Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems

# Interrelation Between the Class of Bent-Sequences and the Class of Perfect Binary Arrays

Artem Sokolov[0000-0003-0283-7229]

Odesa National Polytechnic University, Shevchenko ave. 1, Odesa, 65044, Ukraine
radiosquid@gmail.com

**Abstract.** The paper is devoted to the research of the interrelation between classes of such perfect algebraic constructions as perfect binary arrays and bent-sequences. The algebraic normal form of bent-sequences of length $n=16$ that generate perfect binary arrays of order $N=4$, are presented. The exact number of perfect binary arrays in the full set of bent-sequences of length $n=64$ is found. The lower bound of cardinality of the full class of perfect binary arrays of order $N=8$ is improved.

Keywords: perfect binary array, 2DPACF, bent-sequence, Walsh-Hadamard transform.



## 1 Introduction and problem statement

Perfect binary arrays (PBA) are an important class of algebraic constructions that have found numerous applications in the tasks of cryptographic information protection [1], the synthesis of error correction codes [2], construction of orthogonal and biorthogonal signal systems, antenna aperture synthesis, as well as in many other applications of science and technology [3].

Nevertheless, despite the numerous applications and a large number of publications devoted to the problems of the synthesis of PBA, in the general case, there are no methods for constructing their full classes for the derived value of the PBA order $N$. Moreover, today there is not even an accurate estimation of the cardinality of the full class of PBA of practically valuable orders $N>4$, in particular order $N=8$. Significant progress in solving the problem of synthesizing the full class of PBA of order $N=8$ was obtained in [4], in particular, it was found that the cardinality of the PBA class of order $N=8$ is not less than $J_{8x8} \geq 688\,128$, while $688\,128$ PBA were constructed using the original constructive method.

Another major class of perfect algebraic constructions is the class of the bent-sequences (the truth tables of bent-functions), which was introduced in [5] and also found their numerous applications in cryptography and coding theory [6]. Methods for the synthesis of a full class of bent-sequences of length $n=16$ (the truth tables of bent-functions of four variables) are described in [7], while constructive methods for

2019. P. 339—349

the synthesis of a full class of bent-sequences of length $n = 64$ are proposed in [8, 9]. Recent researches of the PBA class carried out in [7] made it possible to establish that the full class of bent-sequences of length $n = 16$ and cardinality $J_{bent} = 896$ includes the full class of PBA of order $N = 4$ and cardinality $J_{PBA} = 384$.

However, the characteristics of the interrelation between the classes of bent-sequences of length $n = 16$ and PBA of order $N = 4$ remains unspecified. Researches on the interrelation between the class of bent-sequences of length $n = 64$ and PBA of order $N = 8$ are absent in the literature.

The purpose of this paper is to determine the interrelation between the class of bent-sequences of practically significant lengths $n = 16; 64$ and PBA of orders $N = 4; 8$.

## 2 Basic definitions

We introduce the basic definitions:

**Definition 1 [10].** A perfect binary array is a two-dimensional sequence (matrix)

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

having an ideal two-dimensional periodic autocorrelation function (2DPACF), whose elements

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

where $m, \tau = 0,1,...,N-1$, and all indices of elements $h_{i+m,j+\tau}$ are reduced modulo $N$.

Let us give as an example a perfect binary array of order $N = 4$ as well as its two-dimensional periodic autocorrelation function

$$H = \begin{bmatrix} + & + & + & - \\ + & + & + & - \\ + & + & + & - \\ - & - & - & + \end{bmatrix}, \quad R = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3}$$

where the symbol "+" denotes +1, and the symbol "–" denotes –1, respectively.

**Definition 2 [11].** The Walsh-Hadamard transform (WHT) of a vector $F(n)$ in matrix form is defined as

$$W_f(w) = A(n)F(n), \tag{4}$$

where $F(n)$ is the binary sequence of length $n$, $A(n)$ is the Hadamard matrix of order $n$, which is constructed in accordance with the following recurrence relation

$$A(n) = \begin{bmatrix} A(n/2) & A(n/2) \\ A(n/2) & -A(n/2) \end{bmatrix}, \quad A(1) = [+]. \tag{5}$$

**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 $W_B(\omega)$.

## 3 Interrelation Between the Class of Bent-Sequences of Length $n = 16$ and the Class of Perfect Binary Arrays of Order $N = 4$

Let us consider the currently known methods of classification of PBA and bent-sequences in order to establish the interrelation between these classes of perfect algebraic constructions. The modern approach to the classification of PBA involves the use of the following proposition:

