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.


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) 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 methods are used: 1) Abelian group Z2, 2) 2-point Fourier transform F2, and 3) complex field C, i.e., these transforms are associated with the triple (Z2, F2, C).

In previous papers [7, 8], we have shown a new unified approach to the GF(p) - transforms, or Clifford-valued complementary sequences and Golay transforms. It was associated not with the triple (Z2, F2, C), but with triples

(Z2, {CS1(q, α, γ), CS2(q, α, γ)}, Alg) and (Z2, {CS1(q, α, γ), Alg}, where \( CS1(q, α, γ) \), \( CS2(q, α, γ) \) is a set of arbitrary unitary(2×2)-transforms of type

\[
CS(q, α, γ) = \begin{bmatrix} e^{iα} \cos q & e^{iγ} \sin q \\ -e^{-iα} \sin q & -e^{-iγ} \cos q \end{bmatrix},
\]

k = 1,..., n,
and \( CS(q, α, γ) \) is a single transform, Alg is an algebra (for example, Clifford algebra).

In this work, we develop a new unified approach to the so-called generalized multi-parameter m-sequence. This construction has a rich algebraic structure. It is associated not not with the triple (Z2, F2, C), but with

1) \( (Z_m, U_m, Alg) \),
2) \( (Z_m, \{U^1_m, U^2_m, ..., U^m_m\}, Alg) \),
3) \( (Gr_m, \{U^1_m, U^2_m, ..., U^m_m\}, Alg) \),
4) \( (\{Gr^1_m, Gr^2_m, ..., Gr^m_m\}, \{U^1_m, U^2_m, ..., U^m_m\}, Alg) \).

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

\[
U^r_m = U^s_m(q_1, q_2, ..., q_s) = U^s_m(q_1) = \prod_{r=1}^{m} J(q_r),
\]

where

\[
J(q, r, s) = \begin{bmatrix} 1 & ... & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & ... & -c(r, s) & ... & -c(r, s) \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{bmatrix},
\]

is the Jacobi orthonormal rotation with reflection,

\( q_r = (q_1, q_2, ..., q_s) \), \( q_s = (q_s^0, q_s^1, ..., q_s^n) \) are the Jacobi parameters,
\( q = C^m_m = (m-1)/2 \), \( c(r, s) = \cos (q_r), \) \( s(r, s) = \sin (q_r) \).

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 \( U^1_m, U^2_m, ..., U^m_m \) and single group \( Z_m \). Then we generalize the previously method on n unitary (m×m)-transforms \( U^1_m, U^2_m, ..., U^m_m \) and on m-finite groups \( \{Gr^1_m, Gr^2_m, ..., Gr^m_m\} \). 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]

\[
mGCS = \{\text{com}_m(t) \} \text{=} \{ (c_0(t), c_1(t), \ldots, c_{m-1}(t)) \}
\]

is defined by \( \sum_{k=0}^{m-1} \text{COR}_m(t) = m \cdot \delta(t) \), \( \sum_{k=0}^{m-1} |\text{COM}_m(z)|^2 = m \),

where \( \{\text{COR}_m(t)\}_{m-1}^{n-1} \) are the periodic autocorrelation functions of \( \{\text{com}_m(t)\}_i \) and \( \text{COM}_m(z) = Z \{\text{com}_m(t)\} \) are their \( Z \) - transforms.

We use two symbols \( \alpha_m \in [0, m^m - 1] = Z_m^n \) and \( t \in [0, m^m - 1] = Z_m^n \) for numeralation of Golay sequences and discrete time, respectively. For integer \( \alpha_m \in [0, m^m - 1] = Z_m^n \) and \( t \in [0, m^m - 1] = Z_m^n \) we shall use m-ary codes \( \alpha_m = (\alpha_{m-1}, \alpha_{m-2}, \ldots, \alpha_0) \), \( t = (t_m, t_{m-1}, \ldots, t_0) \), where \( \alpha_m, t \in \{0, ..., m-1\} = Z_m, \ i = 1, 2, ..., n. \)

