MANY-PARAMETER M-COMPLEMENTARY GOLAY SEQUENCES AND TRANSFORMS

V.G. Labunets [1], V.P. Chasovskikh [1], Ju.G. Smetanin [2], E. Ostheimer [3]
[1] Ural State Forest Engineering University, Sibirskiy trakt, 37, Ekaterinburg, Russia, 620100,
[2] Federal Research Center "Information and Control" of the RAS, Vavilov street 44 |(2), Moscow, Russia, 119333,
[3] Capricat LLC, Pompano Beach, Florida, USA

Abstract

In this paper, we develop the family of Golay–Rudin–Shapiro (GRS) m-complementary many-parameter sequences and many-parameter Golay transforms. The approach is based on a new generalized iteration generating construction, associated with n unitary many-parameter transforms and n arbitrary groups of given fixed order. We are going to use multi-parameter Golay transform in Intelligent-OFDM-TCS instead of discrete Fourier transform in order to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects.

Keywords: complementary sequences, many-parameter orthogonal transforms, fast algorithms, OFDM systems.

Citation: Labunets VG, Chasovskikh VP, Smetanin JuG, Ostheimer E. Many-parameter *m*-complementary Golay sequences and transforms. Computer Optics 2018; 42(6): 1074-1082. DOI: 10.18287/2412-6179-2018-42-6-1074-1082.

Acknowledgments: This work was supported by grants the RFBR № 17-07-00886 and by Ural State Forest Engineering's Center of Excellence in "Quantum and Classical Information Technologies for Remote Sensing Systems".

Introduction

Binary ± 1-valued *Golay – Rudin – Shapiro* sequences (2-GRSS) associated with the cyclic group $\mathbf{Z}_2^n$ were introduced independently by Golay [1, 2, 3] in 1949-1951, Shapiro [4, 5] and Rudin [6] in 1951.M.J.E.Golay [2] introduced the general concept of "complementary pairs" of finite sequences all of whose entries are ± 1. For building the classical FGRST in bases of classical 2-GRSS the following actors are used: 1) Abelian group $\mathbf{Z}_2$, 2) 2-point Fourier transform $\mathcal{F}_2$, and 3) complex field $\mathbf{C}$, *i.e.,* these transforms are associated with the triple $(\mathbf{Z}_2, \mathcal{F}_2, \mathbf{C})$.

In previous papers [7, 8], we have shown a new unified approach to the $\mathbf{GF}(p)$ -, or Clifford-valued complementary sequences and Golay transforms. It was associated not with the triple $(\mathbf{Z}_2, \mathcal{F}_2, \mathbf{C})$, but with triples

$$(\mathbf{Z}_2\ , \{\mathcal{CS}_2^1(\varphi_1,\alpha_1,\gamma_1), \mathcal{CS}_2^2(\varphi_2,\alpha_2,\gamma_2),..., \mathcal{CS}_n^1(\varphi_n,\alpha_n,\gamma_n)\}, \mathcal{A}lg)$$

and $\left(\mathbf{Z}_2, \mathcal{CS}_2(\varphi,\alpha,\gamma), \mathcal{A}lg\right)$, where $\{\mathcal{CS}_2^1(\varphi_1,\alpha_1,\gamma_1), \mathcal{CS}_2^2(\varphi_2,\alpha_2,\gamma_2),...,\mathcal{CS}_n^1(\varphi_n,\alpha_n,\gamma_n)\}$ is a set of arbitrary unitary(2×2) -transforms of type

$$\mathcal{CS}_2(\varphi_k,\alpha_k,\gamma_k) = \begin{bmatrix} e^{i\alpha_k}\cos\varphi_k & e^{i\gamma_k}\sin\varphi_k \\ e^{-i\gamma_k}\sin\varphi_k & -e^{-i\alpha_k}\cos\varphi_k \end{bmatrix},$$

$$k = 1,...,n,$$

and $\mathcal{CS}_2(\varphi,\alpha,\gamma)$ is a single transform, $\mathcal{A}lg$ is an algebra (for example, Clifford algebra).

In this work, we develop a new unified approach to the so-called generalized multi-parameter $m-$ complementary sequences. This construction has a rich algebraic structure. It is associated not with the triple $\left(\mathbf{Z}_2, \mathcal{F}_2, \mathbf{C}\right)$, but with

1) $\left(\mathbf{Z}_m, \mathbf{U}_m, \mathcal{A}lg\right)$, 2) $\left(\mathbf{Z}_m, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$,

3) $\left(\mathbf{Gr}_m, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$,

4) $\left(\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2,...,\mathbf{Gr}_m^n\right\}, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$.

where $\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2,...,\mathbf{Gr}_m^n\right\}$ is a set of arbitrary finite groups of given order m Here $\left\{\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n\right\}$ is a set of arbitrary unitary (m×m) – transforms represented in the many-parameter Jacobi-Euler form [9 – 10]:

$$\mathbf{U}_m^1 = \mathbf{U}_m^1(\varphi_0^1,\varphi_1^1,...,\varphi_q^1) = \mathbf{U}_m^1(\boldsymbol{\varphi}_q^1) = \prod_{r=1}^{m-1}\prod_{s=r+1}^{m}\mathbf{J}(\varphi_{r,s}^1),$$

$$\mathbf{U}_m^2 = \mathbf{U}_m^2(\varphi_0^2,\varphi_1^2,...,\varphi_q^2) = \mathbf{U}_m^2(\boldsymbol{\varphi}_q^2) = \prod_{r=1}^{m-1}\prod_{s=r+1}^{m}\mathbf{J}(\varphi_{r,s}^2),$$

...,

$$\mathbf{U}_m^n = \mathbf{U}_m^n(\varphi_0^n,\varphi_1^n,...,\varphi_q^n) = \mathbf{U}_m^n(\boldsymbol{\varphi}_q^n) = \prod_{r=1}^{m-1}\prod_{s=r+1}^{m}\mathbf{J}(\varphi_{r,s}^n),$$

where

$$\mathbf{J}(\varphi_{r,s}) = \begin{array}{c} \\ \\ \\ r \\ \\ s \\ \\ \\ \end{array} \begin{array}{c} \qquad\qquad r \qquad\qquad\qquad s \qquad\qquad \\ \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & c(\varphi_{r,s}) & \cdots & s(\varphi_{r,s}) & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & s(\varphi_{r,s}) & \cdots & -c(\varphi_{r,s}) & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array},$$

is the Jacobi orthonormal rotation with reflection, $\boldsymbol{\varphi}_q^1 = (\varphi_0^1,\varphi_1^1,...,\varphi_q^1),...,\boldsymbol{\varphi}_q^n = (\varphi_0^n,\varphi_1^n,...,\varphi_q^n)$ are the Jacobi parameters, $q = C_m^2 = m(m-1)/2$, $c(\varphi_{r,s}) = \cos(\varphi_{r,s})$, $s(\varphi_{r,s}) = \sin(\varphi_{r,s})$.

The rest of the paper is organized as follows: in Section 2, the object of the study (*Golay – Rudin – Shapiro* m-ary sequences) is described. In Section 3 we propose method based on new generalized iteration rule with n unitary (m×m)-transforms $\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n$ and single group $\mathbf{Z}_m$. Then we generalize the previously method on n unitary (m×m)-transforms $\mathbf{U}_m^1, \mathbf{U}_m^2,...,\mathbf{U}_m^n$ and on n finite groups $\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2,...,\mathbf{Gr}_m^n\right\}$. In Section 5 we derive fast algorithms for binary Golay transforms.

The object of the study.
New iteration construction for original Golay sequences

We begin by describing the original Golay m-complementary sequences.

Definition 1. *A generalization of the Golay complementary pair, known as the Golay m-Complementary m-element Set (m-*GCS*) of complex-valued sequences* [11]

$$
m\text{-GCS}=\begin{cases}\mathrm{com}_0(t)\ :=\ \left(c_0(0),\ \ c_0(1),\ ...,\ c_0(m-1)\right),\\ \mathrm{com}_1(t)\ :=\ \left(c_1(0),\ \ c_1(1),\ ...,\ c_1(m-1)\right),\\ \text{...},\\ \mathrm{com}_{m-1}(t):=\left(c_{m-1}(0),c_{m-1}(1),...,c_{m-1}(m-1)\right)\end{cases}
$$

is defined by $\sum\limits_{k=0}^{m-1}COR_k(\tau)=m\cdot\delta(\tau),\ \sum\limits_{k=0}^{m-1}\left|\mathrm{COM}_1(z)\right|^2=m,$ where $\left\{COR_k(\tau)\right\}_{k=0}^{m-1}$ are the periodic autocorrelation functions of $\left\{\mathrm{com}_k(t)\right\}_{k=1}^{m}$ and $\mathrm{COM}_k(z)=\mathcal{Z}\left\{\mathrm{com}_k(t)\right\}$ are their $\mathcal{Z}$ – transforms.

