REGULAR SYNTHESIS METHOD OF THE SEQUENCES OF LENGTH $N = 24$ WITH OPTIMAL PAPR OF WALSH-HADAMARD SPECTRUM

A.V. Sokolov

Abstract — The paper is devoted to the development of regular method of synthesis of sequences of length $N=24$ with an optimal Peak-to-Average Power Ratio (PAPR) of Walsh-Hadamard spectrum on the basis of spectral rectangles. The range distribution of the PAPR of Walsh-Hadamard spectrum for full code of the length $N=24$ is determined. The synthesized sequences can be applied in MC-CDMA technologies.

Index Terms — Peak-to-average power ratio, Multi-code code division multiple access, Walsh-Hadamard transform.

I. INTRODUCTION

Active use of the technology of Multi-code code division multiple access (MC-CDMA) in modern communications systems makes it an actual task of further researches. The key objects in MC-CDMA technology which determines its effectiveness are the orthogonal functions that are used in the system. The most frequently used functions are discrete Walsh functions [1]. In the MC-CDMA systems binary data vector $b=(b_i),\ i=\overline{0,N-1}$ is subjected to orthogonal transform. Each data bit b_i changes the sign of one of the orthogonal functions of discrete time, and the output is the sum of N modulated functions $h_i(t)$, then the transmitted signal is a Walsh-Hadamard transformant of the binary sequences b

$$S_b(t)=\sum_{i=0}^{N-1} b_i h_i(t). \tag{1}$$

It is clear that use of Walsh-Hadamard transformation coefficients as a signal gives rise to such significant lack of MC-CDMA systems as high PAPR [2]

$$\kappa = {P_{\max}}\big/{P_{av}} = \frac{1}{N}\max_t\left\{\left|S_b(t)\right|^2\right\}. \tag{2}$$

where $P_{\max}$ — peak power of $S_b(t)$ signal;

P_{av} — average power of signal $S_b(t)$;

N — length of signal $S_b(t)$.

The problem of reducing of the PAPR of used in the MC-CDMA technology signals got its decision in [2] through the use of C-code based on bent-sequences.

Nevertheless, the existence of bent-sequences is possible only if length of signals is equal to $N=2^{2k}, k\in\mathbf{N}$ [3], while modern communication systems require a greater value of flexibility and scalability of the number of users. Thus, an actual task is to research the possibility of using other lengths of signals in particular $N=12\cdot 2^k$.

The purpose of this article is to build a regular method of synthesis of optimal C-code with codeword length $N=12\cdot 2^k$.

II. Constructing of Hadamard matrices of order 24

For the construction of Hadamard matrices of the order L aliquot to 12 the Paley construction is commonly used, which is based on a Jacobsthal matrix [4]. To construct the Jacobsthal matrix in the field $GF(q)$ we use the character $\chi(a)$, showing whether the element a is a perfect square of some other element of the field b. Thus,

$$\begin{cases} \chi(0)=0, \\ \chi(a)=1, \quad \text{if} \quad \text{exists} \quad b \in GF(q) \mid a=b^2 \\ \chi(a)=-1, \quad \text{if} \quad b \in GF(q) \mid a=b^2 \text{ does not exist} \end{cases} \tag{3}$$

Jacobsthal matrix Q is a matrix, elements of which have row index μ, column index ν and value $\chi(\mu-\nu)$.

We construct a Jacobsthal matrix for the field $GF(11)$

$$Q=\begin{bmatrix} 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}. \tag{4}$$

In accordance with the Paley construction [4] on the basis of the Jacobsthal matrix the Hadamard matrix of order $L=q+1=12$ can be built by the rule

$$H=E+\begin{bmatrix} 0 & \alpha^T \\ \alpha & Q \end{bmatrix}, \tag{5}$$

where α is a column vector of length q, consisting of -1;

E — diagonal matrix of order $q+1$.