Let \( \alpha_m = (\alpha_{m-1}, \alpha_{m-2}, \ldots, \alpha_0) \) and \( t = (t_m, t_{m-1}, \ldots, t_0) \) be m-ary codes, then define

\[
\alpha_m = [\alpha_{m-1}] = \sum_{i=0}^{m-1} \alpha_{m-i} m^{-i}, \quad \text{and} \quad t = [t_{m-1}] = \sum_{i=0}^{m-1} t_{m-i} m^{-i}
\]

\[
G_{m-1}^{[n+1]} = \begin{bmatrix}
\text{com}^{[n+1]}_{m-1}(t_{m-1}) \\
\text{com}^{[n+1]}_{m-2}(t_{m-1}) \\
\text{com}^{[n+1]}_{m-3}(t_{m-1}) \\
\ldots \\
\text{com}^{[n+1]}_{m-1}(t_{m-1}) \\
\end{bmatrix}
\]

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

\[
G_{m}^{[n+1]} = \begin{bmatrix}
\text{com}^{[n+1]}_{m-1}(t_{m-1}) \\
\text{com}^{[n+1]}_{m-2}(t_{m-1}) \\
\text{com}^{[n+1]}_{m-3}(t_{m-1}) \\
\ldots \\
\text{com}^{[n+1]}_{m-1}(t_{m-1}) \\
\end{bmatrix}
\]

**Example 1.** For \( n = 1 \) and \( n = 2 \) we have, respectively,
Many-parameter \( m \)-complementary Golyay sequences and transforms

Labunets V.G., Chasovskikh V. P., Smetanin Ju.G., Ostheimer E.

# Many-parameter \( m \)-complementary Golyay sequences and transforms

It is easy to check that

\[
G_{\alpha} = \begin{bmatrix}
\text{com}_1^{(1)}(t_1) \\
\text{com}_1^{(2)}(t_1) \\
\vdots \\
\text{com}_m^{(1)}(t_1) \\
\text{com}_m^{(2)}(t_1)
\end{bmatrix} = \begin{bmatrix}
\text{com}_1^{(1)}(t_{1,0}) \\
\text{com}_1^{(2)}(t_{1,0}) \\
\vdots \\
\text{com}_m^{(1)}(t_{1,0}) \\
\text{com}_m^{(2)}(t_{1,0})
\end{bmatrix}
\]

\[
G_{\alpha}^{(2)} = \begin{bmatrix}
\text{com}_1^{(1)}(t_2) \\
\text{com}_1^{(2)}(t_2) \\
\vdots \\
\text{com}_m^{(1)}(t_2) \\
\text{com}_m^{(2)}(t_2)
\end{bmatrix} = \begin{bmatrix}
\text{com}_1^{(1)}(t_{2,0}) \\
\text{com}_1^{(2)}(t_{2,0}) \\
\vdots \\
\text{com}_m^{(1)}(t_{2,0}) \\
\text{com}_m^{(2)}(t_{2,0})
\end{bmatrix}
\]

The matrix \( G_{\alpha}^{(m+1)} \) is constructed by an iteration construction. The initial matrix \( G_{\alpha}^{(1)} \) is formed by starting with an arbitrary unitary \( (m \times m) \)-matrix (in many-parameter form or not)

\[
U_m = [A_0(t)] := G_{\alpha}^{(1)} = \begin{bmatrix}
\text{com}_1^{(1)}(t_1) \\
\text{com}_1^{(2)}(t_1) \\
\vdots \\
\text{com}_m^{(1)}(t_1) \\
\text{com}_m^{(2)}(t_1)
\end{bmatrix} = \begin{bmatrix}
A_0(0) & A_0(1) & A_0(2) & \ldots & A_0(m-1) \\
A_1(0) & A_1(1) & A_1(2) & \ldots & A_1(m-1) \\
A_2(0) & A_2(1) & A_2(2) & \ldots & A_2(m-1) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
A_{m-1}(0) & A_{m-1}(1) & A_{m-1}(2) & \ldots & A_{m-1}(m-1)
\end{bmatrix}
\]

where \( A_i(t) \in \text{Alg} \).

\[
\text{com}_1^{(1)}(t) = (A_0(0), A_0(1), \ldots, A_0(m-1)).
\]

