Linear codes invariant with respect to generalized shift operators

V.G. Labunets[1], **E. Osthaimer**[2]

[1]Ural State Forest Engineering University, Sibirskytrakt, 37, Ekaterinburg, Russia, 620100
[2]Capricat LLC, Pompano Beach, Florida, USA

Abstract. The purpose of this paper is to introduce new linear codes with generalized symmetry. We extend cyclic and group codes in the following way. We introduce codes, invariant with respect to a family of generalized shift operators (GSO). In particle case when this family is a group (cyclic or Abelian), these codes are ordinary cyclic and group codes. They are invariant with respect to this group. We deal with GSO-invariant codes with fast code and encode procedures based on fast generalized Fouriertransforms. The hope is that these more general structures will lead to larger classes of useful codes "good" properties.

Keywords: linear codes, Levitan-Delsarte algebras of generalized shift operators, orthogonal Fourier-Galois transforms.

1. Introduction

Let $\mathbf{F}$ be a finite field $\mathbf{F}$. A *block code* of length N is a subset $\mathsf{C}$of $\mathbf{F}^N$, i.e., a collection of N length vectors with components from $\mathbf{F}$. Most of the literature on block codes pertains to block codes over finite fields $\mathbf{F}=\mathbf{GF}(q)$ or finite rings $\mathbf{F}=\mathbf{GR}(q)$, where $q=p^s$ and p is a prime. Although any subset forms a code, there are codes with more structure that are very useful and compose the majority of block codes in practice. A *linear block code* is a block code that is an $\mathbf{F}$-subspace of the $\mathbf{F}$-vector space $\mathbf{F}^N$.In addition to linearity, there are many structural properties that make for good codes. One of the most prevalent such structural properties is symmetry of code, that is described as invariance with respect to a group. Invariance (code symmetry), in many circumstances, leads to some nice encoding and decoding algorithms yet it is a very simple structure to describe. For these reasons, it is one of the most studied structural properties in coding theory.

Definition 1 [1,2].*A cyclic block code* $\mathsf{C}\subset\mathbf{F}^N$ *of length* N *over a finite field* $\mathbf{F}$ *is a linear block code withthe property that if* $(c_0,c_1,...,c_{N-2},c_{N-1})\in\mathsf{C}$*then* $(c_{N-1},c_0,...,c_{N-3},c_{N-2})\in\mathsf{C}$.

It means that group of code symmetry of a cyclic code $\mathsf{C}\subset\mathbf{F}^N$ is $\mathbf{Symm}\{\mathsf{C}\}\approx\mathbf{Z}_N$.Cyclic codes are studied from many points of view. One way is to view them as ideals of an algebra. Define $\rho:\mathbf{F}^N\to\mathbf{F}[x]/\langle x^N-1\rangle$ via

$$\rho:(c_0,c_1,...,c_{N-2},c_{N-1})\mapsto c_0+c_1x+...+c_{N-2}x^{N-2}+c_{N-1}x^{N-1}$$

It can be shown that ρ is an isomorphism. Let $\mathsf{C}\subset \mathbf{F}^N$ be cyclic block code. Then $\rho(\mathsf{C})$ is a subspace of the $\mathbf{F}$-vectorspace $\mathbf{F}[x]/\langle x^N-1\rangle$. Now the added condition of being cyclic translates to the following: if $\rho(c)\in\rho(\mathsf{C})$ then

$$x\cdot\rho(c)=x\cdot\left(c_0+c_1x+...+c_{N-2}x^{N-2}+c_{N-1}x^{N-1}\right)=$$
$$=\left(c_{N-1}+c_0x+c_1x^2+...+c_{N-2}x^{N-1}\right)\in\rho(\mathsf{C}).$$

With this extra condition, $\rho(\mathsf{C})\lhd\mathbf{F}[x]/\langle x^N-1\rangle$.

There are many generalizations of cyclic codes, some of which may be viewed as ideals of particular rings [3]:

- negacyclic(skew-cyclic) codes[4-11]- ideal of the ring $\mathsf{A}lg^N(\mathbf{F})[x]/\langle x^N+1\rangle$,
- constacyclic codes [12]- ideal of the ring $\mathsf{A}lg^N(\mathbf{F})[x]/\langle x^N-\lambda\rangle$,where $\lambda\in\mathsf{A}lg(\mathbf{F})$,
- polycyclic codes [3]- ideal of the ring $\mathsf{A}lg^N(\mathbf{F})[x]/\langle f(x)\rangle$,where $f(x)\in\mathsf{A}lg(\mathbf{F})[x]$.

The terminology of the cyclic codes theory may be extended to define a larger family ofcodes. We start by introducing vector-induced clockwise and counterclockwise shifts. Given a vector $\mathbf{s}=(s_0,s_1,...,s_{N-2},s_{N-1})\in\mathbf{F}^N$, the $\mathbf{s}$-clockwise and $\mathbf{s}$ -counterclockwise shifts of codeword $\mathsf{C}\ni(c_0,c_1,...,c_{N-2},c_{N-1})\subset\mathbf{F}^N$ are the following correspondences

$$R^{\mathbf{s}}\mathbf{c}=R^{\mathbf{s}}(c_0,c_1,...,c_{N-1})=(0,c_0,c_1,...,c_{N-2})+c_{N-1}(s_0,s_1,s_2,...,s_{N-1})=$$
$$=(c_{N-1}s_0,\ c_0+s_1c_{N-1},\ c_1+s_2c_{N-1},...,c_{N-2}+s_{N-1}c_{N-1}),$$
$$\mathbf{L}^{\mathbf{s}}\mathbf{c}=\mathbf{L}^{\mathbf{s}}(c_0,c_1,...,c_{N-1})=(c_1,c_2,...,c_{N-1},0)+c_0(s_0,s_1,s_2,...,s_{N-1})=$$
$$=(c_1+s_0c_0,\ c_2+s_1c_0,...,c_{N-1}+s_{N-2}c_0,s_{N-1}c_0).$$

Dyadic codes are defined only for length N, a power of 2, say $N=2^n$, as follows.