**Proposition 1 [3].** Each PBA of order $N$ generates a $E(N)$-class of equivalent PBA matrices by using the cyclic rows and columns shift and inversion, with the cardinality of the equivalent matrices class

$$J_{E(N)} = 2N^2. \tag{6}$$

Thus, in accordance with **Proposition 1**, for the order of the PBA $N = 4$, the cardinality of each equivalent class is $J_{E(8)} = 2 \cdot 4^2 = 32$, and accordingly, the full set of PBA of cardinality $J_{PBA} = 384$ can be divided into $384/32 = 12$ nonequivalent classes. Representatives of these non-equivalent classes are given in [3].

In [7] it was shown that the full class of bent-sequences of length $n = 16$ includes the full class of PBA of order $N = 4$ in the case of their representation as vectors by successive concatenation of the rows (columns) of the corresponding PBA.

For example, we concatenate the rows of PBA (3), as a result of which we obtain the following sequence and its Walsh-Hadamard transform coefficients in accordance with (4)

$$\begin{gathered} B_1 = [+++-+++-+++----+]^T, \\ W_{B_1}(w) = A(16)B_1 = \\ = [4\ \ 4\ \ 4\ -4\ \ 4\ \ 4\ \ 4\ -4\ \ 4\ \ 4\ \ 4\ -4\ -4\ -4\ -4\ \ 4]. \end{gathered} \tag{7}$$

It is easy to see that the sequence (7) really satisfies the condition of **Definition 3** and is a bent-sequence of length $n = 16$.

A modern approach to the classification of bent-sequences is based on the consideration of affine-equivalent classes. This classification is easiest to make on the basis of the representation of bent-sequences in algebraic normal form.

**Definition 4 [11].** 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

$$\varphi\left(x_1, x_2, ..., x_k\right) = \bigoplus_{i=0}^{N-1} a_i X_i^s, \tag{8}$$

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 [11], i.e. by multiplying the original sequence by the Reed-Muller matrix $RM_v$

$$\{a_i\} = T \cdot RM_v, \quad T = \{a_i\} \cdot RM_v, \tag{9}$$

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

$$RM_0 = [1], \quad RM_v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes RM_{v-1} = \begin{bmatrix} RM_{v-1} & 0 \\ RM_{v-1} & RM_{v-1} \end{bmatrix}, \tag{10}$$

where $\otimes$ is the Kronecker product.

**Definition 5 [11].** 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, $x_0$, $x_1$, $x_2$, $x_3$ on the basis of which corresponding affine codewords can be formed.

For example, we can represent as the ANF obtained from the PBA bent-sequence (7)

$$B_1 = x_3 x_4 + x_1 x_2 . \tag{11}$$

It is known [8] that 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. 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.

In this paper, through numerous experiments, the following statement was established:

**Proposition 2.** Let $H_0$ to be PBA of order $N = 4$, and $T_0$ to be the sequence obtained by concatenating its rows (columns). Then the sequences $T_0, T_1, ..., T_{2^{k+1}-1}$ obtained by adding to the ANF sequences one or several affine terms construct, by line-by-line (column) filling, a set of matrices $H_0, H_1, ..., H_{2^{k+1}-1}$ that are also PBA.

Note that the **Proposition 2** is valid only for PBA of order $N = 4$, and fully corresponds to **Proposition 1**, in terms of structure. However, **Proposition 2** makes it easy to establish the interconnection between the generating PBA represented as their ANF (which contain affine terms) and the corresponding generating bent-sequences. We present all 28 generating bent-sequences, among which 12 (in bold font) generates affine non-equivalent classes of PBA of cardinality 32 PBA in each one, corresponding to **Proposition 2**

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

## 4 Interrelation Between the Class of Bent-Sequences of Length $n = 64$ and the Class of Perfect Binary Arrays of Order $N = 8$

In the general case, the problem of synthesizing a complete class of PBA of order $N = 8$ is computationally complex and has not been solved yet. Significant progress in the construction of PBA classes was made in [4], where a method for synthesizing the PBA class based on the classes of thinned matrices was proposed and the constructions for their reproduction and superposition were found.