We use two symbols $\boldsymbol{\alpha}_n\in[0,m^{n-1}-1]=\mathbf{Z}_{m^n}$ and $\mathbf{t}_n\in[0,m^{n-1}-1]=\mathbf{Z}_{m^n}$ for numeration of Golay sequences and discrete time, respectively. For integer $\boldsymbol{\alpha}_n\in[0,m^{n-1}-1]=\mathbf{Z}_{m^n}$ and $\mathbf{t}_n\in[0,m^{n-1}-1]=\mathbf{Z}_{m^n}$ we shall use m-arycodes $\vec{\boldsymbol{\alpha}}_n=\left(\alpha_1,\alpha_2,...,\alpha_n\right)$, $\vec{\mathbf{t}}_n=\left(t_1,t_2,...,t_n\right)$, where $\alpha_i t_i\in\{0,1,\ldots,m-1\}=\mathbf{Z}_m$, $i=1,2,\ldots,n$.

Let $\vec{\boldsymbol{\alpha}}_n=\left(\alpha_1,\alpha_2,...,\alpha_n\right)$ *and* $\vec{\mathbf{t}}_n=\left(t_1,t_2,...,t_n\right)$ *be* m-*ary codes, then define*

$$
\boldsymbol{\alpha}_n=\left|\vec{\boldsymbol{\alpha}}_n\right|=\sum_{i=1}^{n}\alpha_{n-i+1}m^{i-1},\ \text{and}\ \mathbf{t}_n=\ \left|\vec{\mathbf{t}}_n\right|=\sum_{i=1}^{n}t_{n-i+1}m^{n-i}
$$

as integers whose m-ary codes are $\vec{\boldsymbol{\alpha}}_n=\left(\alpha_1,\alpha_2,...,\alpha_n\right)$ and $\vec{\mathbf{t}}_n=\left(t_1,t_2,...,t_n\right)$, where α_n, t_1 are less significant bits (LSB) and α_1, t_n are most significant bits (MSB) of $\vec{\boldsymbol{\alpha}}_n=\left(\alpha_1,\alpha_2,...,\alpha_n\right)$ and $\vec{\mathbf{t}}_n=\left(t_1,t_2,...,t_n\right)$, respectively. Obviously,

$$
\begin{array}{ll}
\vec{\boldsymbol{\alpha}}_1=(\alpha_1)\in\mathbf{Z}_m, & \boldsymbol{\alpha}_1=\alpha_1\in\mathbf{Z}_m,\\
\vec{\boldsymbol{\alpha}}_2=\left(\vec{\boldsymbol{\alpha}}_1,\alpha_2\right)\in\mathbf{Z}_m\times\mathbf{Z}_m=\mathbf{Z}_m^2, & \left(\boldsymbol{\alpha}_1,\alpha_2\right)\in\mathbf{Z}_m\times\mathbf{Z}_m,\\
\vec{\boldsymbol{\alpha}}_3=\left(\vec{\boldsymbol{\alpha}}_2,\alpha_3\right)\in\mathbf{Z}_m^2\times\mathbf{Z}_m=\mathbf{Z}_m^3, & \left(\boldsymbol{\alpha}_2,\alpha_3\right)\in\mathbf{Z}_{m^2}\times\mathbf{Z}_m,\\
\text{......................................}, & \text{...........................},\\
\vec{\boldsymbol{\alpha}}_n=\left(\vec{\boldsymbol{\alpha}}_{n-1},\alpha_n\right)\in\mathbf{Z}_m^{n-1}\times\mathbf{Z}_m=\mathbf{Z}_m^n, & \left(\boldsymbol{\alpha}_{n-1},\alpha_n\right)\in\mathbf{Z}^1_{m^{n-1}}\times\mathbf{Z}_m;\\
\vec{\mathbf{t}}_1=\left(t_1\right)\in\mathbf{Z}_m, & \mathbf{t}_1=t_1\in\mathbf{Z}_m,\\
\vec{\mathbf{t}}_2=\left(\vec{\mathbf{t}}_1,t_2\right)\in\mathbf{Z}_m\times\mathbf{Z}_m=\mathbf{Z}_m^2, & \left(\mathbf{t}_1,t_2\right)\in\mathbf{Z}_m\times\mathbf{Z}_m,\\
\vec{\mathbf{t}}_3=\left(\vec{\mathbf{t}}_2,t_3\right)\in\mathbf{Z}_m^2\times\mathbf{Z}_m=\mathbf{Z}_m^3, & \left(\mathbf{t}_2,t_3\right)\in\mathbf{Z}_{m^2}\times\mathbf{Z}_m,\\
\text{...}, & \text{...........................},\\
\vec{\mathbf{t}}_n=\left(\vec{\mathbf{t}}_{n-1},t_n\right)\in\mathbf{Z}_m^{n-1}\times\mathbf{Z}_m=\mathbf{Z}_m^n, & \left(\mathbf{t}_{n-1},t_n\right)\in\mathbf{Z}_{m^{n-1}}\times\mathbf{Z}_m.
\end{array}
$$

Let $\left\{\mathrm{com}^{[n+1]}_{\boldsymbol{\alpha}_{n+1}}(\mathbf{t}_{n+1})\right\}$ be m^{n+1}-element set of m complementary sequences (of length m^{n+1}), where $\boldsymbol{\alpha}_{n+1},\mathbf{t}_{n+1}=0,1,..,m^{n+1}-1$ They form rows of a $(m^{n+1}\times m^{n+1})$ -matrix $\mathbf{G}^{[n+1]}_{m^{n+1}}=\left[\mathrm{com}^{[n+1]}_{\boldsymbol{\alpha}_{n+1}}(\mathbf{t}_{n+1})\right]^{m^{n+1}-1}_{\boldsymbol{\alpha}_{n+1},\mathbf{t}_{n+1}=0}$, that is called *the m-Golay matrix.* Here index $[n+1]$ shows that Golay matrix have been obtained on the $n+1$ iteration step. We are going to group these rows (sequences) as

$$
\mathbf{G}^{[n+1]}_{m^{n+1}}=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n+1}=0}^{m^{n+1}-1}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n+1})}(\mathbf{t}_{n+1})=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n}=0}^{m^{n}-1}\left(\mathop{\boxplus}_{\alpha_{n+1}=0}^{m-1}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,\alpha_{n+1})}(\mathbf{t}_{n+1})\right)=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n}=0}^{m^{n}-1}\begin{bmatrix}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,1)}(\mathbf{t}_{n+1})\\ ...\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,m-1)}(\mathbf{t}_{n+1})\end{bmatrix}. \quad (1)
$$

Let us to select the more fine structure of the m-Golay matrix:

$$
\mathbf{G}^{[n+1]}_{m^{n+1}}=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n+1}=0}^{m^{n+1}-1}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n+1})}(\mathbf{t}_{n+1})=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n}=\mathbf{0}}^{\mathbf{m^n}\text{-}\mathbf{1}}\begin{bmatrix}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,1)}(\mathbf{t}_{n+1})\\ \text{....................}\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,m-1)}(\mathbf{t}_{n+1})\end{bmatrix}=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n-1}=0}^{m^{n-1}\text{-}1}\left(\mathop{\boxplus}_{\alpha_{n}=0}^{m\text{-}1}\begin{bmatrix}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n1)}(\mathbf{t}_{n+1})\\ \text{.....................}\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_nm-1)}(\mathbf{t}_{n+1})\end{bmatrix}\right)=\mathop{\boxplus}_{\boldsymbol{\alpha}_{n-1}=0}^{m^{n-1}\text{-}1}\left[\begin{array}{c}\mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},0,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},0,1)}(\mathbf{t}_{n+1})\\ ...\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},0,m-1)}(\mathbf{t}_{n+1})\\ \hline \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},1,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},1,1)}(\mathbf{t}_{n+1})\\ ...\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},1,m-1)}(\mathbf{t}_{n+1})\\ \hline \vdots\\ \vdots\\ \hline \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},m-1,0)}(\mathbf{t}_{n+1})\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},m-11)}(\mathbf{t}_{n+1})\\ ...\\ \mathrm{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},m-1m-1)}(\mathbf{t}_{n+1})\end{array}\right]. \quad (2)
$$