Applying (5) to the Jacobsthal matrix (4) we obtain the Hadamard matrix of order 12

$$H_{12}^{'}=\begin{bmatrix} +-----------\\ ++-+---+++-+\\ +++-+---+++-\\ +-++-+---+++\\ ++-++-+---++\\ +++-++-+---+\\ ++++-++-+---\\ +-+++-++-+--\\ +--+++-++-+-\\ +---+++-++-+\\ ++---+++-++-\\ +-+---+++-++ \end{bmatrix}. \tag{6}$$

Multiplying the matrix (6) on its first line we receive the canonical form of Hadamard matrix of order 12

$$H_{12}=\begin{bmatrix}
+&+&+&+&+&+&+&+&+&+&+&+\\
+&-&+&-&+&+&+&-&-&-&+&-\\
+&-&-&+&-&+&+&+&-&-&-&+\\
+&+&-&-&+&-&+&+&+&-&-&-\\
+&-&+&-&-&+&-&+&+&+&-&-\\
+&-&-&+&-&-&+&-&+&+&+&-\\
+&-&-&-&+&-&-&+&-&+&+&+\\
+&+&-&-&-&+&-&-&+&-&+&+\\
+&+&+&-&-&-&+&-&-&+&-&+\\
+&+&+&+&-&-&-&+&-&-&+&-\\
+&-&+&+&+&-&-&-&+&-&-&+\\
+&+&-&+&+&+&-&-&-&+&-&-
\end{bmatrix}. \tag{7}$$

Note, that as well as for Hadamard matrix of order $L=2^k, k\in\mathbf{N}$ to the Hadamard matrix (7) Sylvester construction is applicable to increase recurrently its order [5]

$$H_{12n}=\begin{bmatrix} H_{12(n-1)} & H_{12(n-1)} \\ H_{12(n-1)} & -H_{12(n-1)} \end{bmatrix}, \tag{8}$$

wherein as the source matrix H_{12} is used the constructed by the Paley construction matrix (7). For example, it is easy to construct the Hadamard matrix of order $L=24$

$$H_{24}=\begin{bmatrix}
+&+\\
+&-&+&-&+&+&+&-&-&-&+&-&+&-&+&-&+&+&+&-&-&-&+&-\\
+&-&-&+&-&+&+&+&-&-&-&+&+&-&-&+&-&+&+&+&-&-&-&+\\
+&+&-&-&+&-&+&+&+&-&-&-&+&+&-&-&+&-&+&+&+&-&-&-\\
+&-&+&-&-&+&-&+&+&+&-&-&+&-&+&-&-&+&-&+&+&+&-&-\\
+&-&-&+&-&-&+&-&+&+&+&-&+&-&-&+&-&-&+&-&+&+&+&-\\
+&-&-&-&+&-&-&+&-&+&+&+&+&-&-&-&+&-&-&+&-&+&+&+\\
+&+&-&-&-&+&-&-&+&-&+&+&+&+&-&-&-&+&-&-&+&-&+&+\\
+&+&+&-&-&-&+&-&-&+&-&+&+&+&+&-&-&-&+&-&-&+&-&+\\
+&+&+&+&-&-&-&+&-&-&+&-&+&+&+&+&-&-&-&+&-&-&+&-\\
+&-&+&+&+&-&-&-&+&-&-&+&+&-&+&+&+&-&-&-&+&-&-&+\\
+&+&-&+&+&+&-&-&-&+&-&-&+&+&-&+&+&+&-&-&-&+&-&-\\
+&+&+&+&+&+&+&+&+&+&+&+&-&-&-&-&-&-&-&-&-&-&-&-\\
+&-&+&-&+&+&+&-&-&-&+&-&-&+&-&+&-&-&-&+&+&+&-&+\\
+&-&-&+&-&+&+&+&-&-&-&+&-&+&+&-&+&-&-&-&+&+&+&-\\
+&+&-&-&+&-&+&+&+&-&-&-&-&-&+&+&-&+&-&-&-&+&+&+\\
+&-&+&-&-&+&-&+&+&+&-&-&-&+&-&+&+&-&+&-&-&-&+&+\\
+&-&-&+&-&-&+&-&+&+&+&-&-&+&+&-&+&+&-&+&-&-&-&+\\
+&-&-&-&+&-&-&+&-&+&+&+&-&+&+&+&-&+&+&-&+&-&-&-\\
+&+&-&-&-&+&-&-&+&-&+&+&-&-&+&+&+&-&+&+&-&+&-&-\\
+&+&+&-&-&-&+&-&-&+&-&+&-&-&-&+&+&+&-&+&+&-&+&-\\
+&+&+&+&-&-&-&+&-&-&+&-&-&-&-&-&+&+&+&-&+&+&-&+\\
+&-&+&+&+&-&-&-&+&-&-&+&-&+&-&-&-&+&+&+&-&+&+&-\\
+&+&-&+&+&+&-&-&-&+&-&-&-&-&+&-&-&-&+&+&+&-&+&+
\end{bmatrix}. \tag{9}$$