The results of [4] are based on the following proposition:

**Proposition 3 [3].** The PBA $H_0(N)$ of the arbitrary order $N$ can always be represented as an interleaving ($\cup$) of its thinned matrices

$$H_0(N) = \|h_{i,j}\| = \|a_{i,j}\| \cup \|b_{i,j}\| \cup \|c_{i,j}\| \cup \|d_{i,j}\| = \\ = A_0(N/2) \cup B_0(N/2) \cup C_0(N/2) \cup D_0(N/2), \tag{13}$$

where $\|a_{i,j}\| = h_{2i,2j}$, $\|b_{i,j}\| = h_{2i,2j+1}$, $\|c_{i,j}\| = h_{2i+1,2j}$, $\|d_{i,j}\| = h_{2i+1,2j+1}$ are the corresponding thinned matrices, $i, j = 0,1,...,N/2-1$, and the indices $h_{i,j}$ vary within the limits $i, j = 0,1,...,N-1$.

Each PBA can be represented as (13). In the general case, the set of various structures of thinned matrices obtained by thinning the full class of PBA, we denote as

$$\left.\begin{matrix} \{A_i(N/2)\}; & \{B_j(N/2)\}; & \{C_\mu(N/2)\}; & \{D_\nu(N/2)\}; \\ i = 1,2,...,\psi_A; & j = 1,2,...,\psi_B; & \mu = 1,2,...,\psi_C; & \nu = 1,2,...,\psi_D \end{matrix}\right\}, \tag{14}$$

where the parameters $\psi_A$, $\psi_B$, $\psi_C$, $\psi_D$ are the number of different structures (degrees of freedom) of the corresponding thinned matrices $A, B, C, D$ of order $N/2$.

Different matrix structures from (14) can be obtained by using the cyclic shift operations in rows and columns, inversion, transposition, and mirroring of the set of generating matrices.

In [4], such a set of thinned matrices was obtained, the structures of which are presented in Table 1.

**Table 1.** The known set of thinned matrices of order $N/2 = 8/2$

| Thinned matrix | 2DPACF | Thinned matrix | 2DPACF |
|---|---|---|---|
| $A = \begin{bmatrix} - & + & - & + \\ + & + & + & + \\ - & + & - & + \\ + & + & + & + \end{bmatrix}$ | $R_A = \begin{bmatrix} 16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ | $B = \begin{bmatrix} + & + & - & - \\ - & + & + & - \\ + & + & - & - \\ - & + & + & - \end{bmatrix}$ | $R_B = \begin{bmatrix} 16 & 0 & -16 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & -16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ |
| $C = \begin{bmatrix} - & + & - & + \\ + & + & + & + \\ + & - & + & - \\ - & - & - & - \end{bmatrix}$ | $R_C = \begin{bmatrix} 16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ -16 & 0 & -16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ | $D = \begin{bmatrix} + & + & - & - \\ + & + & - & - \\ - & - & + & + \\ - & - & + & + \end{bmatrix}$ | $R_D = \begin{bmatrix} 16 & 0 & -16 & 0 \\ 0 & 0 & 0 & 0 \\ -16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ |
| $A_0 = \begin{bmatrix} - & - & - & - \\ + & + & + & + \\ + & + & + & + \\ + & + & + & + \end{bmatrix}$ | $R_{A0} = \begin{bmatrix} 16 & 16 & 16 & 16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ | $E_0 = \begin{bmatrix} - & + & - & + \\ - & + & - & + \\ - & + & - & + \\ + & - & + & - \end{bmatrix}$ | $R_{E_0} = \begin{bmatrix} 16 & -16 & 16 & -16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ |
| $A_1 = \begin{bmatrix} - & + & + & + \\ - & + & + & + \\ - & + & + & + \\ - & + & + & + \end{bmatrix}$ | $R_{A_1} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \end{bmatrix}$ | $E_1 = \begin{bmatrix} - & - & - & + \\ + & + & + & - \\ - & - & - & + \\ + & + & + & - \end{bmatrix}$ | $R_{E_1} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ -16 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ -16 & 0 & 0 & 0 \end{bmatrix}$ |
| $A_2 = \begin{bmatrix} - & + & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & - \end{bmatrix}$ | $R_{A_2} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}$ | $E_2 = \begin{bmatrix} - & - & - & + \\ - & + & + & + \\ - & + & - & - \\ + & + & - & + \end{bmatrix}$ | $R_{E_2} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & -16 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & -16 \end{bmatrix}$ |