Example 1. For $n=1$ and $n=2$ we have, respectively,

$$\mathbf{G}_{3^1}^{[1]}=\left[\mathrm{com}_{\boldsymbol{\alpha}_1}^{[1]}(\mathbf{t}_1)\right]_{\boldsymbol{\alpha}_1,\mathbf{t}_1=0}^{2}=\boxplus_{\boldsymbol{\alpha}_1=0}^{2}\mathrm{com}_{\boldsymbol{\alpha}_1}^{[1]}(\mathbf{t}_1)=\begin{bmatrix}\mathrm{com}_{(0)}^{[1]}(\mathbf{t}_1)\\ \mathrm{com}_{(1)}^{[1]}(\mathbf{t}_1)\\ \mathrm{com}_{(2)}^{[1]}(\mathbf{t}_1)\end{bmatrix},$$

$$\mathbf{G}_{3^2}^{[2]}=\boxplus_{\boldsymbol{\alpha}_1=0}^{2}\begin{bmatrix}\mathrm{com}_{(\boldsymbol{\alpha}_1,0)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(\boldsymbol{\alpha}_1,1)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(\boldsymbol{\alpha}_1,2)}^{[2]}(\mathbf{t}_2)\end{bmatrix}=\begin{bmatrix}\mathrm{com}_{(0,0)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(0,1)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(0,2)}^{[2]}(\mathbf{t}_2)\\ \hline \mathrm{com}_{(1,0)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(1,1)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(1,2)}^{[2]}(\mathbf{t}_2)\\ \hline \mathrm{com}_{(2,0)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(2,1)}^{[2]}(\mathbf{t}_2)\\ \mathrm{com}_{(2,2)}(\mathbf{t}_2)\end{bmatrix}. \square$$

The matrix $\mathbf{G}_{m^{n+1}}^{[n+1]}$ is constructed by an iteration construction. The initial matrix $\mathbf{G}_{m^1}^{[1]}$ is formed by starting with an arbitrary unitary $(m\times m)$-matrix (in many-parameter form or not)

$$\mathbf{U}_m=\left[A_\alpha(t)\right]:=\mathbf{G}_{m^1}^{[1]}=\begin{bmatrix}\mathrm{com}_0^{[1]}(\mathbf{t}_1)\\ \mathrm{com}_1^{[1]}(\mathbf{t}_1)\\ \ldots\ldots\ldots\ldots\\ \mathrm{com}_{m-1}^{[1]}(\mathbf{t}_1)\end{bmatrix}=$$

$$=\begin{bmatrix}A_0(0) & A_0(1) & A_0(2) & \ldots & A_0(m-1)\\ A_1(0) & A_1(1) & A_1(2) & \ldots & A_1(m-1)\\ A_2(0) & A_2(1) & A_2(2) & \ldots & A_2(m-1)\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ A_{m-1}(0) & A_{m-1}(1) & A_{m-1}(2) & \ldots & A_{m-1}(m-1)\end{bmatrix},$$

where $A_\alpha(t)\in\mathcal{A}lg$,

$\mathrm{com}_\alpha^{[1]}(t)=\left(A_\alpha(0),\,A_\alpha(1),\ldots,\,A_\alpha(m-1)\right)$.

Example 2. The initial matrix $\mathbf{G}_{m^1}^{[1]}$ can be the Fourier transform on Abelian group $\mathbf{Z}_m$:

$$\mathbf{G}_{m^1}^{[1]}=\begin{bmatrix}\mathrm{com}_0^{[1]}(\mathbf{t}_1)\\ \mathrm{com}_1^{[1]}(\mathbf{t}_1)\\ \mathrm{com}_2^{[1]}(\mathbf{t}_1)\\ \ldots\ldots\ldots\ldots\\ \mathrm{com}_{m-1}^{[1]}(\mathbf{t}_1)\end{bmatrix}= \qquad (3)$$

$$=\begin{bmatrix}1 & 1 & 1 & \ldots & 1\\ 1 & \varepsilon^{1\cdot1} & \varepsilon^{1\cdot2} & \ldots & \varepsilon^{1\cdot(m-1)}\\ 1 & \varepsilon^{2\cdot1} & \varepsilon^{2\cdot2} & \ldots & \varepsilon^{2\cdot(m-1)}\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ 1 & \varepsilon^{(m-1)\cdot1} & \varepsilon^{(m-1)\cdot2} & \ldots & \varepsilon^{(m-1)\cdot(m-1)}\end{bmatrix},$$

where $\varepsilon_m=\sqrt[m]{1}\in\mathcal{A}lg$, $\mathrm{com}_k^{[1]}(\mathbf{t})=\left(1,\varepsilon^{k\cdot1},\varepsilon^{k\cdot2},\ldots,\varepsilon^{k\cdot(m-1)}\right)$, $(k=0,1,\ldots,m-1)$ are characters $\mathbf{Z}_m$. $\square$

It is easy to check that

$$\left(\left|\mathrm{COM}_0(z)\right|^2+\left|\mathrm{COM}_1(z)\right|^2+\ldots+\left|\mathrm{COM}_{m-1}(z)\right|^2\right)_{|z|=1}=m.$$

Indeed,

$$\sum_{k=1}^{m-1}\left|\mathrm{COM}_k(z)\right|^2=\sum_{k=1}^{m-1}\mathrm{COM}_k(z)\overline{\mathrm{COM}}^k(\overline{z})=$$
$$=\sum_{k=1}^{m-1}\left(\sum_{t=0}^{m-1}a_k(t)z^t\right)\left(\sum_{s=0}^{m-1}\overline{a}_k(s)\overline{z}^s\right)=$$
$$=\sum_{s=0}^{m-1}\sum_{t=0}^{m-1}\left(\sum_{k=0}^{m-1}a_k(t)\overline{a}_k(s)\right)z^t\overline{z}^s=\sum_{s=0}^{m-1}\sum_{t=0}^{m-1}\delta_{t-s}z^t\overline{z}^s=\sum_{t=0}^{m-1}|z|^{2t},$$

since $\sum_{k=0}^{m-1}a_k(t)\overline{a}_k(s)=\delta_{t-s}$ is true for an arbitrary unitary (orthogonal) matrix. Hence,

$$\left(\sum_{k=1}^{m-1}\left|\mathrm{COM}_k(z)\right|^2\right)\Bigg|_{|z|=1}=\left(\sum_{t=0}^{m-1}|z|^{2t}\right)_{|z|=1}=m$$

and initial sequences in the form of rows of an unitary matrix (in particular case, in the form of characters $\mathrm{com}_k(\mathbf{t}_1)=(1,\varepsilon^{k\cdot1},\varepsilon^{k\cdot2},\ldots,\varepsilon^{k\cdot(m-1)})$ of cyclic group $\mathbf{Z}_m$) are the Golay m-complementary sequences.

Methods

The matrix $\mathbf{G}_{m^{n+1}}^{[n+1]}$ is constructed by an iteration construction

$$\mathbf{G}_{m^1}^{[1]}(\mathbf{U}_m^1)\xrightarrow{\mathbf{U}_m^2}\mathbf{G}_{m^2}^{[2]}(\mathbf{U}_m^1,\mathbf{U}_m^2)\xrightarrow{\mathbf{U}_m^3}\ldots\xrightarrow{\mathbf{U}_m^{n+1}}\mathbf{G}_{m^{n+1}}^{[n+1]}(\mathbf{U}_m^1,\ldots,\mathbf{U}_m^n,\mathbf{U}_m^{n+1}), \quad (4)$$

where

$$\mathcal{U}_{n+1}:=\left\{\mathbf{U}_m^1,\ldots,\mathbf{U}_m^n,\mathbf{U}_m^{n+1}\right\}=\left\{\mathcal{U}_n,\mathbf{U}_m^{n+1}\right\},$$
$$\mathcal{U}_n:=\left\{\mathbf{U}_m^1,\ldots,\mathbf{U}_m^n\right\}.$$

Here $\mathbf{U}_m^s(\boldsymbol{\varphi}_q^s)=\left[A_\alpha^s(t\mid\boldsymbol{\varphi}_q^s)\right]_{\alpha,t=0}^{m-1}\in SU(\mathcal{A}lg,m)$ $(s=1,2,\ldots,n)$ are a sequence of unitary many-parameter $(m\times m)$ -transforms, belonging to the special unitary group $SU(\mathcal{A}lg,m)$, where $s=1,2,\ldots,n+1$ and $A_\alpha^s(t\mid\boldsymbol{\varphi}_q^s)$ are $\mathcal{A}lg$-valued many-parameter sequences.