Definition 2. For any integer $i\in\{0,1,2,...,N-1\}$, let $i=(i_{n-1},i_{n-2},...,i_1,i_0)$. Denote its radix-2 representation, where

$$i=i_{n-1}2^{n-1}+i_{n-2}2^{n-1}+...+i_12^1+i_02^0=\sum_{l=0}^{n-1}i_l2^l$$

and $i_1\in\{0,1\}$ for $l=0,1,2,...,n-1$. Dyadic addition of two numbers i and j denoted by $i\underset{2}{\oplus}j$ is defined by

$$k=i\underset{2}{\oplus}j=(i_{n-1},i_{n-2},...,i_1,i_0)\underset{2}{\oplus}(j_{n-1},j_{n-2},...,j_1,j_0)=$$
$$=(i_{n-1}\oplus j_{n-1},i_{n-2}\oplus j_{n-2},...,i_1\oplus j_1,i_0\oplus j_0)=(k_{n-1},k_{n-2},...,k_1,k_0)$$

where $k_l=(i_l\oplus j_l)\bmod 2$, for $l=0,1,2,...,n-1$. The dyadic shift, $m=0,1,2,...,N-1$, of a vector $(c_0,c_1,...,c_{N-1})$ is the vector $\left(c_{0\underset{2}{\oplus}m},c_{1\underset{2}{\oplus}m},...,c_{(N-1)\underset{2}{\oplus}m}\right)$.

Definition 3. Linear code of length $N=2^n$ is called dyadic code if the m-dyadic shift of every codeword is also a codeword for all $m=0,1,2,...,N-1$.

The class of dyadic codes is a special case of abelian group codes [13, 14-16] which is briefly discussed in the next section.

In this paper, we would like tointroduce new linear codes with generalized symmetry. We extend cyclic and group codes in the following way. We introduce codes, invariant with respect to a family of generalized shift operators (GSO). In particle case when this family is a group (cyclic or Abelian), these codes are ordinary cyclic and group codes. They are invariant with respect to this group. We deal with GSO-invariant codes with fast code and encode procedures based on fast generalized

Fouriertransforms.The hope is that these more general structures will lead to larger classes of useful codes “good” properties.

The rest of the paper isorganized as follows: in Section 2, the proposed method based on families of generalized shift operators (GSO) is explained.

2. Methods

2.1. Generalized shift operators

The purpose of this subsection is to introduce the mathematical representations of generalized shift operators associated with arbitrary orthogonal (or unitary) Fourier transforms (*F*–transforms). For illustration, we also particularize our results for many transforms popular in coding and signal theories. The ordinary group shift operators $\left(T_t^\tau f\right)(t) = f(t+\tau)$ play the leading role in all the properties and tools of the Fourier transform mentioned above. In order to develop for each orthogonal transform a similar wide set of tools and properties as the Fourier transform has, we associate a family of commutative generalized shift operators (GSO) with each orthogonal (unitary) transform. Such families form *hypergroups*. In 1934 F. Marty [17,18] and H.S. Wall [19,20] independently introduced the notion of hypergroup. Only in particular cases these families are Abelian groups and hyperharmonic analysis is the classical Fourier harmonic analysis on groups.

Let $f(t):\Omega \to \mathbf{F}$ be a $\mathbf{F}$-valued signal, where $\mathbf{F}$ be a finite field. Usually, $\Omega = [0, N-1]^d$ in coding theory and digital signal processing, where d is the dimension of Ω: $d = \dim(\Omega)$. Let

$$L(\Omega, \mathbf{F}) := \left\{ f(t) \middle| f(t): \Omega \to \mathbf{F}) \right\} \approx \mathbf{F}^{|\Omega|},$$

be vector space of $\mathbf{F}$-valued functions, where $|\Omega| = \mathrm{card}(\Omega) = N^d$.

Thetheory ofgeneralized shift operators was initiated by Levitan[21]–[22]. According to Levitan the family of generalized shift operators (GSOs) $T_t^\tau[f(t)] := f(t($ depending on $\tau \in \Omega$ as a parameter is defined in signal space $L(\Omega, \mathbf{F})$ by the following axioms.

Axiom 1. For all functions $f_1(t), f_2(t) \in L(\Omega, \mathbf{F})$ and any constants $a, b \in \mathbf{F}$ the following relation holds

$$\hat{T}_t^\tau[a \cdot f_1(t) + b \cdot f_2(t)] = a \cdot \hat{T}_t^\tau[f_1(t)] + b \cdot \hat{T}_t^\tau[f_2(t)] \quad (1)$$

Axiom 2. For an arbitrary function $f(t) \in L(\Omega, \mathbf{F}))$ and arbitrary $s, t, r \in \Omega$ it holds

$$\begin{aligned} &T_\tau^r\left[T_t^\tau[f(t)]\right] = T_t^r\left[T_t^\tau[f(t)]\right], \text{ or} \\ &f\left(t(\ (\tau(\ r)\right) = f\left((t(\ r)(\ r\right), \ \textit{i.e.}, \ T_t^{\tau(\ r} = T_{t(\ \tau}^r. \end{aligned} \quad (2)$$

i. e. the GSOs are associative.

