 equivalent classes (Table 1).

In Table 1, we used the following notation of spectral vectors: the number before the brackets indicates the absolute value of the Walsh-Hadamard that transforms the coefficient, whilst the number in brackets indicates the number of times it occurs in the spectral vector.

Table 1
Classification of spectral vectors of length $N = 16$

No.	The elementary structure of the spectral vector	Cardinality of equivalent class	Number of different position structures	Number of sign coding
1	$\{16(1), 0(15)\}$	32	16	2
2	$\{14(1), 2(15)\}$	512	16	32
3	$\{12(1), 4(7), 0(8)\}$	3840	240	16
4	$\{10(1), 6(3), 2(12)\}$	17920	560	32
5	$\{8(2), 4(8), 0(6)\}$	26880	840	32
6	$\{8(4), 0(12)\}$	1120	140	8
7	$\{6(6), 2(10)\}$	14336	448	32
8	$\{4(16)\}$	896	1	896

Definition 7: The basic (primary) bent-square is said to be those that are being built by direct method based on dyadic shift [8] and based on non-equivalent spectral vectors.

Proposition 1: For each of the basic classes of spectral vectors, the bent-square can be built on the basis of one representative vector and a regular dyadic shift operator.

Definition 8: The dyadic shift operator can be represented in the form of a square matrix of the order n, which is based on the recurrent rule [10].

$$\mathrm{Dyad}(n) = \begin{bmatrix} \mathrm{Dyad}(n/2), & \mathrm{Dyad}(n/2) + n/2 \\ \mathrm{Dyad}(n/2) + n/2, & \mathrm{Dyad}(n/2) \end{bmatrix} \quad (5)$$

where $\mathrm{Dyad}(2) = \begin{bmatrix} 1, 2 \\ 2, 1 \end{bmatrix}$.

Using Equation (5), it is not difficult to construct a dyadic shift matrix of the order $n = 16$.

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

For example, let us consider a third class of spectral vectors by selecting one representative spectral vector

$$S=[12\ -4\ -4\ -4\ -4\ -4\ -4\ -4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0] \quad (7)$$

Applying *Proposition 1*, on the basis of a representative vector in Equation (7), we can construct a bent-square by using dyadic shift operator in Equation (6).

$$BS_3 = \begin{bmatrix}
12 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & 12 & -4 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & 12 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & -4 & 12 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & -4 & -4 & 12 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & -4 & -4 & -4 & 12 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & -4 & -4 & -4 & -4 & 12 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & -4 & -4 & -4 & -4 & -4 & -4 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & -4 & -4 & -4 & -4 & -4 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & 12 & -4 & -4 & -4 & -4 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & 12 & -4 & -4 & -4 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & 12 & -4 & -4 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & 12 & -4 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & 12 & -4 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & -4 & 12 & -4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 12
\end{bmatrix} \quad (8)$$

Based on bent-square in Equation (8), we can build a lot of square-equivalent bent-functions with the help of the sign coding operations and permutations of rows and columns of the original bent-square [7].

The operation of sign coding of bent-square in Equation (8) is used to obtain a new square-equivalent bent-functions based on the application of sign coding matrices. To perform the permutation operation of bent-square rows in this article, we developed such a new design as semidyadic permutations.

Definition 9: The semidyadic permutation is a permutation in which each component Boolean function is an affine Boolean function.

In this paper, we proposed an algorithm for the synthesis of semidyadic permutations that can be written in the form of specific steps accompanied with an example for the length $N = 16$.

Step 1: Consider the biorthogonal code of length $N = 16$ and cardinality $J' = 32$. We deleted from the biorthogonal code such codewords, which are not balanced (consisting of all elements "0" or "1"), thereby the cardinality of the obtained code is $J = 30$, and the codewords are represented by further matrix.

$$\begin{bmatrix}
0101010101010101 & 1010101010101010 \\
0011001100110011 & 1100110011001100 \\
0110011001100110 & 1001100110011001 \\
0000111100001111 & 1111000011110000 \\
0101101001011010 & 1010010110100101 \\
0011110000111100 & 1100001111000011 \\
0110100101101001 & 1001011010010110 \\
0000000011111111 & 1111111100000000 \\
0101010110101010 & 1010101001010101 \\
0011001111001100 & 1100110000110011 \\
0110011010011001 & 1001100101100110 \\
0000111111110000 & 1111000000001111 \\
0101101010100101 & 1010010101011010 \\
0011110011000011 & 1100001100111100 \\
0110100110010110 & 1001011001101001
\end{bmatrix} \quad (9)$$

Step 2. To construct a permutation of the length $N = 16$, we used balanced Walsh functions in Equation (9) as a component of Boolean functions. Selecting the component Boolean functions from the code of cardinality $J = 30$, which is built in *Step 1* combination can be done in $C_{30}^4 = 27\,405$ ways.