Let us assume that we have m-Golay matrix $\mathbf{G}_{m^n}^{[n]}(\mathbf{U}_1,\ldots,\mathbf{U}_n)=\mathbf{G}_{m^n}^{[n]}(\mathcal{U}_n)$ (depending on n previous transforms $\mathbf{U}_m^1,\ldots,\mathbf{U}_m^n$). We need to construct the next m-Golay matrix $\mathbf{G}_{m^{n+1}}^{[n+1]}(\mathbf{U}_m^1,\ldots,\mathbf{U}_m^{n+1})=\mathbf{G}_{m^{n+1}}^{[n+1]}(\mathcal{U}_{n+1})$ using only $\mathbf{G}_{m^n}^{[n]}(\mathbf{U}_m^1,\ldots,\mathbf{U}_m^n)$ and $\mathbf{U}_m^{n+1}$. We are going to use for m-Golay matrix $\mathbf{G}_{m^n}^{[n]}(\mathcal{U}_n)$ the same structure as in (1):

$$\mathbf{G}_{m^n}^{[n]}(\mathcal{U}_n)=\boxplus_{\boldsymbol{\alpha}_n=0}^{m^n-1}\mathrm{com}_{(\boldsymbol{\alpha}_n)}^{[n]}(\mathbf{t}_n\mid\mathcal{U}_n)=$$
$$=\boxplus_{\boldsymbol{\alpha}_n=\mathbf{0}}^{\mathbf{m^n-1}}\begin{bmatrix}\mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \ldots\ldots\ldots\ldots\\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},m-1)}^{[n]}(\mathbf{t}_n\mid\mathcal{U}_n)\end{bmatrix}. \qquad (5)$$

For constructing $\mathbf{G}_{m^{n+1}}^{[n+1]}(\mathcal{U}_{n+1})$ from $\mathbf{G}_{m^n}^{[n]}(\mathcal{U}_n)$ we take each complementary set in the form

$$m\text{-GCS}^{[n]}\left(\mathcal{U}_n\right)=\begin{bmatrix}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},0)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},1)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \dots\dots\dots\dots\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},m-1)}(\mathbf{t}_n\mid\mathcal{U}_n)\end{bmatrix}$$

and construct m shifted versa of their components

$$m\text{-GCS}^{[n]}\left(\mathcal{U}_n\right)\rightarrow\begin{array}{l}\nearrow\ m\text{-GCS}^{[n]}_{\alpha_n=0}\left(\mathcal{U}_{n+1}\right),\\ \quad m\text{-GCS}^{[n]}_{\alpha_n=1}\left(\mathcal{U}_{n+1}\right),\\ \quad\dots\dots\dots\\ \searrow\ m\text{-GCS}^{[n]}_{\alpha_n=m-1}\left(\mathcal{U}_{n+1}\right),\end{array}$$

where

$$m\text{-GCS}^{[n]}_{\alpha_n}\left(\mathcal{U}_{n+1}\right)=\mathbf{U}^{n+1}_m\left(\mathbf{P}^{\alpha_n}_m\begin{bmatrix}\mathbf{I}_{\mathbf{t}_n}&&&\\&\mathbf{T}^{1\cdot m^n}_{\mathbf{t}_n}&&\\&&\ddots&\\&&&\mathbf{T}^{(m-1)\cdot m^n}_{\mathbf{t}_n}\end{bmatrix}\tilde{\mathbf{P}}^{\alpha_n}_m\right)\times$$
$$\times\begin{bmatrix}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},0)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},1)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \dots\dots\dots\dots\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},m-1)}(\mathbf{t}_n\mid\mathcal{U}_n)\end{bmatrix}\equiv\begin{bmatrix}\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,0)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\\ \text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,1)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\\ \dots\dots\dots\dots\\ \text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,m-1)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\end{bmatrix}. \quad (6)$$

Here $\alpha_n=0,1,\dots,m-1$, $\mathbf{P}^{\alpha_n}_m$ is the cyclic permutation operator on α_n positions (modulo m), $\mathbf{T}^{\mathbf{m}^{\mathbf{n}}s}_{\mathbf{t}_n}$ is the shift operator on $m^n s$ positions $\mathbf{T}^{m^n s}_{\mathbf{t}_n}f(\mathbf{t}_n):=f(\mathbf{t}_n+m^n\,\text{s})$, $\tilde{\mathbf{P}}_m$ is transposed matrix of $\mathbf{P}_m$.

According to (1) we obtain

$$\mathbf{G}^{[n+1]}_{m^{n+1}}(\mathcal{U}_{n+1})=\boxplus_{\alpha_n=0}^{m^n\text{-}1}\begin{bmatrix}\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,0)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\\ \text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,1)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\\ \dots\dots\dots\dots\\ \text{com}^{[n+1]}_{(\boldsymbol{\alpha}_n,m-1)}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})\end{bmatrix}=$$
$$=\boxplus_{\alpha_n=0}^{m^n\text{-}1}\mathbf{U}^{n+1}_m\cdot\left(\mathbf{P}^{\alpha_n}_m\cdot\begin{bmatrix}\mathbf{I}_{\mathbf{t}_n}&&&\\&\mathbf{T}^{1\cdot m^n}_{\mathbf{t}_n}&&\\&&\ddots&\\&&&\mathbf{T}^{(m-1)\cdot m^n}_{\mathbf{t}_n}\end{bmatrix}\cdot\tilde{\mathbf{P}}^{\alpha_n}_m\right)\times \quad (7)$$
$$\times\begin{bmatrix}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},0)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},1)}(\mathbf{t}_n\mid\mathcal{U}_n)\\ \dots\dots\dots\dots\\ \text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},m-1)}(\mathbf{t}_n\mid\mathcal{U}_n)\end{bmatrix},$$

and, consequently,

$$\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})=$$
$$=\sum_{\beta_n=0}^{m-1}a^{n+1}_{\alpha_{n+1}}(\beta_n)\mathbf{T}^{\mathbf{m}^{\mathbf{n}}(\beta_n\oplus\alpha_n)}_{\mathbf{t}_n}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},\beta_n)}(\mathbf{t}_n\mid\mathcal{U}_n).$$

Since $\mathbf{t}_{n+1}=(\mathbf{t}_n,t_{n+1})$, then believing $t_{n+1}=\alpha_n\underset{m}{\oplus}\beta_n$, we obtain:

$$\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})=\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_n,t_{n+1}\mid\mathcal{U}_{n+1})=$$
$$=\sum_{t_{n+1}=0}^{m-1}A^{n+1}_{\alpha_{n+1}}(\alpha_n\underset{m}{\oplus}t_{n+1})\mathbf{T}^{m^n t_{n+1}}_{\mathbf{t}_n}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n\underset{m}{\oplus}t_{n+1})}(\mathbf{t}_n\mid\mathcal{U}_n)= \quad (8)$$
$$=\sum_{t_{n+1}=0}^{m-1}A^{n+1}_{\alpha_{n+1}}(\alpha_n\underset{m}{\oplus}t_{n+1})\mathbf{T}^{m^n t_{n+1}}_{\mathbf{t}_n}\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n\underset{m}{\oplus}t_{n+1})}(\mathbf{t}_n+m^n t_{n+1}\mid\mathcal{U}_n).$$

So,

$$\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_n,t_{n+1}\mid\mathcal{U}_{n+1})=$$
$$=A^{n+1}_{\alpha_{n+1}}(\alpha_n\underset{m}{\oplus}t_{n+1})\cdot\text{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n\underset{m}{\oplus}t_{n+1})}(\mathbf{t}_n\mid\mathcal{U}_n). \quad (9)$$

It is finally recurrent relation between m-complementary sequences of $\mathbf{G}^{[n+1]}_{m^{n+1}}\left[\mathcal{U}_{n+1}\right]$ and $\mathbf{G}^{[n]}_{m^n}\left[\mathcal{U}_n\right]$. From (9) we obtain expression for $\text{com}^{[n+1]}_{\vec{\boldsymbol{\alpha}}_{n+1}}(\mathbf{t}_{n+1}\mid\mathcal{U}_{n+1})$:

$$\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n+1})}(\mathbf{t}_{n+1})=\prod_{s=1}^{n}A^{s+1}_{\alpha_{s+1}\underset{m}{\oplus}t_{s+2}}(\alpha_s\underset{m}{\oplus}t_{s+1}),\quad\alpha_0,t_{n+2}\equiv0. \quad (10)$$

In particular, for matrices in the form of the Fourier transform $\mathbf{U}^1_m=\mathbf{U}^2_m=\dots=\mathbf{U}^n_m=[\varepsilon^{\alpha t}_m]$ we have

$$\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_{n+1})=\text{com}^{[n+1]}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}(\mathbf{t}_n,t_{n+1})=$$
$$=\varepsilon_m^{\sum_{s=1}^{n}(\alpha_s\underset{m}{\oplus}t_{s+1})\left(\alpha_{s+1}\underset{m}{\oplus}t_{s+2}\right)}. \quad (11)$$

Where $\alpha_0,t_{n+2}\equiv0$. New sequences in (9) are orthogonal and m-complementary sequences.

Generalizations

In this section, we introduce generalized m-complementary sequences. It is based on using new permutation matrices $\mathbf{P}^{\alpha_n}_m$ in (7). The mappings g: $\mathbf{X}\to\mathbf{X}$ of a set $\mathbf{X}$ into (or onto) itself are of particular importance. They form the following set $\mathbf{X}^{\mathbf{X}}:=\{g|g:\mathbf{X}\to\mathbf{X}\}$.

Definition 2. *One-to-one map from a set* $\mathbf{X}$ *to itself* g: $\mathbf{X}\to\mathbf{X}$, $x'=g(x)=g\circ x$ *is called a transformation of the set* X.