Axiom 3. There exists an element $\tau_0 \in \Omega$ with $T_x^{\tau_0}[f(t)] \equiv f(t)$ for all $t \in \Omega$ and for all $f(t) \in L(\Omega, \mathbf{F})$. This means that the family of GSOs contains identity operator.

If moreover the following axiom is fulfilled, then the GSOs are called commutative.

Axiom 4. For any elements $\tau, t \in \Omega$ and arbitrary $f(t) \in L(\Omega, \mathbf{F})$ holds

$$\begin{aligned} &T_\tau^r\left[T_t^\tau[f(t)]\right] = T_r^\tau\left[T_t^r[f(t)]\right], \text{ or} \\ &f\left(t(\ (\tau(\ r)\right) = f\left(t(\ (r(\ \tau)\right), \ \textit{i.e.}, \ T_\tau^r T_t^\tau = T_r^\tau T_t^r \end{aligned} \quad (3)$$

We expand notion GSOs on the more complex signal space. Let $f(t):\Omega \to Alg(\mathbf{F})$ be a $Alg(\mathbf{F})$-valued signal. The set Ω of the values of the variable t constitutes the *domain* of the signal. Usually, $\Omega = [0, N-1]^d$ in coding theory and digital signal processing, where d is the dimension of Ω: $d = \dim(\Omega)$. Theset of $Alg(\mathbf{F})$ of values of the signal $f(t)$ is the *range* of the signal.About the range of the signal we assume, that $Alg(\mathbf{F})$ is a commutative algebra with aninvolution operation

$a \to \bar{a}$, $\forall a \in \mathsf{A}lg(\mathbf{F})$. In particular, if $\mathsf{A}lg(\mathbf{F})$ is the complex field then the involution operation is complex conjugate.

Let Ω^* be the space dual to Ω. The first one will be called the *spectral domain*, the second one be called *signal domain* keeping the original notion of $t \in \Omega$ as «time» and $\omega \in \Omega^*$ as «frequency». Let

$$L(\Omega, \mathsf{A}lg(\mathbf{F})) := \{ f(t) \mid f(t) : \Omega \to \mathsf{A}lg(\mathbf{F}) \} \approx \mathsf{A}lg^{|\Omega|}(\mathbf{F}),$$

$$L(\Omega^*, \mathsf{A}lg(\mathbf{F})) := \{ F(\omega) \mid F(\omega) : \Omega^* \to \mathsf{A}lg(\mathbf{F}) \} \approx \mathsf{A}lg^{|\Omega^*|}(\mathbf{F})$$

be two vector spaces of $\mathsf{A}lg(\mathbf{F})$-valued functions. Here, $|\Omega| = |\Omega^*| = N^d$.

Let $\{\varphi_\omega(x)\}_{\omega \in \Omega^*}$ be an orthonormal system of functions in $L(\Omega, \mathsf{A}lg(\mathbf{F}))$. Then for any function $f(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$ there exists such a function $F(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$, for which the following equations hold:

$$F(\omega) = (\mathsf{F}f)(\omega) = \sum_{t \in \Omega} f(t) \overline{\varphi}_\omega(t), \tag{4}$$

$$f(t) = (\mathsf{F}^{-1}F)(t) = \sum_{\omega \in \Omega^*} F(\omega) \varphi_\omega(t). \tag{5}$$

The function $F(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ is called the Fourier spectrum (F-spectrum) of the $\mathsf{A}lg(\mathbf{F})$-valued signal $f(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and expressions (1)-(2) are called the pair of *generalized Fourier transforms* (or F-transforms). In the following we will use the notation $f(t) \xleftrightarrow{\mathsf{F}} F(\omega)$ in order to indicate F-transforms pair.

A fundamental and important tool of coding and signal theories are shift operators in the «time» and «frequency» domains. They are defined as

$$(T_t^\tau f)(t) := f(t+\tau), \quad (D_\omega^\nu F)(\omega) := F(\omega+\nu),$$
$$(\overline{T}_t^\tau f)(t) := f(t-\tau) \quad \text{and} \quad (\overline{D}_\omega^\nu F)(\omega) := F(\omega-\nu).$$

For $f(t) = e^{j\omega t}$ and $F(\omega) = e^{-j\omega t}$ we have

$$T_t^\tau e^{j\omega t} = e^{j\omega(t+\tau)} = e^{j\omega\tau} e^{j\omega t} = \lambda_\omega(\tau) e^{j\omega t}, \quad D_\omega^\nu e^{j\omega t} = e^{-j(\omega+\nu)t} = e^{-j\nu t} e^{-j\omega t} = \lambda_\nu(t) e^{-j\omega t},$$
$$\overline{T}_t^\tau e^{j\omega t} = e^{j\omega(t-\tau)} = e^{-j\omega\tau} e^{j\omega t} = \overline{\lambda}_\omega(\tau) e^{j\omega t} \quad \text{and} \quad \overline{D}_\omega^\nu e^{j\omega t} = e^{-j(\omega-\nu)t} = e^{j\nu t} e^{-j\omega t} = \overline{\lambda}_\nu(t) e^{-j\omega t},$$

i.e., harmonic signals $e^{j\omega t}$ and $e^{-j\omega t}$ are eigenfunctions of «time»-shift and «frequency»-shift operators $T_t^\tau, \overline{T}_t^\tau$ and $D_\omega^\nu, \overline{D}_\omega^\nu$, correspondingto eigenvalues $\lambda_\omega(\tau) = e^{j\omega\tau}$, $\overline{\lambda}_\omega(\tau) = e^{-j\omega\tau}$ and $\lambda_\nu(t) = e^{-j\nu t}$, $\overline{\lambda}_\nu(t) = e^{j\nu t}$, respectively.