Step 3. Based on the obtained codes in *Step 2*, permutations should be tested for bijectivity. All non-bijective permutations must be eliminated. Thus, we obtained a set of 13 440 permutations.

Step 4: The obtained set in *Step 3* permutations underwent all the possible permutations component Boolean functions. For the results based on each semidyadic permutation, we derived a set of $(\log_2 16)! = 4! = 24$ new semidyadic permutations.

Total cardinality of semidyadic permutations is the superposition of all the above sets, which is $J_D = 13\,440 \cdot 24 = 322\,560$. Note that each semidyadic permutation applied to the rows of bent-square in Equation (8) generates a new unique bent-square and respectively, a new bent-sequence.

III. The Method of Construction for Families of Constant Amplitude Correction Codes

Let us separately perform the Walsh-Hadamard transformation for each row of bent-square in Equation (8), whereby rows are represented in the temporal domain.

$$BST_3 = \begin{bmatrix}
- & + & + & + & + & + & + & + & - & + & + & + & + & + & + & + \\
- & - & + & - & + & - & + & - & - & + & - & + & - & + & - & + \\
- & + & - & - & + & + & - & - & + & - & - & + & + & - & - & + \\
- & - & - & + & + & - & + & - & - & + & + & - & + & - & + & - \\
- & + & + & + & - & - & - & - & + & + & + & - & - & - & - & - \\
- & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
- & + & - & - & - & + & + & - & + & - & - & + & - & + & + & - \\
- & - & - & + & - & + & + & - & - & + & + & - & + & - & - & + \\
- & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - \\
- & - & + & - & + & - & + & - & + & + & - & + & - & + & - & + \\
- & + & - & - & + & + & - & - & - & - & + & + & + & + & - & - \\
- & - & - & + & + & - & + & - & + & + & - & - & - & - & + & + \\
- & + & + & + & - & - & - & + & - & - & - & + & + & + & + & + \\
- & - & + & - & + & - & + & + & + & - & + & - & + & - & + & - \\
- & + & - & - & - & + & + & - & + & - & - & + & - & + & + & - \\
- & - & - & + & - & + & + & - & - & + & + & - & + & - & - & +
\end{bmatrix}. \quad (10)$$

For the construction of the set of bent-sequences based on a plurality of equivalent bent-squares, we performed concatenation of its rows. Thus, the distance property of bent-square rows defines a distance property of the code, which can be built on its basis.

The research of the property of bent-square rows in temporal domain in Equation (10) shows that the Hamming distance between the rows of the matrix for each pair is equal to 8. Accordingly, a set of the matrix BST_3 rows is the equidistant code with a codeword length $N = 8$. Thus, the following statement in Proposition 2 is true:

Proposition 2: Selecting such different permutations of the matrix rows in Equation (10) in such a way that rows (segments) of two different bent-sequences in the matrix will be different from each other, resulting in the total distance will either increase by 8 or does not increase at all. Thus, by manipulating the permutations of the matrix rows, we can control the code distance of the constructed code.

Obviously, the maximum possible distance of the code on the basis of the matrix in Equation (10) will be equal to $d_{\max} = 16 \cdot 8 = 128$. To achieve higher cardinality of the code based on bent-squares, we propose a few rules of coding and permutations of the original matrix.

Rule 1: It was discovered that the permutations of dyadic shift (6) have a number of matches $\lambda = 0$. Thus, we can apply to the original matrix rows (10) 16 dyadic shift permutations (6), receiving 16 new codewords with a code distance of 128.

Rule 2: Bent-square allows column-wise symbolic coding (element-wise multiplication of the columns) of codewords by biorthogonal code, and the code distance in the length of

the resulting code of length $N=16$ stays unchanged and equal to 8.

Using *Rule 1* and *Rule 2* allows us to reach a total cardinality of code equals to $J=32\cdot16=512$ codewords. Note that from the permutations of a complete set of semidyadic permutations, for example the length of $N=16$ and cardinality $J=322\,560$, we can choose (even by a brute force method) such permutations, that the number of matches in them would be smaller than $\lambda\le\lambda_0$. Thus, by varying the value of λ_0, we can control the code distance of constructed correcting code.