**Example 2.** The initial matrix \( G_{\alpha}^{(1)} \) can be the Fourier transform on Abelian group \( \mathbb{Z}_m \):

\[
G_{\alpha}^{(1)} = \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
1 & \varepsilon^{11} & \varepsilon^{12} & \ldots & \varepsilon^{1(m-1)} \\
1 & \varepsilon^{21} & \varepsilon^{22} & \ldots & \varepsilon^{2(m-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \varepsilon^{(m-1)1} & \varepsilon^{(m-1)2} & \ldots & \varepsilon^{(m-1)(m-1)}
\end{bmatrix}
\]

\[
= \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
\varepsilon^{11} & \varepsilon^{12} & \ldots & \varepsilon^{1(m-1)} \\
\varepsilon^{21} & \varepsilon^{22} & \ldots & \varepsilon^{2(m-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\varepsilon^{(m-1)1} & \varepsilon^{(m-1)2} & \ldots & \varepsilon^{(m-1)(m-1)}
\end{bmatrix}
\]

where \( \varepsilon_m = \sqrt{-1} \in \text{Alg} \), \( \text{com}_1^{(1)}(t) = (1, \varepsilon^{11}, \varepsilon^{12}, \ldots, \varepsilon^{1(m-1)}) \).

\( k = 0, 1, \ldots, m-1 \) are characters \( \mathbb{Z}_m \).

It is easy to check that

\[
\left| \text{COM}_0(z)^{2} + \text{COM}_1(z)^{2} + \ldots + \text{COM}_m(z)^{2} \right|_{H_{1}} = m.
\]

Indeed,

\[
\sum_{j=1}^{n} \left| \text{COM}_j(z)^{2} \right| = \sum_{j=1}^{n} \text{COM}_j(z) \overline{\text{COM}_j(z)} = \sum_{j=1}^{n} \left( \sum_{i=0}^{n} a_i(t) z^i \right) \overline{\left( \sum_{i=0}^{n} a_i(t) z^i \right)} = \sum_{j=1}^{n} \sum_{i=0}^{n} a_i(t) \overline{a_i(t)} (z^i \overline{z^i}) = \sum_{j=1}^{n} \sum_{i=0}^{n} \delta_{i,-j} z^i \overline{z^i} = \sum_{i=0}^{n} |z|^i,
\]

since \( \sum_{i=0}^{n} a_i(t) \overline{a_i(t)} = \delta_{i,-j} \) is true for an arbitrary unitary (orthogonal) matrix. Hence,

\[
\left( \sum_{j=1}^{n} \text{COM}_j(z)^{2} \right)^{\frac{1}{2}} = \left( \sum_{i=0}^{n} |z|^i \right)^{\frac{1}{2}} = m
\]

and initial sequences in the form of rows of an unitary matrix (in particular case, in the form of characters \( \text{com}_m(t_i) = (1, 1^{k}, \varepsilon^{1k}, \varepsilon^{2k}, \ldots, \varepsilon^{(m-1)k}) \) of cyclic group \( \mathbb{Z}_m \) are the Golyay \( m \)-complementary sequences.

## Methods

The matrix \( G_{\alpha}^{(m+1)} \) is constructed by an iteration construction

\[
G_m(U_m^{(1)}) \rightarrow G_m^{(2)}(U_m^{(2)}, U_m^{(3)}) \rightarrow \ldots \rightarrow G_m^{(n)}(U_m^{(n)}, U_m^{(n+1)}),
\]

where

\[
U_{m+1} := \{ U_m, U_m^{(1)}, U_m^{(2)} \} = \{ U_{m}, U_{m+1} \}, \]

\( U_{m} := \{ U_{m}, U_{m+1} \} \).

Here

\[
U_m^{(s)}(\varphi_{s}) = [A_{s}(t) \mid \varphi_{s})]_{s=1}^{n \rightarrow 0} \in SU(\text{Alg}, m)
\]

\( s = 1, 2, \ldots, n \) are a sequence of unitary many-parameter \((m \times m)\)-transforms, belonging to the special unitary group \( SU(\text{Alg}, m) \), where \( s = 1, 2, \ldots, n+1 \) and \( A_{s}(t) \mid \varphi_{s} \) are \( \text{Alg} \)-valued many-parameter sequences.