If $\mathbf{X}$ is finite and consists of m elements (for example, $\mathbf{X}=\{0,1,2,\dots,m\}$) then a transformation of the set X is called a *permutation.* As is well known, the set of all permutations of $\mathbf{X}$ forms a group $S_m=Sum\{\mathbf{X}\}$ in which the product $\sigma\pi$ of a pair of permutations σ,π is defined by $(\sigma\pi)\circ x:=\sigma\circ(\pi\circ\text{x})$.

If $\mathbf{X}$ contains more than two elements, S_m is not commutative. Any subgroup of S_m is called a *permutation group* on $\mathbf{X}$, or a *group of permutations* of $\mathbf{X}$. We shall say that the permutations in $Sym(\text{X})$ *act* or *operate* on the elements of $\mathbf{X}$.

Definition 3. *A homomorphism of a group on a set* h*:* $\mathbf{Gr}\to Sym\{\mathbf{X}\}$ *is called a permutation representation (or realization) of .*
The image $h(\mathbf{Gr})\subset Sym\{\mathbf{X}\}$ is a permutation group and the elements of are represented as permutations of . A permutation representation is equivalent to an action of on the set : To specify an action, we need to define for element $\text{g}\in\mathbf{Gr}$ the corresponding permutation $h(g)$ of , that is, $h(g)\circ x$ for any $x\in\mathbf{X}$. We are going to write $h(g)\circ x$

in the short form $g\circ x$ and to call the group of transformations of . The pair $\langle\rangle$ is called a space with transformation group the elements $x\in\mathbf{X}$ are called points of the space .

Definition 4. *If is a permutation group of degree , then the permutation representation of is the linear permutation representation of :* $\mathbf{P}:\mathbf{Gr}\to\mathrm{GL}_m(\mathcal{A}lg)$ *which maps to the corresponding permutation matrix* $\mathbf{P}(g)$, .

That is, acts on by permuting the standard basis vectors $\{e_n\}_{n\in\mathbf{X}}\in\mathcal{A}lg^m$ such that

$$\mathbf{P}(g)e_n=e_{g\circ n}=e_{n'}\in\{e_n\}_{n\in\mathbf{X}},$$

where $\mathbf{P}(g)$'s are the operators in $\mathcal{A}lg^m$ which define the above mentioned *linear* representation.

Example 3. Let

$$\mathbf{X}=[0,1,...,m-1],\ \mathbf{Gr}=\mathbf{Z}_m=\left\langle\{0,1,...,m-1\},\underset{m}{\oplus}\right\rangle$$

be the cyclic group of order m. Then

$$\mathbf{P}(0)=\begin{bmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&1\end{bmatrix},\ \mathbf{P}(1)=\begin{bmatrix}&1&&&\\&&1&&\\&&&\ddots&\\&&&&1\\1&&&&\end{bmatrix},\ \mathbf{P}(2)=\begin{bmatrix}&&1&&\\&&&1&\\&&&&\ddots\\1&&&&\\&1&&&\end{bmatrix},...,\mathbf{P}(m-1)=\begin{bmatrix}&&&&1\\1&&&&\\&\ddots&&&\\&&&1&\\&&&&1\end{bmatrix}.$$

In particular, for $m=2$ and $m=3$we have

$$\mathbf{P}(0)=\begin{bmatrix}1&\\&1\end{bmatrix},\ \mathbf{P}(1)=\begin{bmatrix}&1\\1&\end{bmatrix};$$

$$\mathbf{P}(0)=\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\ \mathbf{P}(1)=\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix},\ \mathbf{P}(2)=\begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix}.\ \square$$

In expression (7) was used *linear* permutation representation $\mathbf{P}(g)$ of only one group . However, we can use others finite groups of given order m. Let $\mathbf{Gr}=\mathbf{Gr}_m=\{g_\alpha\}_{\alpha=0}^{m-1}$ be a group of given order m and $\{\mathbf{P}(g_\alpha)\}_{\alpha=0}^{m-1}$. Then

$$\mathbf{G}^{[n+1]}_{m^{n+1}}(\mathcal{U}_{n+1};\mathbf{Gr}_m)=\underset{\boldsymbol{\alpha}_n=0}{\overset{m^n-1}{\boxplus}}\begin{bmatrix}\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_n,0)}(\mathbf{t}_n\,|\,\mathcal{U}_{n+1};\mathbf{Gr}_m)\\\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_n,1)}(\mathbf{t}_n\,|\,\mathcal{U}_{n+1};\mathbf{Gr}_m)\\\cdots\cdots\cdots\\\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_n,m-1)}(\mathbf{t}_n\,|\,\mathcal{U}_{n+1};\mathbf{Gr}_m)\end{bmatrix}=$$

$$=\underset{\boldsymbol{\alpha}_n=0}{\overset{m^n-1}{\boxplus}}\mathbf{U}^{n+1}_m\cdot\left(\mathbf{P}_m(g_{\alpha_n})\cdot\begin{bmatrix}\mathbf{I}_{\mathbf{t}_n}&&&\\&\mathbf{T}^{1\cdot m^n}_{\mathbf{t}_n}&&\\&&\ddots&\\&&&\mathbf{T}^{(m-1)\cdot m^n}_{\mathbf{t}_n}\end{bmatrix}\cdot\tilde{\mathbf{P}}_m(g_{\alpha_n})\right)\cdot\begin{bmatrix}\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},0)}(\mathbf{t}_n\,|\,\mathcal{U}_n;\mathbf{Gr}_m)\\\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},1)}(\mathbf{t}_n\,|\,\mathcal{U}_n;\mathbf{Gr}_m)\\\cdots\cdots\cdots\\\mathrm{com}^{[n]}_{(\boldsymbol{\alpha}_{n-1},m-1)}(\mathbf{t}_n\,|\,\mathcal{U}_n;\mathbf{Gr}_m)\end{bmatrix}\qquad(12)$$

is the Golay matrix associated with triple $\left(\mathbf{Gr}_m,\{\mathbf{U}^1_m,\mathbf{U}^2_m,...,\mathbf{U}^{n+1}_m\},\mathcal{A}lg\right)$.

Example 4. For $m=4$ we have two groups: $\mathbf{Z}_4=\{0,1,2,3\}$ and $\mathbf{Z}_2\times\mathbf{Z}_2=\{(0,0),(0,1),(1,0),(1,1)\}$. For both groups we have the following permutation representations:

$$\mathbf{P}(0)=\begin{bmatrix}1&&&\\&1&&\\&&1&\\&&&1\end{bmatrix},\ \mathbf{P}(1)=\begin{bmatrix}&1&&\\&&1&\\&&&1\\1&&&\end{bmatrix},\ \mathbf{P}(2)=\begin{bmatrix}&&1&\\&&&1\\1&&&\\&1&&\end{bmatrix},\ \mathbf{P}(3)=\begin{bmatrix}&&&1\\1&&&\\&1&&\\&&1&\end{bmatrix},$$

$$\mathbf{P}(0,0)=\begin{bmatrix}1&&&\\&1&&\\&&1&\\&&&1\end{bmatrix},\ \mathbf{P}(0,1)=\begin{bmatrix}&1&&\\1&&&\\&&&1\\&&1&\end{bmatrix},\ \mathbf{P}(1,0)=\begin{bmatrix}&&1&\\&&&1\\1&&&\\&1&&\end{bmatrix},\ \mathbf{P}(1,1)=\begin{bmatrix}&&&1\\&&1&\\&1&&\\1&&&\end{bmatrix}.$$

Hence, we can construct two different set of Golay matrices associated with two triples

1) $\left(\mathbf{Z}_4,\{\mathbf{U}^1_m,\mathbf{U}^2_m,...,\mathbf{U}^{n+1}_m\},\mathcal{A}lg\right)$,