The matrix H_{24} may be used as the basic signal system for use in MC-CDMA technology. Each row of the matrix (9) may be a unique code assigned to each of 24 users $b_1, b_2, ..., b_{24}$ working in the communication system, whilst in turn each user will code his transmitted information by positive or inversed line of matrix (9). Suppose for example, at some point of discrete time t, each user were transmitting the following information bits

$$I(t)=\{b_i\}=\begin{bmatrix}
\underset{-}{b_1} & \underset{-}{b_2} & \underset{+}{b_3} & \underset{-}{b_4} & \underset{+}{b_5} & \underset{+}{b_6} & \underset{-}{b_7} & \underset{+}{b_8} & \underset{+}{b_9} & \underset{+}{b_{10}} & \underset{-}{b_{11}} & \underset{-}{b_{12}} \\
\underset{+}{b_{13}} & \underset{+}{b_{14}} & \underset{-}{b_{15}} & \underset{+}{b_{16}} & \underset{-}{b_{17}} & \underset{-}{b_{18}} & \underset{+}{b_{19}} & \underset{-}{b_{20}} & \underset{-}{b_{21}} & \underset{-}{b_{22}} & \underset{+}{b_{23}} & \underset{+}{b_{24}}
\end{bmatrix}. \tag{10}$$

Obviously, the resulting signal in accordance with (1) will be the product of

$$S_b(t)=I(t)\cdot H_{24}=[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ {-24}\ 0\ 0\ 0\ 0\ 0\ 0]. \tag{11}$$

In accordance with (2) the PAPR of this signal would be $\kappa = 24^2/24 = 24$, such a signal is difficult and inconvenient for transmission and leads to irrational use of transmitter power and a large non-linear distortion in communication systems with MC-CDMA.

The solution to this problem can be found by use of the C-code, with the fixed value of the PAPR of each individual codeword. Fig. 1 shows the scheme of C-code use.

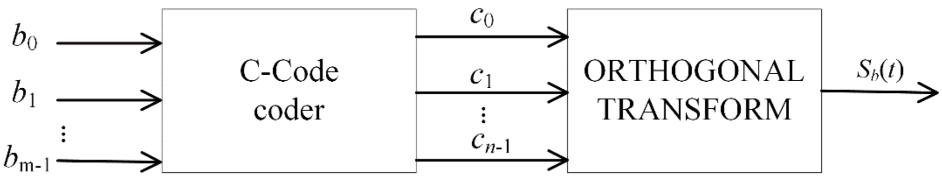

Fig. 1 The scheme of C-code use in MC-CDMA system before orthogonal transform

It is obvious that C-code codewords c_i of length n must have the lowest PAPR value among all the codewords of length n.

III. C-CODE SYNTHESIS METHOD

To find the optimal, in terms of the PAPR signals, we will connect to the input of the orthogonal transformation (9) to the full set of $J = 2^{24}$ codewords, and define values of PAPR for each of them. The results are shown in Table I, where J — the number of sequences of length $N = 24$, which have a given value of the PAPR κ.

TABLE I
Distribution of values of the PAPR for sequences of length $N = 24$

κ	1.5	2.6667	4.17	6	8.17
J	7040	2409088	6243072	5456176	2040192
κ	10.7	13.5	16.7	20.17	24
J	510048	97152	13248	1152	48

It is clear that from the point of view of practical application in MC-CDMA technology of greatest interest are sequences having a minimum value of PAPR, if the case of length of it $N = 24$, which $\kappa = 1.5$ are called the optimal coding sequences (OCS).

For example, consider the sequence A6C260 represented in hexadecimal form, which can be easily represented in binary and exponential form.

$$\begin{aligned} S_1 &= \mathrm{A6C260} = [1010011011000001001100000] = \\ &= [-+-++--+--++++-++--+++++]. \end{aligned} \tag{12}$$

Multiplying this sequence to obtained Hadamard matrix H_{24} (9) we can get its Walsh-Hadamard spectrum

$$W = S_1 H_{24} = [6\,6\,6\,{-6}\,6\,6\,6\,{-6}\,{-6}\,6\,{-6}\,{-6}\,{-6}\,{-6}\,{-6}\,{-6}\,{-2}\,2\,2\,{-2}\,{-2}\,2\,{-2}\,{-2}\,{-2}], \tag{13}$$

so, its PAPR is really equal to $\kappa = 6^2/24 = 1.5$, and this sequence is optimal.