Let us assume that we have \( m \)-Golyay matrix \( G_m^{(s)}(U_m^{(1)}, \ldots, U_m^{(n)}) = G_m^{(s)}(U_{m+1}) \) (depending on \( n \) previous transforms \( U_m^{(1)}, \ldots, U_m^{(n)} \)). We need to construct the next \( m \)-Golyay matrix \( G_m^{(s)}(U_m^{(1)}, \ldots, U_m^{(n+1)}) = G_m^{(s)}(U_{m+1}) \) using only \( G_m^{(s)}(U_m^{(1)}, \ldots, U_m^{(n)}) \) and \( U_{m+1} \). We are going to use for \( m \)-Golyay matrix \( G_m^{(s)}(U_{m+1}) \) the same structure as in (1):

\[
G_m^{(s)}(U_{m+1}) = \begin{bmatrix}
\text{com}_m^{(s)}(t_1 \mid U_{m+1}) \\
\text{com}_m^{(s)}(t_2 \mid U_{m+1}) \\
\vdots \\
\text{com}_m^{(s)}(t_{m+1} \mid U_{m+1})
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\text{com}_m^{(s-1,0)}(t_1 \mid U_{m+1}) \\
\text{com}_m^{(s-1,1)}(t_1 \mid U_{m+1}) \\
\vdots \\
\text{com}_m^{(s-1,m)}(t_1 \mid U_{m+1})
\end{bmatrix}
\]

For constructing \( G_m^{(s+1)}(U_{m+1}) \) from \( G_m^{(s)}(U_{m+1}) \) we take each complementary set in the form
Many-parameter $m$-complementary Golay sequences and transforms

Labunets V. G., Chasovskikh V. P., Smetanin Ju. G., Ostheimer E. M.

Computer Optics, 2018, Vol. 42(6) 1077

$m$-GCS$^{(1)}(U_{\alpha, \beta}) = \begin{bmatrix}
\text{com}^{[1]}_{(n, 1, 0)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[1]}_{(n, 1, 1)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[1]}_{(n, 1, m-1)}(t_1 \mid U_{\alpha}) \\
\vdots
\end{bmatrix}
\begin{bmatrix}
I_{m} \\
T_{m}^{\nu} \\
\vdots
\end{bmatrix}
\begin{bmatrix}
\tilde{P}_{m}^\nu \\
T_{m}^{\nu-1}\tilde{P}_{m}^\nu \\
\vdots
\end{bmatrix}
$}

$\text{and construct } m \text{ shifted versa of their components}$

$m$-GCS$^{(1)}(U_{\alpha, \beta}) \rightarrow$

$m$-GCS$^{(2)}(U_{\alpha, \beta}) = \begin{bmatrix}
\text{com}^{[2]}_{(n, 1, 0)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[2]}_{(n, 1, 1)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[2]}_{(n, 1, m-1)}(t_1 \mid U_{\alpha}) \\
\vdots
\end{bmatrix}
\begin{bmatrix}
I_{m} \\
T_{m}^{\nu} \\
\vdots
\end{bmatrix}
\begin{bmatrix}
\tilde{P}_{m}^\nu \\
T_{m}^{\nu-1}\tilde{P}_{m}^\nu \\
\vdots
\end{bmatrix}$

where

$m$-GCS$^{(2)}(U_{\alpha, \beta}) = U_{\alpha, \beta}^{(2)} = \begin{bmatrix}
\text{com}^{[2]}_{(n, 1, 0)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[2]}_{(n, 1, 1)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[2]}_{(n, 1, m-1)}(t_1 \mid U_{\alpha}) \\
\vdots
\end{bmatrix}
\begin{bmatrix}
I_{m} \\
T_{m}^{\nu} \\
\vdots
\end{bmatrix}
\begin{bmatrix}
\tilde{P}_{m}^\nu \\
T_{m}^{\nu-1}\tilde{P}_{m}^\nu \\
\vdots
\end{bmatrix}$

Here $\alpha_n = 0, 1, \ldots, m-1$, $P_{m}$ is the cyclic permutation operator on $\alpha_n$ positions (modulo $m$), $T_{m}^{\nu}$ is the shift operator on $m$'s positions $T_{m}^{\nu} = T_{m}^{\nu \alpha} f(t) := f(t + m^\nu)$, $\tilde{P}_{m}^\nu$ is transposed of $P_{m}$.