| | | | |
|---|---|---|---|
| $A_3 = \begin{bmatrix} + & + & + & - \\ + & + & - & + \\ + & - & + & + \\ - & + & + & + \end{bmatrix}$ | $R_{A_3} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \\ 0 & 0 & 16 & 0 \\ 0 & 16 & 0 & 0 \end{bmatrix}$ | $E_3 = \begin{bmatrix} + & + & - & + \\ - & + & - & - \\ - & + & + & + \\ - & - & - & + \end{bmatrix}$ | $R_{E_3} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & -16 \\ 0 & 0 & 16 & 0 \\ 0 & -16 & 0 & 0 \end{bmatrix}$ |
| $A_4 = \begin{bmatrix} - & + & - & + \\ + & + & + & + \\ + & - & + & - \\ + & + & + & + \end{bmatrix}$ | $R_{A_4} = \begin{bmatrix} 16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 16 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ | $E_4 = \begin{bmatrix} - & - & - & - \\ - & + & - & + \\ + & + & + & + \\ - & + & - & + \end{bmatrix}$ | $R_{E_4} = \begin{bmatrix} 16 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -16 & 0 & -16 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ |
| $A_5 = \begin{bmatrix} - & + & + & + \\ + & + & - & + \\ - & + & + & + \\ + & + & - & + \end{bmatrix}$ | $R_{A_5} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \end{bmatrix}$ | $E_5 = \begin{bmatrix} - & - & - & + \\ + & - & + & + \\ - & - & - & + \\ + & - & + & + \end{bmatrix}$ | $R_{E_5} = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & -16 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & -16 & 0 \end{bmatrix}$ |

As a result, the PBA class of cardinality $J_{PBA8\times8} = 688\,128$ was built, which increased the lower bound estimation of the cardinality of PBA class of order $N = 8$ in factor of 7 compared to the previous result obtained in [12].

It is known, that all the representatives of PBA class of the order $N = 4$, when concatenating the PBA rows (columns) generates bent-sequences. The research carried out in this paper allowed us to establish that there are just $J'_{PBA8\times8,bent} = 98\,304$ representatives in the PBA class of order $N = 8$ (synthesized in [4]) that forms the bent-sequences of length $n = 64$ when concatenating their rows (columns).

At the same time, the other $688\,128 - 98\,304 = 589\,824$ PBA (when concatenating rows or columns) have non-uniform Walsh-Hadamard transform coefficients (absolute values). In order to classify these spectral coefficients, it is most convenient to use the definition of the elementary structure of the Walsh-Hadamard transform coefficients [13].

**Definition 6 [13].** The elementary structure of the vector $W(\omega)$ of Walsh-Hadamard transform coefficients is the set of absolute values of its spectral components.

It was established experimentally that all remaining 589 824 PBA, on the basis of which it is impossible to form bent-sequences by applying the operation of concatenation of their rows (columns), according to **Definition 6**, have an elementary structure $\{0(12), 8(48), 16(4)\}$.

This notation of the elementary structure should be understood as follows: the number in front of the parentheses characterizes the absolute value of the Walsh-Hadamard transform coefficient, whereas the number in parentheses indicates how many times it occurs in the vector of the Walsh-Hadamard transform coefficients.

Let us consider, for example, one of these PBA, as well as its 2DPACF

$$H_{8\times 8}=\begin{bmatrix} - & - & - & - & - & + & - & + \\ + & - & - & - & - & - & + & - \\ - & - & + & + & - & + & + & - \\ - & - & + & + & + & - & - & + \\ - & - & - & - & - & + & - & + \\ - & + & + & + & + & + & - & + \\ - & - & + & + & - & + & + & - \\ + & + & - & - & - & + & + & - \end{bmatrix},\quad R=\begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{15}$$

Applying the concatenation of the rows (columns) of PBA (15), we obtain a binary sequence and, according to **Definition 2**, corresponding to it vector of Walsh-Hadamard transform coefficients, which has an elementary structure $\{0(12), 8(48), 16(4)\}$

$$\begin{aligned} T=\{&-----+-++-----+---++-++--++--+-\\ &-----+-+-++++++-+--++-++-++--++--+-\}; \\ W_T=\{&-8\ -8\ -8\ -8\ -8\ \ 8\ -8\ \ 8\ -8\ -8\ -8\ -8\ -8\ \ 8\ -8\ \ 8\\ &-8\ -8\ \ 8\ \ 8\ -8\ \ 8\ \ 8\ -8\ -8\ -8\ \ 8\ \ 8\ -8\ \ 8\ \ 8\ -8\\ &-8\ \ 8\ -8\ \ 8\ \ 0\ \ 0\ \ 0\ \ 0\ \ 8\ -8\ \ 8\ -8\ \ 0\ \ 0\ \ 0\ \ 0\\ &-8\ \ 8\ \ 8\ -8\ \ 0\ \ 0\ 16\ 16\ \ 8\ -8\ -8\ \ 8\ \ 0\ \ 0\ -16\ -16\}. \end{aligned} \tag{16}$$

The research performed in this paper shows that establishing the interrelation between the class of PBA of order $N=8$ and the class of bent-sequences of length $n=64$ can significantly increase the lower bound of the number of PBA due to their new structures, that exist in the class of bent-sequences.