2) $\left(\mathbf{Z}_2\times\mathbf{Z}_2,\{\mathbf{U}^1_m,\mathbf{U}^2_m,...,\mathbf{U}^{n+1}_m\},\mathcal{A}lg\right)$,

respectively. □

Let $\mathcal{G}_{n+1} := \left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2, ..., \mathbf{Gr}_m^n, \mathbf{Gr}_m^{n+1}\right\} = \left\{\mathcal{G}_m^n, \mathbf{Gr}_m^{n+1}\right\}$ be a set of arbitrary groups of given order m: $\mathbf{Gr}_m^1 = \left\{g_{\alpha_1}^1\right\}_{\alpha_1=0}^{m-1}, ..., \mathbf{Gr}_m^{n+1} = \left\{g_{\alpha_{n+1}}^1\right\}_{\alpha_{n+1}=0}^{m-1}$. Then we can use on each k^{th}iteration permutation representations $\left\{\mathbf{P}_m^k(g_{\alpha_k})\right\}_{\alpha_{k=0}}^{m-1}$ for $\mathbf{Gr}_m^k$. In this case, we obtain the following Golay transform

$$\mathbf{G}_{m^{n+1}}^{[n+1]}(\mathcal{U}_{n+1};\mathcal{G}_{n+1}) = \boxplus_{\boldsymbol{\alpha}_n=0}^{m^n-1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_n,0)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_{n+1};\mathcal{G}_{n+1}) \\ \mathrm{com}_{(\boldsymbol{\alpha}_n,1)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_{n+1};\mathcal{G}_{n+1}) \\ \dots\dots\dots\dots \\ \mathrm{com}_{(\boldsymbol{\alpha}_n,m-1)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_{n+1};\mathcal{G}_{n+1}) \end{bmatrix} =$$

$$= \boxplus_{\boldsymbol{\alpha}_n=0}^{m^n-1} \mathbf{U}_m^{n+1} \cdot \left(\mathbf{P}_m^{n+1}(g_{\alpha_n}) \cdot \begin{bmatrix} \mathbf{I}_{\mathbf{t}_n} & & & \\ & \mathbf{T}_{\mathbf{t}_n}^{1\cdot m^n} & & \\ & & \ddots & \\ & & & \mathbf{T}_{\mathbf{t}_n}^{(m-1)\cdot m^n} \end{bmatrix} \cdot \tilde{\mathbf{P}}_m^{n+1}(g_{\alpha_n}) \right) \cdot \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_n;\mathcal{G}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_n;\mathcal{G}_n) \\ \dots\dots\dots\dots \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},m-1)}^{[n]}(\mathbf{t}_n \mid \mathcal{U}_n;\mathcal{G}_n) \end{bmatrix}. \quad (13)$$

It is associated with triple

$$\left(\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2, ..., \mathbf{Gr}_m^{n+1}\right\}, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2, ..., \mathbf{U}_m^{n+1}\right\}, \mathcal{A}lg\right).$$

Fast Golay transforms

Let us consider expressions (8) and (9) for $m=2$ (*i.e.,* expressions (6) and (7) from our work [7]):

$$\mathrm{com}_{(\boldsymbol{\alpha}_{n+1})}^{[n+1]}(\mathbf{t}_{n+1}) = \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}^{[n+1]}(\mathbf{t}_n, t_{n+1}) = \sum_{t_{n+1}=0}^{1} (-1)^{\left(\alpha_n \oplus_2 t_{n+1}\right)\alpha_{n+1}} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n \oplus_2 t_{n+1})}^{[n]}\left(\mathbf{t}_n + 2^n \cdot t_{n+1}\right), \quad (14)$$

$$\mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n,\alpha_{n+1})}^{[n+1]}(\mathbf{t}_n, t_{n+1}) = (-1)^{\left(\alpha_n \oplus_2 t_{n+1}\right)\alpha_{n+1}} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n \oplus_2 t_{n+1})}^{[n]} \times \left(\mathbf{t}_n\right) = (-1)^{\alpha_n\alpha_{n+1}}(-1)^{\alpha_{n+1}t_{n+1}} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n \oplus_2 t_{n+1})}^{[n]}\left(\mathbf{t}_n\right) \quad (15)$$

and find matrix representations of these expressions. We introduce the following σ-parametrized ($2^n \times 2^n$)-matrix:

$${}^{\sigma}\mathbf{G}_{2^n}^{[n]} := \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} P_2^{\sigma} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix} = \begin{cases} {}^{0}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 0, \\ {}^{1}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 1; \end{cases}$$

$$= \begin{cases} {}^{0}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} P_2^{0} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 0 \\ {}^{1}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} P_2^{1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 1 \end{cases} = \begin{cases} {}^{0}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 0, \\ {}^{1}\mathbf{G}_{2^n}^{[n]} = \boxplus_{\boldsymbol{\alpha}_n=0}^{2^n-1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \end{bmatrix}, & \sigma = 1, \end{cases}$$

and construct the direct sum of introduced matrices

$$\tilde{\mathbf{G}}_{2^{n+1}}^{[n+1]} = \bigoplus_{\sigma=0}^{1} {}^{(\sigma)}\mathbf{G}_{2^n}^{[n]} = \left[\begin{array}{c:c} {}^{(0)}\mathbf{G}_{2^n}^{[n]} & \\ \hdashline & {}^{(1)}\mathbf{G}_{2^n}^{[n]} \end{array}\right] = \left[\begin{array}{c:c} \left(\mathbf{I}_{2^{n-1}} \otimes \mathbf{P}_2^0\right)\mathbf{G}_{2^n}^{[n]} & \\ \hdashline & \left(\mathbf{I}_{2^{n-1}} \otimes \mathbf{P}_2^1\right)\mathbf{G}_{2^n}^{[n]} \end{array}\right] =$$

$$= \left[\begin{array}{c:c} \boxplus_{\boldsymbol{\alpha}_{n-1}=0}^{2^{n-1}-1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n) \end{bmatrix} & \\ \hdashline & \boxplus_{\boldsymbol{\alpha}_{n-1}=0}^{2^{n-1}-1} \begin{bmatrix} \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},1)}^{[n]}(\mathbf{t}_n + 2^n) \\ \mathrm{com}_{(\boldsymbol{\alpha}_{n-1},0)}^{[n]}(\mathbf{t}_n + 2^n) \end{bmatrix} \end{array}\right]. \quad (16)$$

From (16) we see that $\tilde{\mathbf{G}}_{2^{n+1}}^{[n+1]}$ represents $\mathrm{com}_{(\boldsymbol{\alpha}_{n-1},\alpha_n \oplus_2 t_{n+1})}^{[n]}\left(\mathbf{t}_n + 2^n \cdot t_{n+1}\right)$ in (14). It is easy to see, that

$$\tilde{\mathbf{G}}_{2^{n+1}}^{[n+1]} = \left[\begin{array}{c:c} \left[\mathbf{I}_{2^{n-1}} \otimes \mathbf{P}_2^0\right] & \\ \hdashline & \left[\mathbf{I}_{2^{n-1}} \otimes \mathbf{P}_2^1\right] \end{array}\right] \times \left[\begin{array}{c:c} \mathbf{G}_{2^n}^{[n]} & \\ \hdashline & \mathbf{G}_{2^n}^{[n]} \end{array}\right] == \left[\delta_{\alpha_{n+1}}^{(2)}(t_{n+1})\left[\mathbf{I}_{2^{n-1}} \otimes \mathbf{P}_2^{t_{n+1}}\right]\right] \times \left[\mathbf{I}_2 \otimes \mathbf{G}_{2^n}^{[n]}\right] = \mathbf{P}_2^{\{t_{n+1}\}} \cdot \left[\mathbf{I}_2 \otimes \mathbf{G}_{2^n}^{[n]}\right],$$

where

$$
\mathbf{P}_{2^{n+1}}^{\{t_{n+1}\}} := \left[\delta_{\alpha_{n+1}}^{(2)}(t_{n+1})\left[\mathbf{I}_{2^{n-1}}\otimes\mathbf{P}_2^{t_{n+1}}\right]\right] = \left[\begin{array}{c:c} \left[\mathbf{I}_{2^{n-1}}\otimes\mathbf{P}_2^{0}\right] & \\ \hdashline & \left[\mathbf{I}_{2^{n-1}}\otimes\mathbf{P}_2^{1}\right] \end{array}\right]
$$

is the permutation matrix with controlling digit $\{t_{n+1}\}$. According to (15) the Golay matrix $\mathbf{G}_{2^{n+1}}^{[n+1]}$ is the product of three matrices

$$
\begin{gathered}
\mathbf{G}_{2^{n+1}}^{[n+1]} = \Delta\left\{(-1)^{\alpha_n\alpha_{n+1}}\right\}\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}(-1)^{\alpha_{n+1}t_{n+1}}\right]\tilde{\mathbf{G}}_{2^{n+1}}^{[n+1]} = \Delta\left\{(-1)^{\alpha_n\alpha_{n+1}}\right\}\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}(-1)^{\alpha_{n+1}t_{n+1}}\right], \\
\left[\delta_{\alpha_{n+1}}^{(2)}(t_{n+1})\left[\mathbf{I}_{2^{n-1}}\otimes\mathbf{P}_2^{t_{n+1}}\right]\right]\left[\mathbf{I}_2\otimes\mathbf{G}_{2^n}^{[n]}\right] = \Delta\left\{(-1)^{\alpha_n\alpha_{n+1}}\right\}\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}(-1)^{\alpha_{n+1}t_{n+1}}\right]\mathbf{P}_{2^{n+1}}^{\{t_{n+1}\}}\left[\mathbf{I}_2\otimes\mathbf{G}_{2^n}^{[n]}\right].
\end{gathered} \tag{17}
$$