According to (1) we obtain

$G^{[1]}_{\alpha, \beta}(U_{\nu+1}) = \begin{bmatrix}
\text{com}^{[1]}_{(n, 1, 0)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[1]}_{(n, 1, 1)}(t_1 \mid U_{\alpha}) \\
\text{com}^{[1]}_{(n, 1, m-1)}(t_1 \mid U_{\alpha}) \\
\vdots
\end{bmatrix}$

and, consequently,

$\text{com}^{[1]}_{(n, 1, 0)}(t_1 \mid U_{\alpha}) = \sum_{\beta_n=0}^{\nu} \alpha_n a_{n, \beta_n}(\beta_n) T_{m}^{\nu \alpha}(\beta_n, \alpha_n) \text{com}^{[1]}_{(n, 1, \beta_n)}(t_1 \mid U_{\alpha}).$

Since $t_{1+1} = (t_n, t_{n+1})$, then believe $t_{1+1} = \alpha_n \oplus \beta_n$, we obtain:

$\text{com}^{[1]}_{(n, n, 0, \alpha_n)}(t_{n+1} \mid U_{\nu+1}) = \sum_{\beta_n=0}^{\nu} \alpha_n a_{n, \beta_n}(\beta_n) T_{m}^{\nu \alpha}(\beta_n, \alpha_n) \text{com}^{[1]}_{(n, 1, \beta_n)}(t_1 \mid U_{\alpha}).$

It is finally recurrent relation between $m$-complementary sequences of $G^{[1]}_{\alpha, \beta}(U_{\nu+1})$ and $G^{[\nu]}_{\alpha, \beta}(U_{\nu+1})$.

From (9) we obtain expression for $\text{com}^{[\nu]}_{(n, 1, 0)}(t_{n+1} \mid U_{\nu+1})$:

$\text{com}^{[\nu]}_{(n, 1, 0)}(t_{n+1} \mid U_{\nu+1}) = \sum_{\beta_n=0}^{\nu} \alpha_n a_{n, \beta_n}(\beta_n) T_{m}^{\nu \alpha}(\beta_n, \alpha_n) \text{com}^{[\nu]}_{(n, 1, \beta_n)}(t_1 \mid U_{\alpha}).$

From (9) we obtain expression for $\text{com}^{[\nu]}_{(n, 1, 0)}(t_{n+1} \mid U_{\nu+1})$:

$\text{com}^{[\nu]}_{(n, 1, 0)}(t_{n+1} \mid U_{\nu+1}) = \sum_{\beta_n=0}^{\nu} \alpha_n a_{n, \beta_n}(\beta_n) T_{m}^{\nu \alpha}(\beta_n, \alpha_n) \text{com}^{[\nu]}_{(n, 1, \beta_n)}(t_1 \mid U_{\alpha}).$

In particular, for matrices in the form of the Fourier transform $U_0 = U_0 \ldots U_0 = \cdots = U_m = [e_{m}^\nu]$ we have

$\text{com}^{[\nu]}_{(n, 1, 0)}(t_{n+1}) = \text{com}^{[\nu]}_{(n, 1, 0)}(t_1) = \text{com}^{[\nu]}_{(n, 1, 0)}(t_1) = \text{com}^{[\nu]}_{(n, 1, 0)}(t_1) = \text{com}^{[\nu]}_{(n, 1, 0)}(t_1).
$
in the short form $g \in X$ and to call the group of transformations of $\cdot$. The pair $\cdot$ is called a space with transformation group the elements $x \in X$ are called points of the space.

**Definition 4.** If is a permutation group of degree $n$, then the permutation representation of is the linear permutation representation of : $P : \text{Gr} \rightarrow \text{GL}_n(\mathbb{A}lg)$ which maps to the corresponding permutation matrix $P(g)$.

That is, acts on by permuting the standard basis vectors $\{e_a\}_{a \in X} \in \mathbb{A}lg^n$ such that

$$P(g)e_a = e_{a'} \in \{e_a\}_{a \in X},$$

where $P(g)$’s are the operators in $\mathbb{A}lg^n$ which define the above mentioned linear representation.