Table 2 summarizes the data about families of correcting codes based on a predetermined bent-square to the different selected values of λ_0.

Table 2
The Characteristics of The Families of The Error-Correcting C-Codes

n	$k=\log_2 J$	d	t	Perms	J	κ	λ_0
256	9	128	63	16	512	1	0
256	11.8074	120	59	112	3584	1	1
256	13.4717	112	55	355	11360	1	2
256	18.8341	96	47	14604	467328	1	4
256	23.2992	64	31	322560	10321920	1	8

In Table 2, the following designations were used: n is the length of codeword of error-correcting C-code; k is the number of information bits, d is the minimum code distance, t is the number of correctable errors, Perms is the number of permutations of the semidyadic permutations set having the number of matches $\lambda\le\lambda_0$; J is the cardinality of error-correcting code; κ is the PAPR.

IV. Encoding and Decoding Algorithms

Consider the code $(n,k,d,\kappa)=(256,9,128,1)$ for example; however, the algorithm may be applied to other codes (Table 2) with a difference only in the number of lines permutations of chosen bent-square.

Obviously, the source of information is stored in the number of dyadic permutation ($\log_2 16=4$ bits) and in a number of Walsh function ($\log_2 32=5$ bits).

Suppose the initial information word to be $I=[11010111]\Rightarrow I_1=[1101];\ I_2=[0111]$. Next we performed a coding procedure.

A. Algorithm A.1. Coding

Step 1: In accordance with *Rule 1* we performed the temporal bent-square (10) dyadic shift permutation of number $I_1+1=14$ (numbering begins from one), resulting in a new temporal bent-square.

$$BST1=\begin{bmatrix}
--+--+-+++-++-+-\\
-+++----+---+++\\
---+-++-+++-+--+\\
-+----+++-++++--\\
--+-+-+-++-+-+-+\\
-++++++++-------\\
---++--++++--++-\\
-+--+--+---+--++\\
--+-+-+---+-+---\\
-+----++-+----++\\
--+-+-+---+-+-+-\\
-+++++++-++++++\\
---++--+---++--+\\
-+--++---+--++--
\end{bmatrix}. \quad (11)$$

Step 2: In accordance with *Rule 2*, we performed a sign coding. Because of $I_2+1=8$, each column of $BST1$ was multiplied by the eighth Walsh function in a Hadamard matrix. As a result, we obtained the following matrix.

$$BST2=\begin{bmatrix}
--+--+-++++-++-+-\\
+---++++-+++----\\
+++-+--+---+-++-\\
-+----++++-++++--\\
++-+-+-+-+--+-+-+-\\
-++++++++-------\\
---++--++++--++-\\
+-++--+-+--+--++--\\
--+---+-+--+--+-+\\
+---++++++--++++\\
+++-+--++++-+--+\\
-+----++-+----++\\
++-+-+-++-+-+-+\\
-++++++++++++++\\
---+---+---++--+\\
+-++--++-++--++
\end{bmatrix}. \quad (12)$$

Step 3: To obtain a codeword, we performed a consistent string concatenation of the matrix in Equation (12).

$$\begin{array}{l}
S=[--+--+-+++-++-+-+---++++-+\\
++----+++-+--+---+-++--+----+\\
++-++++--++-+-+-+--+-+-+--+++\\
+++++----------++--++++--++-+\\
-++--++-+--++-----+--+-+--+--+\\
-++---+++++---++++++++-+--++++\\
-+--+-+-----+-+---++++-+-+-+\\
++-+-+-+-++++++-++++++---++\\
--+---++--++-++--+++-++--++].
\end{array} \quad (13)$$

Assume that during the transmission of the codeword 63, the errors occurred were equivalent to the multiplication of the transmitted vector in Equation (13) to the next error vector.

$$\begin{array}{l}
E=[-+-+++-++-+++++++--++\\
++--++-++++++++++-+--++\\
+-++++++++++-+++-++++--+-\\
+++-+-+++++--+-++++-++++\\
+++++-+++++-+++-+++-++++\\
--+-++++++++++++-+--+++++\\
+++++++++++---+-++++++-+\\
++-++---++++--++++-+++++\\
+++++++-++-++++++++++-+++\\
++-++++++++-++++++++++-++\\
++++-++-++-++++++++].
\end{array} \quad (14)$$