Definition 4. The following operators (with respect to which all basis functions are invariant eigenfunctions)

$$(T_t^\tau \varphi_\omega)(t) := \varphi_\omega(\tau) \cdot \varphi_\omega(t) = \lambda_\omega(\tau) \varphi_\omega(t), \quad \forall \tau \in \Omega,$$
$$(\overline{T}_t^\tau \varphi_\omega)(t) := \overline{\varphi}_\omega(\tau) \cdot \varphi_\omega(t) = \overline{\lambda}_\omega(\tau) \varphi_\omega(t), \quad \forall \tau \in \Omega \tag{6}$$

and

$$(D_\omega^\nu \overline{\varphi}_\omega)(t) := \overline{\varphi}_\nu(t) \cdot \overline{\varphi}_\omega(t) = \lambda_\nu(t) \cdot \overline{\varphi}_\omega(t), \quad \forall \nu \in \Omega^*,$$
$$(\overline{D}_\omega^\nu \overline{\varphi}_\omega)(t) := \varphi_\nu(t) \cdot \overline{\varphi}_\omega(t) = \overline{\lambda}_\nu(t) \cdot \overline{\varphi}_\omega(t), \quad \forall \nu \in \Omega^* \tag{7}$$

are called commutative F–generalized"time"–shift and "frequency"–shift operators (GSO's), respectively, where $\lambda_\omega(\tau) = \varphi_\omega(\tau)$, $\overline{\lambda}_\omega(\tau) = \overline{\varphi}_\omega(\tau)$ and $\lambda_\nu(t) = \overline{\varphi}_\nu(t)$, $\overline{\lambda}_\nu(t) = \varphi_\nu(t)$ are eigenvalues of GSO's $T_t^\tau, \overline{T}_t^\tau$ and $D_\omega^\nu, \overline{D}_\omega^\nu$, respectively.

For these operators we introduce the following designations:

$$\left(T_t^{\tau}\varphi_{\omega}\right)(t) := \varphi_{\omega}(t\,(\,\tau),\quad \left(\overline{T}_t^{\tau}\varphi_{\omega}\right)(t) := \varphi_{\omega}(t\,'\,\tau),\quad \forall\tau\in\Omega,$$
$$\left(D_{\omega}^{\nu}\overline{\varphi}_{\omega}\right)(t) := \overline{\varphi}_{\omega\oplus\nu}(t),\quad \left(\overline{D}_{\omega}^{\nu}\overline{\varphi}_{\omega}\right)(t) := \overline{\varphi}_{\omega\$\,\nu}(t),\quad \forall\nu\in\Omega^{*},$$

Here, symbols "$(\,,\oplus$","$'\,,\$$" denote quasi-sums and quasi-differences, respectively.

If $T_{t,\sigma}^{\tau}, \overline{T}_{t,\sigma}^{\tau}$ and $D_{\omega,\alpha}^{\nu}, \overline{D}_{\omega,\alpha}^{\nu}$ are matrix elements of operators $T_t^{\tau}=\left[T_{t,\sigma}^{\tau}\right]$, $\overline{T}_t^{\tau}=\left[\overline{T}_{t,\sigma}^{\tau}\right]$ and $D_{\omega,\alpha}^{\nu}=\left[D_{\omega,\alpha}^{\nu}\right]$, $\overline{D}_{\omega,\alpha}^{\nu}=\left[\overline{D}_{\omega,\alpha}^{\nu}\right]$, then

$$\begin{aligned}\left(T_t^{\tau}\varphi_{\omega}\right)(t)&=\varphi_{\omega}(t\,(\,\tau)=\varphi_{\omega}(\tau)\cdot\varphi_{\omega}(t)=\sum_{\sigma\in\Omega}T_{t,\sigma}^{\tau}\varphi_{\omega}(\sigma),\\ \left(\overline{T}_t^{\tau}\varphi_{\omega}\right)(t)&=\varphi_{\omega}(t\,'\,\tau)=\overline{\varphi}_{\omega}(\tau)\cdot\varphi_{\omega}(t)=\sum_{\sigma\in\Omega}\overline{T}_{t,\sigma}^{\tau}\varphi_{\sigma}(\sigma),\end{aligned}\tag{8}$$

and

$$\begin{aligned}\left(D_{\omega}^{\nu}\overline{\varphi}_{\omega}\right)(t)&=\overline{\varphi}_{\omega\oplus\nu}(t)=\overline{\varphi}_{\nu}(t)\cdot\overline{\varphi}_{\omega}(t)=\sum_{\alpha\in\Omega^{*}}D_{\omega,\alpha}^{\nu}\overline{\varphi}_{\alpha}(t),\\ \left(\overline{D}_{\omega}^{\nu}\overline{\varphi}_{\omega}\right)(t)&=\overline{\varphi}_{\omega\$\,\nu}(t)=\varphi_{\nu}(t)\cdot\overline{\varphi}_{\omega}(t)=\sum_{\alpha\in\Omega^{*}}\overline{D}_{\omega,\alpha}^{\nu}\overline{\varphi}_{\alpha}(t)\end{aligned}\tag{9}$$

The expressions (8)–(9) are called *multiplication formulae* for basis functions $\left\{\varphi_{\omega}(t)\right\}_{\omega\in\Omega^{*}}\in L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right)$ and $\left\{\varphi_{\omega}(t)\right\}_{t\in\Omega}\in L\left(\Omega^{*},\mathsf{A}lg(\mathbf{F})\right)$. They show that the set of basis functions form two hypergroups with respect to multiplication rules (8) and (9), respectively. Consequently, two spaces $L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right)$ and $L\left(\Omega^{*},\mathsf{A}lg(\mathbf{F})\right)$ form time and frequency algebras with structure constants $T_{t,\sigma}^{\tau}$ and $D_{\omega,\alpha}^{\nu}$, respectively.