Where $\Delta\{(-1)^{\alpha_n\alpha_{n+1}}\} = \mathbf{diag}\{(-1)^{\alpha_n\alpha_{n+1}}\}$ is diagonal matrix, and $\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}(-1)^{\alpha_{n+1}t_{n+1}}\right]$ has the following structure

$$
\begin{gathered}
\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}(-1)^{\alpha_{n+1}t_{n+1}}\right] = \left[\mathbf{I}_{2^n}\otimes\begin{bmatrix}1\\1\end{bmatrix}\middle|\,\mathbf{I}_{2^n}\otimes\begin{bmatrix}1\\-1\end{bmatrix}\right] = \left[\mathbf{I}_{2^n}\,\middle|\,\mathbf{I}_{2^n}\right]\hat{\otimes}\left[\begin{array}{c|c}1 & 1\\ 1 & -1\end{array}\right] = \\
= \left[\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}\right]\otimes\begin{bmatrix}1\\1\end{bmatrix}\middle|\left[\delta_{\boldsymbol{\alpha}_n,\mathbf{t}_n}^{(2^n)}\right]\otimes\begin{bmatrix}1\\-1\end{bmatrix}\right] = \begin{array}{l} \\ \left\{\begin{array}{l} \alpha_{n+1}=0 \\ \alpha_{n+1}=1 \\ \hline \alpha_{n+1}=0 \\ \alpha_{n+1}=1 \\ \hline \alpha_{n+1}=0 \\ \alpha_{n+1}=1 \\ \hline \alpha_{n+1}=0 \\ \alpha_{n+1}=1 \end{array}\right. \end{array}
\begin{array}{c} \begin{array}{c:c} t_{n+1}=0 & t_{n+1}=1 \end{array} \\ \left[\begin{array}{ccc|ccc}
1 & & & 1 & & \\
1 & & & -1 & & \\ \hdashline
 & 1 & & & 1 & \\
 & 1 & & & -1 & \\ \hdashline
 & \vdots & & & \vdots & \\
 & \vdots & & & \vdots & \\ \hdashline
 & & 1 & & & 1 \\
 & & 1 & & & -1
\end{array}\right] \end{array} := \mathbb{N}_{2^{n+1}}.
\end{gathered} \tag{18}
$$

Here $\hat{\otimes}$ is new tensor product:

$$
\left[\mathbf{I}_{2^n}\,\middle|\,\mathbf{I}_{2^n}\right]\hat{\otimes}\left[\begin{array}{c|c}1 & 1\\ 1 & -1\end{array}\right] := \left[\mathbf{I}_{2^n}\otimes\begin{bmatrix}1\\1\end{bmatrix}\middle|\,\mathbf{I}_{2^n}\otimes\begin{bmatrix}1\\-1\end{bmatrix}\right].
$$

From recurrent relation (17) we obtain

$$
\begin{gathered}
\mathbf{G}_{2^n}^{[n]} = \left(\prod_{k=2}^{n}\left[\mathbf{I}_{2^{n-k}}\otimes\Delta_{2^k}\cdot\mathbb{N}_{2^k}\cdot\mathbf{P}_{2^k}^{\{t_k\}}\right]\right)\cdot\left[\mathbf{I}_{2^{n-k+1}}\otimes\mathbf{G}_{2^1}^{[1]}\right] = \prod_{k=2}^{n}\left\{\mathbf{I}_{2^{n-k}}\otimes\left[\Delta\left\{(-1)^{\alpha_{k-1}\alpha_k}\right\}\right]\cdot\left[\delta_{\boldsymbol{\alpha}_{k-1},\mathbf{t}_{k-1}}^{(2^{k-1})}(-1)^{\alpha_k t_k}\right]\cdot\right. \\
\left.\cdot\left[\delta_{\alpha_k}^{(2)}(t_k)\left[\mathbf{I}_{2^{k-2}}\otimes\mathbf{P}_2^{t_k}\right]\right]\right\}\cdot\left[\mathbf{I}_{2^{n-k+1}}\otimes\mathbf{G}_{2^1}^{[1]}\right].
\end{gathered} \tag{19}
$$

This expression represents the fast algorithm for the Golay transform.

Example 5.

$$
\mathbf{G}_{2^2}^{[2]} = \begin{bmatrix} \mathrm{com}_{(0,0)}^{[2]}(\mathbf{t}_2) \\ \mathrm{com}_{(0,1)}^{[2]}(\mathbf{t}_2) \\ \mathrm{com}_{(1,0)}^{[2]}(\mathbf{t}_2) \\ \mathrm{com}_{(1,1)}^{[2]}(\mathbf{t}_2) \end{bmatrix} = \left[\begin{array}{cccc} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ \hdashline 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{array}\right] = \left[\begin{array}{cc:cc} 1 & & & \\ & 1 & & \\ \hdashline & & 1 & \\ & & & -1 \end{array}\right]\left[\begin{array}{cc:cc} 1 & & 1 & \\ 1 & & -1 & \\ \hdashline & 1 & & 1 \\ & 1 & & -1 \end{array}\right]\left[\begin{array}{cc:cc} 1 & & & \\ & 1 & & \\ \hdashline & & & 1 \\ & & 1 & \end{array}\right]\left[\begin{array}{cc:cc} 1 & 1 & & \\ 1 & -1 & & \\ \hdashline & & 1 & 1 \\ & & 1 & -1 \end{array}\right] =
$$

$$
= \left[\mathbf{I}_{2^0}\otimes\Delta_{2^2}\cdot\mathbb{N}_{2^2}\cdot\mathbf{P}_{2^2}^{\{t_2\}}\right]\cdot\left[\mathbf{I}_{2^1}\otimes\mathbf{G}_{2^1}^{[1]}\right].
$$

$$
\mathbf{G}_{2^3}^{[3]} = \begin{bmatrix} \mathrm{com}_{(0,0,0)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(0,0,1)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(0,1,0)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(0,1,1)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(1,0,0)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(1,0,1)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(1,1,0)}^{[3]}(\mathbf{t}_3) \\ \mathrm{com}_{(1,1,1)}^{[3]}(\mathbf{t}_3) \end{bmatrix} = \left[\begin{array}{cccc:cccc}
1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ \hdashline
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\
-1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ \hdashline
1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ \hdashline
-1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & -1 & 1 & 1
\end{array}\right] = \left[\begin{array}{cccc:cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & -1 & & & & \\ \hdashline
 & & & & 1 & & & \\
 & & & & & 1 & & \\
 & & & & & & -1 & \\
 & & & & & & & 1
\end{array}\right]\cdot\left[\begin{array}{cc:cc:cc:cc}
1 & & & & 1 & & & \\
1 & & & & -1 & & & \\ \hdashline
 & 1 & & & & 1 & & \\
 & 1 & & & & -1 & & \\ \hdashline
 & & 1 & & & & 1 & \\
 & & 1 & & & & -1 & \\ \hdashline
 & & & 1 & & & & 1 \\
 & & & 1 & & & & -1
\end{array}\right]\times
$$

$$
\times\begin{bmatrix}
1&&&&&&&\\
&1&&&&&&\\
&&1&&&&&\\
&&&1&&&&\\
&&&&&1&&\\
&&&&1&&&\\
&&&&&&&1\\
&&&&&&1&
\end{bmatrix}\cdot\begin{bmatrix}
1&1&1&-1&&&&\\
1&1&-1&1&&&&\\
1&-1&1&1&&&&\\
-1&1&-1&1&&&&\\
&&&&1&1&1&-1\\
&&&&1&1&-1&1\\
&&&&1&-1&1&1\\
&&&&-1&1&1&1
\end{bmatrix}=\begin{bmatrix}
1&&&&&&&\\
&1&&&&&&\\
&&1&&&&&\\
&&&-1&&&&\\
&&&&1&&&\\
&&&&&1&&\\
&&&&&&-1&\\
&&&&&&&1
\end{bmatrix}\times
$$

$$
\times\begin{bmatrix}
1&&&&1&&&\\
1&&&&-1&&&\\
&1&&&&1&&\\
&1&&&&-1&&\\
&&1&&&&1&\\
&&1&&&&-1&\\
&&&1&&&&1\\
&&&1&&&&-1
\end{bmatrix}\cdot\begin{bmatrix}
1&&&&&&&\\
&1&&&&&&\\
&&1&&&&&\\
&&&1&&&&\\
&&&&&1&&\\
&&&&1&&&\\
&&&&&&&1\\
&&&&&&1&
\end{bmatrix}\cdot\begin{bmatrix}
1&&&&&&&\\
&1&&&&&&\\
&&1&&&&&\\
&&&-1&&&&\\
&&&&1&&&\\
&&&&&1&&\\
&&&&&&1&\\
&&&&&&&-1
\end{bmatrix}\times
$$

$$
\times\begin{bmatrix}
1&&1&&&&&\\
1&&-1&&&&&\\
&1&&1&&&&\\
&1&&-1&&&&\\
&&&&1&&1&\\
&&&&1&&-1&\\
&&&&&1&&1\\
&&&&&1&&-1
\end{bmatrix}\cdot\begin{bmatrix}
1&&&&&&&\\
&1&&&&&&\\
&&&1&&&&\\
&&1&&&&&\\
&&&&1&&&\\
&&&&&1&&\\
&&&&&&&1\\
&&&&&&1&
\end{bmatrix}\cdot\begin{bmatrix}
1&1&&&&&&\\
1&-1&&&&&&\\
&&1&1&&&&\\
&&1&-1&&&&\\
&&&&1&1&&\\
&&&&1&-1&&\\
&&&&&&1&1\\
&&&&&&1&-1
\end{bmatrix}=
$$

$$
=\left[\mathbf{I}_{2^0}\otimes\Delta_{2^3}\cdot\mathbb{N}_{2^3}\cdot\mathbf{P}_{2^3}^{\{t_3\}}\right]\cdot\left[\mathbf{I}_{2^1}\otimes\Delta_{2^2}\cdot\mathbb{N}_{2^2}\cdot\mathbf{P}_{2^2}^{\{t_2\}}\right]\cdot\left[\mathbf{I}_{2^2}\otimes\mathbf{G}_{2^1}^{[1]}\right]. \qquad \square
$$