An important task is the development of regular rules for constructing a full class of OCS of length $N = 24$.

In this paragraph we are introducing a regular method of construction of a full class of OCS of length $N = 24$ having a PAPR $\kappa = 1.5$.

This article offers another representation of optimal sequences in the form of spectral rectangles, which can be defined similarly to Agievich bent rectangles [6]

$$R = \begin{bmatrix} S(1,2,\ldots 12)\cdot H_{12} \\ S(13,14,\ldots,24)\cdot H_{12} \end{bmatrix}. \tag{13}$$

Thus, the sequence (12) can be matched to a spectral rectangle

$$R = \begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ 6 & 6 & 6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \end{bmatrix}. \tag{14}$$

As we can see from the rectangle (14), it consists of three columns of type $[0 \quad 6]^T$ and 9 columns of type $[4 \quad 2]^T$, form where T — denotes transposition. Thus, the total number of possible permutations of columns in the spectral rectangle (14) is defined as the number of combinations $C_{12}^{3} = 12!/(3!\cdot 9!) = 220$. Table II shows the hexadecimal equivalents of optimal sequences corresponding to this 220 spectral rectangles.

TABLE II

Full class of forming OCS

A6C260	E1C418	A8D085	C124B2	A212A3	A09259	F66765	831439	E6E65E	C42546
CA54A0	C6A428	D89409	8FE4FA	C6F4E7	87F27D	813313	90A51A	AF32DB	8DF1CF
BC12C0	D51510	CB2412	A886A8	B6B66B	944354	E5D755	D9759B	CBD4DD	D3E43F
873062	9CC188	82F00B	BB37B2	A50652	DD93D9	AC03C1	BD95D9	C1861C	C05417
9AA0A2	F82580	E61441	F2E7AA	ECD6CB	B973D5	9F51FC	B7C73C	88528D	89809B
D46442	C4D04C	EC4604	9605E0	8834C3	D57177	82C0BC	FE17A9	ECB6CD	ED64D7
F30620	D94094	A59209	AAF2EE	826626	9BB17B	CC04D8	9AF5AD	9BE39E	E73637
E0B602	978058	C17405	B762F6	CBB6AB	BCD36D	EB66BC	EDA79A	FF07D4	AEE2AF
A96282	B0E20C	B62302	F9A6DA	AF56E5	AF6376	F8D79C	894594	B6D3CD	CA04A5
CD84C0	A35214	D2C504	DEC6EC	D80782	E6B36B	B10398	C09589	A7D07F	BD5397
936130	EA8288	9B1181	CD76D6	BCE7C6	825165	D5E5DC	CFA0FE	80B02F	D9B597
E52250	8E60C4	FD47F0	84A2CA	F537C3	862073	B9E1BE	81605E	930136	906187
DE0160	E26026	8B02F0	E046C4	BEA3F8	A14235	F7257A	A6026C	DAD1AF	A9F61F
C39031	ACA04A	B02362	8C40E6	858178	B2F337	D0452C	B5B35E	BE31E7	E0260B
8D5051	8BC02C	ADB2F3	C2846A	9811B1	FB23B3	C3F53E	FC63CE	CE746F	84C44D
AA3221	987106	E37673	E5E66E	D6D579	9FC1F5	8A21AA	9881CC	DDC55E	F3971B
B98310	D1A10A	C41661	F65766	F1B739	EF8679	EEC5EC	9CF0DF	94114B	977557
F05301	B54144	D7A772	BF83EA	E20730	FC3753	EAB4BB	BB92BD	F0F54F	DEA5CB
94B141	B13013	9E73E3	DB65E6	ABD3B9	B5E35B	CDD4BD	A82296	FAA72E	D4F70F
89B098	965025	FA97E1	DF14F3	CF35F1	D10551	DE65B6	E1F29F	B3732F	B01705
B29128	85E016	E796F8	F876A7	F3C37C	DB5735	97B1BB	8510D5	D7956D	F9C78D
AF00B0	CC3083	DCB5EA	EBC6B6	EE52F5	928329	F355B5	F5565D	A0C30E	EA7787

Obviously, all the sequences in Table II have an optimal PAPR $\kappa = 1.5$. Based on (13) similar to (14) all the $J = 220$ forming OCS may be represented as spectral rectangles. They are the basis for building a complete class of OCS of length $N = 24$ based on the rules of reproduction of spectral rectangles.