From (8) and (9) we easily obtain the matrix elements of the GSOs in time and frequency domains

$$T_{t,\sigma}^{\tau}=\sum_{\omega\in\Omega^{*}}\varphi_{\omega}(\tau)\varphi_{\omega}(t)\overline{\varphi}_{\omega}(\sigma),\quad \overline{T}_{t,\sigma}^{\tau}=\sum_{\omega\in\Omega^{*}}\overline{\varphi}_{\omega}(\tau)\varphi_{\omega}(t)\overline{\varphi}_{\omega}(\sigma),\tag{10}$$

$$D_{\omega,\alpha}^{\nu}=\sum_{t\in\Omega}\overline{\varphi}_{\nu}(t)\overline{\varphi}_{\omega}(t)\varphi_{\alpha}(t),\quad \overline{D}_{\omega,\alpha}^{\nu}=\sum_{t\in\Omega}\varphi_{\nu}(t)\overline{\varphi}_{\omega}(t)\varphi_{\alpha}(t).\tag{11}$$

The expressions (10)–(11) can be compactly written on the operator language

$$\begin{aligned}T_x^{\tau}&=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{\varphi_{\omega}(\tau)\right\}\cdot\mathsf{F},\quad \overline{T}_t^{\tau}=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{\overline{\varphi}_{\omega}(\tau)\right\}\cdot\mathsf{F},\\ D_{\omega}^{\nu}&=\mathsf{F}\cdot\mathrm{diag}\left\{\varphi_{\nu}(t)\right\}\cdot\mathsf{F}^{-1},\quad \overline{D}_{\omega}^{\nu}=\mathsf{F}\cdot\mathrm{diag}\left\{\overline{\varphi}_{\nu}(t)\right\}\cdot\mathsf{F}^{-1}.\end{aligned}\tag{12}$$

where $\mathrm{diag}\left\{\varphi\right\}$ denotes a diagonal matrix which entries consist of values of the function φ.

If there exist such element t_0 that the equation $\varphi_{\omega}(t_0)\equiv 1$ for all $\omega\in\Omega^{*}$ is fulfilled, then there exist the identity GSO in time domain. Indeed, the substitution of t_0 into the expressions (12) gives

$$\begin{aligned}T_t^{t_0}&=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{\varphi_{\omega}(t_0)\right\}\cdot\mathsf{F}=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{1\right\}\cdot\mathsf{F}=\mathsf{F}^{-1}\cdot\mathsf{F}=I,\\ \overline{T}_t^{t_0}&=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{\overline{\varphi}_{\omega}(t_0)\right\}\cdot\mathsf{F}=\mathsf{F}^{-1}\cdot\mathrm{diag}\left\{\overline{1}\right\}\cdot\mathsf{F}=\mathsf{F}^{-1}\cdot\mathsf{F}=I.\end{aligned}\tag{13}$$

If there exist such an element ω_0 that the equation $\varphi_{\omega_0}(x)\equiv 1$ for all $x\in\Omega$ is fulfilled too, then there exist the identity GSO in frequency domain. Indeed, the substitution of ω_0 into the expressions (12) gives

$$\begin{aligned}\hat{D}_{\omega}^{\omega_0}&=\mathsf{F}\cdot\mathrm{diag}\left\{\varphi_{\omega_0}(x)\right\}\cdot\mathsf{F}^{-1}=\mathsf{F}\cdot\mathrm{diag}\left\{1\right\}\cdot\mathsf{F}^{-1}=\mathsf{F}\cdot\mathsf{F}^{-1}=I,\\ \bar{\hat{D}}_{\omega}^{\omega_0}&=\mathsf{F}\cdot\mathrm{diag}\left\{\overline{\varphi}_{\omega_0}(x)\right\}\cdot\mathsf{F}^{-1}=\mathsf{F}\cdot\mathrm{diag}\left\{\overline{1}\right\}\cdot\mathsf{F}^{-1}=\mathsf{F}\cdot\mathsf{F}^{-1}=I.\end{aligned}\tag{13}$$

We see also that two families of time and frequency GSOs form two hypergroups $\mathsf{HG}=\left\{T_t^\tau\right\}_{t\in\Omega}$ and $\mathsf{HG}^*=\left\{D_\omega^\nu\right\}_{\nu\in\Omega}$. By definition, functions $\left\{\varphi_\omega(t)\right\}_{\omega\in\Omega^*}$ and $\left\{\varphi_\omega(t)\right\}_{t\in\Omega}$ are eigenfunctions of GSOs. For this reason we can call them hypercharacters of hypergroups.