Conclusion and future researches

In this paper, we have shown a new unified approach to the so-called generalized multi-parameter m–complementary sequences. The approach is based on a new iteration generating construction. This construction has a rich algebraic structure. It is associated not with the triple $(\mathbf{Z}_2, \mathcal{F}_2, \mathbf{C})$, but with

1) $(\mathbf{Z}_m, \mathbf{U}_m, \mathcal{A}lg)$,

2) $\left(\mathbf{Z}_m, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2, ..., \mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$,

3) $\left(\mathbf{Gr}_m, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2, ..., \mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$ or with

4) $\left(\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2, ..., \mathbf{Gr}_m^n\right\}, \left\{\mathbf{U}_m^1, \mathbf{U}_m^2, ..., \mathbf{U}_m^n\right\}, \mathcal{A}lg\right)$,

where $\left\{\mathbf{U}_m^1, \mathbf{U}_m^2, ..., \mathbf{U}_m^n\right\}$ is a set of arbitrary unitary $(m\times m)$-transforms and $\left\{\mathbf{Gr}_m^1, \mathbf{Gr}_m^2, ..., \mathbf{Gr}_m^n\right\}$ is a set of arbitrary groups of given order m. Furthermore, we have derived demonstrated fast algorithms for Golay transforms.

We are going to use generalized multi-parameter m-complementary sequences as subcarriers of Intelligent OFDM telecommunication system. Most of the data transmission systems nowadays use orthogonal frequency division multiplexing telecommunication system (OFDM-TCS) based on the discrete Fourier transform (DFT) $\mathcal{F}_N$. The conventional OFDM will be denoted by the symbol $\mathcal{F}_N$-**OFDM**. Conventional OFDM-TCS makes use of signal orthogonality of the multiple sub-carriers $e^{j2\pi kn/N}$ (complex exponential harmonics). Sub-carriers $\left\{\mathbf{subc}_k(n)\right\}_{k=0}^{N-1} = \left\{e^{j2\pi kn/N}\right\}_{k=0}^{N-1}$ form matrix of DFT $\mathcal{F}_N = \left[\mathbf{subc}_k(n)\right]_{k,n=0}^{N-1} \equiv \left[e^{j2\pi kn/N}\right]_{k,n=0}^{N-1}$.

At the time, the idea of using the fast algorithm of different orthogonal transforms $\mathbf{U}_N = \left[\mathbf{subc}_k(n)\right]_{k,n=0}^{N-1}$ for a software-based implementation of the OFDM's modulator and demodulator, transformed this technique from an attractive, but difficult to implement idea, into an incredibly successful story of the data transmission. OFDM-TCS, based on arbitrary orthogonal (unitary) transform $\mathbf{U}_N$ will be denoted as $\mathbf{U}_N$-**OFDM**. The idea which links $\mathcal{F}_N$-**OFDM** and $\mathbf{U}_N$-**OFDM** is that, in the same manner that the complex exponentials $\left\{e^{j2\pi kn/N}\right\}_{k=0}^{N-1}$ are orthogonal to each-other, the members of a family of $\mathbf{U}_N$-sub-carriers $\left\{\mathbf{subc}_k(n)\right\}_{k=0}^{N-1}$ (rows of the matrix $\mathcal{U}_N$) will satisfy the same property. The $\mathbf{U}_N$-**OFDM** reshapes the multi-carrier transmission concept, by using carriers $\left\{\mathbf{subc}_k(n)\right\}_{k=0}^{N-1}$ instead of OFDM's complex exponentials $\left\{e^{j2\pi kn/N}\right\}_{k=0}^{N-1}$. In this paper, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on MPTs. In our Intelligent-OFDM-TCS we are going to use multi-parameter Golay transform $\mathbf{G}_{2^n}(\varphi_1, \varphi_2,\ldots, \varphi_q)$ at the place of DFT $\mathcal{F}_N$. We are going to study of Intell- $\mathbf{G}_{2^n}(\varphi_1, \varphi_2,\ldots, \varphi_q)$-OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects.

References

[1] Golay MJE. Multi-slit spectrometry. J Opt Soc Am 1949; 39(6): 437-444. DOI: 10.1364/JOSA.39.000437.

[2] Golay MJE. Complementary series. IRE Transaction on Information Theory 1961; 7(2): 82-87. DOI: 10.1109/TIT.1961.1057620.

[3] Golay MJE. Sieves for low autocorrelation binary sequences. IEEE Transactions on Information Theory 1977; 23(1): 43-51. DOI: 10.1109/TIT.1977.1055653.

[4] Shapiro HS. Extremal problems for polynomials and power series. ScM.Thesis. Massachusetts Institute of Technology; 1951.

[5] Shapiro HS. A power series with small partial sums. Notices of the AMS 1958; (6)3: 366-378.

[6] Rudin W. Some theorems on Fourier coefficients. Proceedings of the American Mathematical Society 1959; 10(6): 855-859. DOI: 10.2307/2033608.

[7] Labunets VG, Chasovskikh VP, Ostheimer E. Multiparameter Golay 2-complementary sequences and transforms. In Book: Information Technologies and Nanotechnologies. Samara: "Novaya Tehnika" Publisher; 2018: 1013-1022.

[8] Labunets VG, Chasovskikh VP, Ostheimer E. Multiparameter Golay m-complementary sequences and transforms. In Book: Information Technologies and Nanotechnologies. Samara: "Novaya Tehnika" Publisher; 2018: 1005-1012.

[9] Jacobi CGJ. Uber ein leichtes verfahren die in der theorie der sacularstorungen vorkommendern gleichungen numerische aufzulosen. Jurnal fur die Reine und Angewandte Mathematik 1846; 30: 51-94.

[10] Brent RP, Luk FT. The solution of singular-value and symmetric eigenvalue problems on multiprocessor Arrays. SIAM J Sci and Stat Comput 1985; 6(1): 69-83. DOI: 10.1137/0906007.

[11] Lei ZX. Some properties of generalized Rudin-Shapiro polynomials. Chinese Ann Math: Ser A 1991; 12(2): 145-153.Golay MJE. Multi-slit spectrometry. Journal of the Optical Society of America 1949; 39: 437-444.

Authors' information

Valeri Grigorievich Labunets (1946 b.), graduated (1970) from Urals Polytechnical Institute. He received his Candidate's degree in Technical Sciences in 1978 and DrSc degree in 1988. At present, he is Professor of Information Technologies department at Ural State Forest Engineering University. The areas of research interests include digital signal and image processing, geoinformatics and pattern recognition, quantum computing. E-mail: *vlabunets05@yahoo.com* .

Victor Petrovich Chasovskih (1947 b.), graduated (1971) from Urals Polytechnical Institute. He received his Candidate's degree in Technical Sciences in 1985 and DrSc degree in 1992. At present, he is Professor of Information Technologies department at Ural State Forest Engineering University. The areas of research interests include Web technologies, mining of massive datasets and image processing, geoinformatics. E-mail: *u2007u@ya.ru* .

Yuri Gennadievich Smetanin (1951 b.), graduated from Moscow Institute of Physics and Technology (1975). He received his Candidate's degree in Phisical and Mathematical Sciences in 1982 and DrSci degree in 2003. At present, he is a Chief Scientist at the Federal Reseach Center "Informatics and Control". His interests include combinatorics on words, pattern recognition, image analysis. E-mail: *ysmetanin@rambler.ru* .

Ekaterina Ostheimer (Rundblad) (1970 b.), graduated (1993) from Urals Polytechnical Institute. He received his Candidate's degree in Technical Sciences in 1995 and DrSc degree in 2000 from Tampere University. At present, she is Head of Capricat LLC (Florida, USA).The areas of research interests include digital signal and image processing, geoinformatics and pattern recognition, quantum computing. E-mail: *katya@capricat.com* .

GRNTI 28.23.15, 28.17.19, 28.17.24, 89.57.35, 89.57.45.
Received June 25, 2018. The final version – October 29, 2018.