Note that, in the general case, the problem of synthesizing bent-sequences of length $n=64$ is a complex computational problem, coupled with the enumeration of a set of $J=2^{64}=18\,446\,744\,073\,709\,551\,616$ elements. Nevertheless, the theory of bent-squares that was proposed in [14], with the help of which it was possible to synthesize the full set of bent-sequences of length $n=64$ which have the cardinality $J_{bent\,64}=5\,425\,430\,528$.

We established that within this set there is a set of PBA of cardinality $J_{sdr-bent\,64}=2\,326\,528$ in which, of course, we found as a subset of $J'_{PBA8\times 8,bent}=98\,304$ PBA, that was constructed in [4].

As an example, we present one of the PBA and it's 2DPACF, that was found in the bent-sequences of the length $n=64$ class and is not member of set of PBA synthesized in [4]

$$H_8=\begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & - & + & - & - & + & - & + \\ + & - & - & + & + & - & - & + \\ + & + & - & - & - & - & + & + \\ + & - & + & - & + & - & + & - \\ - & + & + & - & + & - & - & + \end{bmatrix},\ R=\begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{17}$$

We concatenate the PBA (17) rows, as a result of which we obtain the following sequence and its Walsh-Hadamard transform coefficients in accordance with (4)

$$B=[+++++++++++++----++--++--+-+--+-+-- \\ +--++--++++----++++-+-+-+--++-+--+]; \\ W_B=[8\ 8\ 8\ 8\ 8\ 8\ 8-8\ 8\ 8\ 8\ 8-8-8-8 \\ 8\ 8-8-8\ 8\ 8-8\ 8\ 8\ 8-8-8\ 8-8\ 8-8-8-8 \\ 8-8\ 8-8\ 8\ 8-8\ 8\ 8-8\ 8-8-8-8\ 8-8\ 8 \\ 8-8-8\ 8-8-8-8\ 8\ 8\ 8-8-8-8\ 8\ 8\ 8], \tag{18}$$

which proves that (18) is indeed a bent-sequence.

Note that PBA (17) consists of thinned matrices presented in Table. 2. These structures of thinned matrices differ from the matrices presented in Table 1. This fact shows that there are exist other structures of thinned matrices that differ from those found in [4].

**Table 2.** Thinned matrices of PBA (17)

| Thinned matrix | 2DPACF | Thinned matrix | 2DPACF |
|---|---|---|---|
| $A'=\begin{bmatrix}+&+&+&+\\+&-&+&-\\+&-&+&-\\+&+&+&+\end{bmatrix}$ | $R_{A'}=\begin{bmatrix}16&0&16&0\\8&0&8&0\\0&0&0&0\\8&0&8&0\end{bmatrix}$ | $B'=\begin{bmatrix}+&+&+&+\\+&-&+&-\\-&+&-&+\\-&-&-&-\end{bmatrix}$ | $R_{B'}=\begin{bmatrix}16&0&16&0\\-8&0&-8&0\\0&0&0&0\\-8&0&-8&0\end{bmatrix}$ |
| $C'=\begin{bmatrix}+&+&-&-\\+&+&-&-\\+&-&-&+\\-&+&+&-\end{bmatrix}$ | $R_{C'}=\begin{bmatrix}16&0&-16&0\\0&-8&0&8\\0&0&0&0\\0&8&0&-8\end{bmatrix}$ | $D'=\begin{bmatrix}+&+&-&-\\-&-&+&+\\+&-&-&+\\+&-&-&+\end{bmatrix}$ | $R_{D'}=\begin{bmatrix}16&0&-16&0\\0&8&0&-8\\0&0&0&0\\0&-8&0&8\end{bmatrix}$ |

Thus, the discovering of the interrelation between the class of PBA of order $N=8$ and bent-sequences of length $n=64$ allows us to improve the estimation of the lower bound of the cardinality of PBA class of order $N=8$. Summarizing, it was established that in [4], the PBA class that produces the bent-sequences has cardinality $J'_{PBA8\times8,bent}=98\,304$, as well as PBA class that does not produce bent-sequences by concatenating rows (columns) has cardinality $J'_{PBA8\times8,nonbent}=589\,824$. In this paper, it is clarified that the full class of bent-sequences of length $n=64$ includes the PBA class of cardinality $J_{PBA8\times8,bent}=2\,326\,528$. Thereby, the cardinality of class of all the known PBA is

$$J_{PBA8\times8}\geq 589\,824+2\,326\,528=2\,916\,352, \tag{19}$$

which is larger by a factor of $\sim 4.2$ compared to the estimation in [4].