For a signal $f(t)\in L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right)$ we define its shifted copies by

$$\begin{aligned}
f(t\,(\,\tau)&=\left(T_t^\tau f\right)(t)=T_t^\tau\left(\sum_{\omega\in\Omega^*}F(\omega)\varphi_\omega(t)\right)=\sum_{\omega\in\Omega^*}F(\omega)\left(T_t^\tau\varphi_\omega\right)(t)=\\
&=\sum_{\omega\in\Omega^*}F(\omega)\varphi_\omega(\tau)\varphi_\omega(t)=\sum_{\omega\in\Omega^*}\left(F(\omega)\varphi_\omega(\tau)\right)\varphi_\omega(t),\\
f(t\,'\,\tau)&=\left(\overline{T}_t^\tau f\right)(t)=\overline{T}_t^\tau\left(\sum_{\omega\in\Omega^*}F(\omega)\varphi_\omega(t)\right)=\sum_{\omega\in\Omega^*}F(\omega)\left(\overline{T}_t^\tau\varphi_\omega\right)(t)=\\
&=\sum_{\omega\in\Omega^*}F(\omega)\overline{\varphi}_\omega(\tau)\varphi_\omega(t)=\sum_{\omega\in\Omega^*}\left(F(\omega)\overline{\varphi}_\omega(\tau)\right)\varphi_\omega(t).
\end{aligned}\tag{14}$$

Analogously, for a spectrum $F(\omega)\in L\left(\Omega^*,\mathsf{A}lg(\mathbf{F})\right)$

$$\begin{aligned}
F(\omega\oplus\nu)&=\left(D_\omega^\nu F\right)(\omega)=D_\omega^\nu\left(\sum_{\omega\in\Omega^*}f(t)\overline{\varphi}_\omega(t)\right)=\sum_{\omega\in\Omega^*}f(t)\left(D_\omega^\nu\overline{\varphi}_\omega\right)(t)=\\
&=\sum_{\omega\in\Omega^*}f(t)\overline{\varphi}_\nu(t)\overline{\varphi}_\omega(t)=\sum_{\omega\in\Omega^*}\left(f(t)\overline{\varphi}_\nu(t)\right)\overline{\varphi}_\omega(t),\\
F(\omega\,\$\,\nu)&=\left(\overline{D}_\omega^\nu F\right)(\omega)=\overline{D}_\omega^\nu\left(\sum_{\omega\in\Omega^*}f(t)\overline{\varphi}_\omega(t)\right)=\sum_{\omega\in\Omega^*}f(t)\left(\overline{D}_\omega^\nu\overline{\varphi}_\omega\right)(t)=\\
&=\sum_{\omega\in\Omega^*}f(t)\varphi_\nu(t)\overline{\varphi}_\omega(t)=\sum_{\omega\in\Omega^*}\left(f(t)\varphi_\nu(t)\right)\overline{\varphi}_\omega(t).
\end{aligned}\tag{15}$$

We will need in the following modulation operators:

$$\left(M_t^\nu f\right)(t):=\varphi_\nu(t)f(t),\qquad\left(\overline{M}_t^\nu f\right)(t):=\overline{\varphi}_\nu(t)f(t),$$

$$\left(M_\omega^\tau F\right)(\omega):=\varphi_\omega(\tau)F(\omega),\quad\left(\overline{M}_\omega^\tau F\right)(\omega):=\overline{\varphi}_\omega(\tau)F(\omega).$$

From the GSOs definition it follows the following result (two theorems about shifts and modulations). Shifts and modulations are connected as follows:

$$f(t\,(\,\tau)\overset{\mathsf{F}}{\longleftrightarrow}F(\omega)\varphi_\omega(\tau),\qquad f(t\,'\,\tau)\overset{\mathsf{F}}{\longleftrightarrow}F(\omega)\overline{\varphi}_\omega(\tau),$$

$$\left(T_t^\tau f\right)(t)\overset{\mathsf{F}}{\longleftrightarrow}\left(M_\omega^\tau F\right)(\omega),\quad\left(\overline{T}_t^\tau f\right)(t)\overset{\mathsf{F}}{\longleftrightarrow}\left(\overline{M}_\omega^\tau F\right)(\omega)$$

and

$$F(\omega\oplus\nu)\overset{\mathsf{F}}{\longleftrightarrow}f(t)\overline{\varphi}_\nu(t),\qquad F(\omega\,\$\,\nu)\overset{\mathsf{F}}{\longleftrightarrow}f(t)\overline{\varphi}_\nu(t)$$

$$\left(D_\omega^\nu F\right)(\omega)\overset{\mathsf{F}}{\longleftrightarrow}\left(M_t^\nu f\right)(t),\quad\left(\overline{D}_\omega^\nu F\right)(\omega)\overset{\mathsf{F}}{\longleftrightarrow}\left(\overline{M}_t^\nu f\right)(t).$$

2.2. Generalized convolutions and correlations

Using the notion GSO, we can formally generalize the definitions of convolution and correlation.

Definition 5. The following functions

$$y(t):=\left(h\lozenge x\right)(t)=\sum_{\tau\in\Omega}h(\tau)x\left(t\,'\,\tau\right),\ Y\left(\omega\right):=\left(H\vee F\right)\left(\omega\right)=\sum_{\nu\in\Omega^*}H\left(\nu\right)F\left(\omega\,\$\,\nu\right)$$

and

$$c(\tau)=\left(f\clubsuit g\right)(\tau):=\sum_{t\in\Omega}f(t)\overline{g}\left(t\,'\,\tau\right),\ \ C(\nu)=\left(F\spadesuit G\right)\left(\nu\right):=\sum_{\omega\in\Omega^*}F\left(\omega\right)\overline{G}\left(\omega\,\$\,\nu\right)$$

are called the $\Diamond$- and $\heartsuit$- convolutions and the cross $\clubsuit$- and $\spadesuit$- correlation functions, respectively, associated with a classical Fourier transform F. If $f = g$ and $F = G$ then cross correlation functions are called the $\clubsuit$- and $\spadesuit$- autocorrelation functions.

The spaces $L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ equipped multiplications $\Diamond$ and $\heartsuit$ form commutative signal and spectral convolution algebras $\langle L(\Omega, \mathsf{A}lg(\mathbf{F})), \Diamond \rangle$ and $\langle L(\Omega^*, \mathsf{A}lg(\mathbf{F})), \heartsuit \rangle$, respectively.