**Example 4.**

For $m = 4$ we have two groups: $\text{Gr}_4 = \{0, 1, 2, 3\}$ and $\text{Gr}_2 = \{0, 1\}$. For both groups we have the following permutation representations:

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

$$P(0,0) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad P(0,1) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad P(1,0) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad P(1,1) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$
respectively. Let \( G_{m+1} := \{ G_{m+1}^0, G_{m+1}^1, ..., G_{m+1}^{n-1} \} \) be a set of arbitrary groups of given order \( m \) : \( G_{m+1}^0 = \{ g_{m+1}^0 \}_{n_0=0}^{n-1}, ..., G_{m+1}^{n-1} = \{ g_{m+1}^{n-1} \}_{n_0=0}^{n-1} \). Then we can use on each iteration permutation representations \( \{ P_{m}^* (g_{m+1}^* ) \}_{n_0=0}^{n-1} \) for \( G_{m+1}^* \). In this case, we obtain the following Golay transform

\[
G_{m+1}^* (U_{m+1}; G_{m+1}) = \begin{pmatrix}
\text{com}_{[a_0,0]}^{[a]}(t_x | U_{m+1}; G_{m+1}) \\
\text{com}_{[a_1,1]}^{[a]}(t_x | U_{m+1}; G_{m+1}) \\
\text{...} \\
\text{com}_{[a_{n-1},m-1]}^{[a]}(t_x | U_{m+1}; G_{m+1})
\end{pmatrix} = \begin{pmatrix}
\text{com}_{[a_0,0]}^{[a]}(t_x | U_{m}; G_{m}) \\
\text{com}_{[a_1,1]}^{[a]}(t_x | U_{m}; G_{m}) \\
\text{...} \\
\text{com}_{[a_{n-1},m-1]}^{[a]}(t_x | U_{m}; G_{m})
\end{pmatrix}.
\]

It is associated with triple \( \{ \{ G_{m+1}^0, G_{m+1}^1, ..., G_{m+1}^{n-1} \}, \{ U_m^1, U_m^2, ..., U_m^{m-1} \} \}, \text{Alg} \).

**Fast Golay transforms**

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

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

\[
G_{2^n}^{[\sigma]} := \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix} = \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix} = \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix}
\]

and construct the direct sum of introduced matrices

\[
G_{2^{n+1}}^{[\sigma]} = \bigoplus_{\sigma=0}^{2^n} G_{2^n}^{[\sigma]} = \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix} = \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix} = \begin{pmatrix}
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x) \\
\text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x) & \text{com}_{[\sigma_1,1]}^{[\sigma]}(t_x)
\end{pmatrix}.
\]

From (16) we see that \( G_{2^{n+1}}^{[\sigma]} \) represents \( \text{com}_{[\sigma_0,0]}^{[\sigma]}(t_x+2^n \cdot t_{\sigma+1}) \) in (14). It is easy to see, that

\[
G_{2^{n+1}}^{[\sigma]} = \left[ I_{2^{n+1}} \otimes P_{2^n}^* \right] \times \left[ G_{2^n}^{[\sigma]} \right] = \left[ G_{2^n}^{[\sigma]} \right] \times \left[ I_{2^n} \otimes P_{2^n}^* \right] = \left[ I_{2^n} \otimes G_{2^n}^{[\sigma]} \right] \times \left[ I_{2^n} \otimes P_{2^n}^* \right] = P_{2^n}^{[\sigma]} \times \left[ I_{2^n} \otimes G_{2^n}^{[\sigma]} \right],
\]

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

\[
G_{2n+1}^{[n+1]} = \Delta \{(-1)^{\nu_{n,t_{n+1}}}\} \left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right] \left[ I_{2n+1} \otimes G_{n}^{[n]} \right],
\]

\[
\left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right] = \Delta \{(-1)^{\nu_{n,t_{n+1}}}\} \left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right] \left[ I_{2n+1} \otimes G_{n}^{[n]} \right].
\]

Where \(\Delta \{(-1)^{\nu_{n,t_{n+1}}}\} = \text{diag} \{(-1)^{\nu_{n,t_{n+1}}}\}\) is diagonal matrix, and \(\left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right]\) has the following structure

\[
\left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right] = \left[ I_{2n+1} \right] \left( t_{n+1} \right) \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right].
\]