Rule 1. The elements in the second line of the spectral rectangle (14) equal to $R_{2,j} = 6$ may be encoded in a four ways

$$Z = \begin{bmatrix} \{+++\}, & \{-+-\}, \\ \{--+\}, & \{+--\}, \end{bmatrix}. \tag{15}$$

Thus, using the Rule 1 based on (14) we obtain 3 new spectral rectangles, each of which defines a sequence with a PAPR $\kappa = 1.5$

$$\begin{bmatrix} \begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ 6 & 6 & 6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \end{bmatrix}; \\ \begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ -6 & 6 & -6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \end{bmatrix}; \\ \begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ -6 & -6 & 6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \end{bmatrix}; \\ \begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ 6 & -6 & -6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \end{bmatrix}. \end{bmatrix} \quad (16)$$

Rule 2. The second line of the spectral rectangle can be taken both in the positive and in the negative.

For example, a spectral rectangle (14) can be used to construct one more new spectral rectangle

$$\begin{bmatrix} 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \\ -6 & -6 & -6 & 2 & -2 & -2 & 2 & 2 & -2 & 2 & 2 & 2 \end{bmatrix}. \quad (17)$$

Rule 3. All the spectral rectangles can be taken both in the positive and in the negative.

For example, the inverse spectral rectangle (14) has the form

$$\begin{bmatrix} 0 & 0 & 0 & 4 & -4 & -4 & 4 & 4 & -4 & 4 & 4 & 4 \\ -6 & -6 & -6 & 2 & -2 & -2 & 2 & 2 & -2 & 2 & 2 & 2 \end{bmatrix}. \quad (18)$$

Rule 4. Rows of the spectral rectangle can be swapped.

Thus, on the basis of spectral rectangle (14), we obtain a new spectral rectangle

$$\begin{bmatrix} 6 & 6 & 6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 & -2 \\ 0 & 0 & 0 & -4 & 4 & 4 & -4 & -4 & 4 & -4 & -4 & -4 \end{bmatrix}. \quad (19)$$

Thus, combining Rules 1...4, and the forming OCS given in Table II we can get a full class of OCS of length $N = 24$ and cardinal number

$$J = 220 \cdot 4 \cdot 2 \cdot 2 \cdot 2 = 7040. \quad (20)$$

Research made with a brute force method validates the results.

Conclusion

1. We have investigated the distribution of possible values of the PAPR of the Walsh-Hadamard spectrum of sequences of length $N = 24$.

2. We introduced a new representation as a spectral rectangle of optimal sequences with a minimum PAPR.

3. We proposed a regular synthesis method of a C-code of length of it’s codewords $N = 24$ which can be used to decrease the PAPR in the MC-CDMA technology.

REFERENCES

1. K.G. Paterson "On codes with low peak-to-average power ratio for multicode CDMA" HP Laboratories Technical Report HPL-2001-115, May 2001.
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. Rothaus O.S. "On “bent” functions" J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976, №20(3), P.300—305.
4. Paley, R.E.A.C. "On orthogonal matrices". Journal of Mathematics and Physics 12: 311–320, 1933.
5. Sokolov, A.V. Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion. Radioelectronics and Communications Systems, vol. 56, no. 8, pp. 415-423.
6. 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.
7. Agievich, S.V. "Bent Rectangles", Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007).Amsterdam: IOS Press. — 2008.— p. 3—22.

Artem V. Sokolov was born in Odessa, USSR, in 1990. He received a Bachelor (Hons) degree in systems of technical data protection in 2011, Master (Hons) degree in systems of technical data protection and automation of it’s processing in 2013 and Ph.D. degree in data protection systems in 2014 from Odessa National Polytechnic University, Odessa, Ukraine.

From 2012 to 2014 he was a Junior Researcher of Data Security department in Odessa National Polytechnic University. Since 2014 he has been a senior lecturer of Data Security department in Odessa National Polytechnic University. He is the author of a book and more than 30 articles. His research interests include data protection methods based on perfect algebraic constructions, nonlinear S-box synthesis methods and stream encryption algorithms.

A.V. Sokolov awards and honors include Gold medal for high achievements in education, Hons Diploma of Winner in Master Competition, 2013; winner of "Information and communication networks" Ukrainian competition of research papers, 2012; Diploma for excellent academic and research activities, 2010.