Theorem 1. Let us take two triplets $y_1(t), h_1(t), x_1(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $y_2(t), h_2(t), x_2(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$. Obviously, $Y_1(\omega), H_1(\omega), X_1(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ and $Y_2(\omega), H_2(\omega), X_2(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$. Let

$$y_1(t) = (h_1 \Diamond x_1)(t) = \sum_{\tau \in \Omega} h_1(\tau) x_1(t \text{ '} \tau) \quad \text{and} \quad Y_2(\omega) = (H_2 \heartsuit X_2)(\omega) = \sum_{\nu \in \Omega^*} H_2(\nu) F_2(\omega \$ \nu)$$

then generalized Fourier transforms F and F^{-1} map $\Diamond$-and $\heartsuit$-convolutions into the products of spectra and signals, respectively,

$$\mathsf{F}\{y_1\} = \mathsf{F}\{h_1 \Diamond x_1\} = \mathsf{F}\{h_1\} \cdot \mathsf{F}\{x_1\}, \quad \mathsf{F}^{-1}\{Y_2\} := \mathsf{F}^{-1}\{H_2 \heartsuit X_2\} = \mathsf{F}^{-1}\{H_2\} \cdot \mathsf{F}^{-1}\{X_2\},$$

i.e.,

$$y_1(t) = (h_1 \Diamond x_1)(t) \overset{\mathsf{F}}{\longleftrightarrow} Y_1(\omega) = H_1(\omega) \cdot X_1(\omega), \quad y_2(t) = h_2(t) x_2(t) \overset{\mathsf{F}}{\longleftrightarrow} Y_2(\omega) = (H_2 \heartsuit X_2)(\omega).$$

Theorem 2. Let us take two triplets $c_1(t), f_1(t), g_1(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $c_2(t), f_2(t), g_2(t) \in L(\Omega, \mathsf{A}lg(\mathbf{F}))$. Obviously, $C_1(\omega), F_1(\omega), G_1(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ and $C_2(\omega), F_2(\omega), G_2(\omega) \in L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$. Let

$$c_1(\tau) = (f_1 \clubsuit g_1)(\tau) = \sum_{t \in \Omega} f_1(t) \overline{g}_1(t \text{ '} \tau), \text{ and } C_2(\omega) = (F_2 \spadesuit G_2)(\nu) = \sum_{\omega \in \Omega^*} F_2(\omega) \overline{G}_2(\omega \$ \nu),$$

then generalized Fourier transforms F and F^{-1} map $\clubsuit$- and $\spadesuit$-correlations into the products of spectra and signals, respectively,

$$\mathsf{F}\{c_1\} = \mathsf{F}\{f_1 \Diamond g_1\} = \mathsf{F}\{f_1\} \cdot \mathsf{F}\{g_1\}, \quad \mathsf{F}^{-1}\{C_2\} := \mathsf{F}^{-1}\{F_2 \heartsuit G_2\} = \mathsf{F}^{-1}\{F_2\} \cdot \mathsf{F}^{-1}\{G_2\},$$

i.e.,

$$c_1(\tau) = (f_1 \clubsuit g_1)(\tau) \overset{\mathsf{F}}{\longleftrightarrow} C_1(\omega) = F_1(\omega) \cdot \overline{G}_1(\omega),), \quad c_2(t) = f_2(t) g_2(t) \overset{\mathsf{F}}{\longleftrightarrow} C_2(\omega) = (F_2 \heartsuit G_2)(\omega).$$

2.3. Codes invariant with respect to generalized shift operators

We are going to consider block codes of length N as subsets $\mathsf{C} \subset L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $\mathsf{C}^* \subset L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$, i.e., a collections of N length vectors with components from $Alg(\mathbf{F})$. Let $\{\varphi_\omega(t)\}_{t \in \Omega}$ and $\{\varphi_\omega(t)\}_{\omega \in \Omega^*}$ be orthonormal systems of functions for $L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$, respectively. They generate two hypergroups HG- and HG^*, respectively.

Definition 6. HG- and HG^*- invariant block codes $\mathsf{C} \subset L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $\mathsf{C}^* \subset L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ are linear block codes with the property that if $c(t) \in \mathsf{C}$ and $C(\omega) \in \mathsf{C}^*$ then

$(T_t^\tau c)(t) = c(t \text{ '} \tau) \in \mathsf{C}, \ \forall T_t^\tau \in \mathsf{HG}$ and $(D_\omega^\nu C)(\omega) = C(\omega \$ \nu) \in \mathsf{C}, \ \forall D_\omega^\nu \in \mathsf{HG}^*$, respectively.

It means that hypergroups of generalized code symmetry of HG- and HG^*- invariant block codes $\mathsf{C} \subset L(\Omega, \mathsf{A}lg(\mathbf{F}))$ and $\mathsf{C}^* \subset L(\Omega^*, \mathsf{A}lg(\mathbf{F}))$ is $\mathbf{Symm}\{\mathsf{C}\} \approx \mathsf{HG}$ and $\mathbf{Symm}\{\mathsf{C}\}^* \approx \mathsf{HG}^*$.