Here \(\hat{\otimes}\) is a new tensor product:

\[
\left[ I_{2n+1} \right] \left( t_{n+1} \right) \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right] = \left[ I_{2n+1} \otimes \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right] \right].
\]

From recurrent relation (17) we obtain

\[
\left[ \delta^{(2t)}_{\nu_{n,t_{n+1}}} \left( -1 \right)^{\nu_{n,t_{n+1}}} \right] = \left[ I_{2n+1} \otimes \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right] \right] = \left[ \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \\ -1 \end{array} \right].
\]

This expression represents the fast algorithm for the Golay transform.

**Example 5.**

\[
G_{2}^{[2]} = \left[ \begin{array}{c} c_{0,0}(t_{2}) \\ c_{1,1}(t_{2}) \\ c_{0,0}(t_{2}) \\ c_{1,1}(t_{2}) \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right].
\]

\[
G_{2}^{[3]} = \left[ \begin{array}{c} c_{0,0}(t_{2}) \\ c_{1,1}(t_{2}) \\ c_{0,0}(t_{2}) \\ c_{1,1}(t_{2}) \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right] = \left[ \begin{array}{c} 1 \\ 1 \\ -1 \\ 1 \\ -1 \end{array} \right].
\]
Many-parameter $m$-complementary Golay sequences and transforms

Labunets V.G., Chasovskikh V. P., Smetanin Ju.G., Ostheimer E.

Computer Optics, 2018, Vol. 42(6) 1081

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 $(\mathbb{Z}_2, \mathbb{F}_2, C)$, but with

1) $(\mathbb{Z}_m, \text{U}_m, A\text{lg})$,
2) $(\mathbb{Z}_m, \{\text{U}_m, \text{U}_m^*, \ldots, \text{U}_m^*\}, A\text{lg})$ or with
3) $(\{\text{Gr}_m, \text{Gr}_m^*, \ldots, \text{Gr}_m^*\}, \{\text{U}_m, \text{U}_m^*, \ldots, \text{U}_m^*\}, A\text{lg})$,
4) $(\{\text{Gr}_m, \text{Gr}_m^*, \ldots, \text{Gr}_m^*\}, \{\text{U}_m, \text{U}_m^*, \ldots, \text{U}_m^*\}, A\text{lg})$,

where $\{\text{U}_m, \text{U}_m^*, \ldots, \text{U}_m^*\}$ is a set of arbitrary unitary $(m \times m)$-transforms and $\{\text{Gr}_m, \text{Gr}_m^*, \ldots, \text{Gr}_m^*\}$ 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 $\{\text{sub}_c(n)\}_{k=0}^{N-1} = \{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ form matrix of DFT $\mathcal{F}_N = [\text{sub}_c(n)]_{k=0}^{N-1} = [e^{j2\pi kn/N}]_{k=0}^{N-1}$.

At the time, the idea of using the fast algorithm of different orthogonal transforms $\text{U}_N = [\text{sub}_c(n)]_{k=0}^{N-1}$ 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 $\text{U}_N$ will be denoted as $\text{U}_N$-OFDM. The idea which links $\mathcal{F}_N$-OFDM and $\text{U}_N$-OFDM is that, in the same manner that the complex exponentials $\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ are orthogonal to each-other, the members of a family of $\text{U}_N$-sub-carriers $\{\text{sub}_c(n)\}_{k=0}^{N-1}$ (rows of the matrix $\text{U}_N$) will satisfy the same property. The $\text{U}_N$-OFDM reshapes the multi-carrier transmission concept, by using carriers $\{\text{sub}_c(n)\}_{k=0}^{N-1}$ in-
stead of OFDM’s complex exponentials \( \{ e^{j2\pi nk/N} \}_{k=0}^{N-1} \). 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 \( G_2(\varphi_1, \varphi_2, \ldots, \varphi_q) \) at the place of DFT \( \mathcal{F} \). We are going to study of Intelligent- \( G_2(\varphi_1, \varphi_2, \ldots, \varphi_q) \)-OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects.

**References**


**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: vsmetanin@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.