Thus, the recipient received the following codeword.

$$\begin{array}{l}
S'=S\cdot E=[+----++++--++-+-++++-\\
+++-+++-----+++-+----+-+-+-\\
--+----++++++---+-++++-++-\\
--+-+-+-+-++++----------+\\
--+-++-+++---+-+-+++--++--\\
--+-+++---+--+-++---++++-++\\
--++++++++---++-+---+--+---\\
+--+----++++-+++--++-+-+-+-\\
-++++--++++++----+-+-+--++\\
+--++++++-+-+-++--++].
\end{array} \quad (15)$$

To perform the decoding operation the receiver should have the initial temporal bent-square in Equation (10). After receiving all the elements of the codeword, and before decoding, the receiver must perform the algorithm for detecting and correcting errors.

B. Algorithm A.2. Error correction

We performed a universal decoding algorithm: Find the distance from the received codeword to a set of allowed codewords and make a decision on the criterion of maximal likelihood. Next, go to the decoding operation. In our case, by using universal decoding algorithm, we get the transferred bent-square in Equation (12).

C. Algorithm A.3. Decoding

The essence of the decoding operation is to determine permutation and Walsh function used in coding operation.

Step 1: We wrote down the permutation of received bent-square with respect to the original bent-square.

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

Accordingly, the dyadic permutation 14 was applied to the initial bent-square in the process of coding operation, and thus the first part of the source code was $I_1 = [1101]$.

Step 2: Find the Walsh function that was used to perform a sign coding of initial bent-square. For this, we performed an element-wise multiplication on the first column of the original temporal bent-square in Equation (10) with the first column of received bent-square in Equation (12).

$$\begin{bmatrix} - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \\ - \end{bmatrix} \times \begin{bmatrix} - \\ + \\ + \\ - \\ + \\ - \\ - \\ + \\ - \\ + \\ + \\ - \\ + \\ - \\ - \\ + \end{bmatrix} = \begin{bmatrix} + \\ - \\ - \\ + \\ - \\ + \\ + \\ - \\ + \\ - \\ - \\ + \\ - \\ + \\ + \\ - \end{bmatrix}, \quad (17)$$

which corresponds to the eighth row of the Hadamard matrix, and accordingly, the second part of information code was $I_2 = [0111]$. As a result, we restored the original information.

IV. CONCLUSION

In this paper, we proposed a family of constant amplitude correction codes based on an arbitrary Agievich bent-square. The effective coding and decoding algorithms based on structural properties of the proposed code were developed.

We introduced the definition of semidyadic permutations. An algorithm for the synthesis of the full set of semidyadic permutations based on the Walsh functions was proposed. The semidyadic permutations may be used to increase the number of Agievich bent-squares, which makes such class of permutations an important element in the theory of bent-functions.

The proposed family of error-correcting constant amplitude codes can be used to implement the concept of operational change of used signals. For example, the selected type of initial bent-square can be used as an element of (long-term) key, providing structure secrecy to the communication system based on the MC-CDMA technology.

REFERENCES

[1] Jiangzhou Wang, "Broadband Wireless Communications", The International Series in Engineering and Computer Science, Volume 620, 2002, P. 64-93.

[2] K. G. Paterson "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, P. 46-71.

[3] K.G. Paterson "On codes with low peak-to-average power ratio for multicode CDMA" HP Laboratories Technical Report HPL-2001-115, May 2001.

[4] Y.C. Kim "Constant amplitude multi-code CDMA with built-in single parity check product code", IEEE Communications Letters, Volume: 10, Issue: 1, Jan 2006, P. 4-6.

[5] N. Tokareva "Generalizations of bent functions. A survey", Journal of Applied and Industrial Mathematics, January 2011, Volume 5, Issue 1, P. 110–129.

[6] N. Tokareva, "Bent Functions, 1st Edition: Results and Applications to Cryptography", Academic Press, 2015, P. 220.

[7] 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.

[8] A.V. Sokolov, "Regular Method for Synthesis of Basic Bent-Squares of Random Order", Science and Technology, 2016, No. 4, P. 345 - 352.

[9] A.V. Sokolov, N. A. Barabanov. "Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes", Radioelectronics and Communications Systems 58, 5 (2015): P. 220-227.

[10] R. Yarlagadda and J.E. Hershey, "Analysis and synthesis of bent sequences," IEEE Proceedings-E, Vol. 136, 1989, P. 112–123.