## 5 Conclusion

We note the main results obtained in the paper:

1. The lower bound estimation for the cardinality of the class of the PBA of order $N=8$ is improved. In particular, it has been established that the cardinality of the

PBA class of order $N = 8$ is not less than $J_{PBA8\times8} \geq 589\,824 + 2\,326\,528 = 2\,916\,352$ that is a factor of $\sim 4.2$ greater than the known estimation.

2. The total cardinality of the PBA class of order $N = 8$, which are producing the bent-sequences of length $n = 64$ by concatenating the rows (columns), is established and equal to $J_{PBA8\times8,bent} = 2\,326\,528$. It is shown that the existence of new structures of thinned matrices, which differ from the previously known ones, are possible.
3. The interrelation between the PBA class of order $N = 4$ and bent-sequences of length $n = 16$ is established. In particular, 12 ANF polynomials of bent-sequences that produce the full PBA class of order $N = 4$, are presented.

It should be noted that the search for new structures of thinned matrices, as well as the rules for their interleaving for formal enumeration of the PBA full class that generates bent-sequences, is an actual direction for further research. The number of PBA, which generate sequences with other (different from the bent-sequences) elementary structures of the Walsh-Hadamard transform vectors also remains unknown and can be the actual direction for further research.

## References


1. Mazurkov M.I., Chechelnytskyi, V.Y., Murr P. Information security method based on perfect binary arrays. Radioelectronics and Communications Systems, vol. 51, no. 11, pp. 612-614. doi:10.3103/s0735272708110095 (2008)
2. Baranov P.Y., Mazurkov M.I., Chechelnytskyi V.Y., Yakovenko A.A. Family of two-dimensional correcting codes on a basis of perfect binary array. Radioelectronics and Communications Systems, vol. 52, no. 9, pp. 501-506. doi:10.3103/s0735272709090088 (2009)
3. Mazurkov M.I. Broadband radio communication systems. Science and Technology, p. 340. (2010)
4. Chechelnytskyi, V. Y. A method for generation of the full class of perfect binary arrays of the order N = 8x8. Radioelectronics and Communications Systems vol. 48, no. 11 pp. 48-52. doi:10.3103/S0735272705110087 (2005)
5. Rothaus, O.S. On “bent” functions. J. Comb. Theory Ser. A., USA: Academic Press Inc, no. 20(3), pp. 300—305. doi:10.1016/0097-3165(76)90024-8 (1976)
6. Tokareva N. Bent Functions: Results and Applications to Cryptography. Academic Press, p. 220. (2015)
7. Mazurkov M.I., Sokolov A.V. The regular rules of constructing the complete class of bent-sequences of length 16. Proceedings of ONPU, no. 2(41), pp. 231-237 (2013)
8. Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui. A novel algorithm enumerating bent functions. Discrete Mathematics, vol. 308, issue 23, pp. 5576–5584. doi:10.1016/j.disc.2007.10.024 (2008)
9. Sokolov, A.V. Synthesis method of a complete class of bent-functions of six variables. Problems of physics, mathematics and technics, no. 4(29), pp. 94-102 (2016)
10. Jedwab J., Mithell C. Constructing new perfect binary arrays. Electronics Letters, vol. 24, no. 11, pp. 650-652. doi:10.1049/el:19880440 (1988)
11. Logachev O.A., Salnikov A.A., Yashchenko V.V. Boolean Functions in Coding Theory and Cryptography, Amer Mathematical Society, p. 334 (2012)

12. Mazurkov M. I., Chechelnitsky V.Ya. Classes of equivalent and generating perfect binary arrays for CDMA technologies. Proceedings of the universities. Radioelectronics, vol. 46, no. 5, pp. 54–63 (2003)
13. Sokolov A.V., Barabanov N.A. Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes. Radioelectronics and Communications Systems, vol. 58, no. 5, pp. 220-227. doi:10.3103/s0735272715050040 (2015)
14. 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, pp. 121—135 (2002)