Reed-Solomon (RS) codes are nonbinary cyclic codes [23]. The most natural definition of HG- and HG^*- invariant RS codesare in terms of a certain evaluation maps from the subspace $\mathsf{A}lg^k(\mathbf{F})$ of all k-tuples $\mathbf{m} = (m_0, m_1, ..., m_{k-1})$ (information symbols = massage) over $\mathsf{A}lg(\mathbf{F})$ to the set of codewords $\mathsf{C} \cong Cod[N, k \mid \mathsf{A}lg(\mathbf{F})] \subset L(\Omega, \mathsf{A}lg(\mathbf{F}))$

$$\mathbf{m}=(m_0,m_1,...,m_{k-1})\mapsto \mathbf{c}(t)=(c(0),c(1),...,c(N-1))$$
$$\mathsf{A}lg^k(\mathbf{F}) \to L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right) \quad (16)$$

or to the set of codewords $\mathsf{C}^*=Cod^*\left[N,k\,|\,\mathsf{A}lg(\mathbf{F})\right]\subset L\left(\Omega^*,\mathsf{A}lg(\mathbf{F})\right)$

$$\mathbf{m}=(m_0,m_1,...,m_{k-1})\mapsto C(t)=(C(0),C(1),...,C(N-1))$$
$$\mathsf{A}lg^k(\mathbf{F}) \to L\left(\Omega^*,\mathsf{A}lg(\mathbf{F})\right)$$

Definition 7. We define an encoding function for HG- and HG^*- invariant Reed-Solomon codes as

HG-RS: $\mathsf{A}lg^k(\mathbf{F}) \to L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right)$,

HG^*-RS: $\mathsf{A}lg^k(\mathbf{F}) \to L\left(\Omega^*,\mathsf{A}lg(\mathbf{F})\right)$

in the following forms. A message $\mathbf{m}=(m_0,m_1,...,m_{k-1})$ with $m_i\in\mathsf{A}lg(\mathbf{F})$ are transformed by F and F^{-1}:

$$\begin{bmatrix} C(0)\\ C(1)\\ C(2)\\ ....\\ ...\\ C(N-2)\\ C(N-1)\end{bmatrix}=\mathsf{F}\begin{bmatrix} m_0\\ m_1\\ ...\\ m_{k-1}\\ 0\\ ...\\ 00\end{bmatrix},\quad \begin{bmatrix} c(0)\\ c(1)\\ c(2)\\ ....\\ ...\\ c(N-2)\\ c(N-1)\end{bmatrix}=\mathsf{F}^{-1}\begin{bmatrix} m_0\\ m_1\\ ...\\ m_{k-1}\\ 0\\ ...\\ 00\end{bmatrix},$$

Hence, generator matrices for HG- and HG^*- invariant Reed-Solomon codesare the generalized Fourier matrices F and F^{-1}.

Convolutional cyclic codes (CC's, for short) form an important class of error-correcting codes in engineering practice. The mathematical theory of these codes has been set off by theseminal papers of Forney [24] and Massey et al. [25].

Definition 8. HG- and HG^*- invariant convolutional codes of length N and dimension k are ideals $\left\langle h(t)\right\rangle$, $\left\langle G(\omega)\right\rangle$ of $\left\langle L\left(\Omega,\mathsf{A}lg(\mathbf{F})\right),\lozenge\right\rangle$ and $\left\langle L\left(\Omega^*,\mathsf{A}lg(\mathbf{F})\right),\blacktriangledown\right\rangle$ having the following forms

$$c(t)=\left(h\lozenge m\right)(t)=\sum_{\tau\in\Omega}h(t'\ \tau)m(\tau) \text{ and } \ C(\omega)=\left(G\blacktriangledown m\right)(\omega)=\sum_{\nu\in\Omega^*}G\left(\omega\,\$\,\nu\right)m(\nu)$$

where

$$H(\omega)=\left(\mathsf{F}h\right)(\omega)=\left(H(0),H(1),...,H(k-1),0,...,0\right)\in\mathsf{A}lg^k(\mathbf{F}),$$
$$g(\omega)=\left(\mathsf{F}^{-1}G\right)(t)=\left(g(0),g(1),...,g(k-1),0,...,0\right)\in\mathsf{A}lg^k(\mathbf{F}).$$

We call matrices $\mathbf{G}=\left[G\left(\omega\,\$\,\nu\right)\right]_{\omega,\nu\in\Omega^*}$ and $\mathbf{H}=\left[h(t'\ \tau)\right]_{t,\tau\in\Omega}$ encoders.

It is easy to see that cyclic convolutional codes and group convolutional codes are particular cases of HG- and HG^*- invariant convolutional codes.

3. Conclusion

In this paper we studied a new class of codes with generalized symmetry. They are invariant with respect to a family of generalized shift operators HGor HG^*. In particle case when this family is a group (cyclic or Abelian), these codes are ordinary cyclic and group codes.We deal with GSO-invariant codes with fast code and encode procedures based on fast generalized Fouriertransforms.The hope is that these more general

4. Acknowledgments

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

5. References

[1] Berlekamp, E.R. Negacyclic codes for the Lee metric / E.R. Berlekamp // Combinatorial Mathematics and its Applications. – N.C.: Univ. North Carolina, Chapel Hill.,1969. – P. 298-316.

[2] Berlekamp, E.R. Algebraic coding theory / E.R. Berlekamp. – Agean Park Press, 1984.

[3] Sergio, R.L-P. Dual generalizations of the concept of cyclicity of codes / R.L-P. Sergio, R. Benigno // Adv. Math. Commun. – 2009. – Vol. 3(3). – P. 227-234.

[4] Boucher, D. Skew-cyclic codes / D. Boucher, W. Geiselmann, F. Ulmer // Appl. Algebra Eng. Comm. Comput. – 2007. – Vol. 18(4). – P. 379-389.

[5] Delphine, B. Skew constacyclic codes over Galois rings / B. Delphine, S. Patrick, U. Felix // Adv. Math. Commun. – 2008. – Vol. 2(3). – P. 273-292.

[6] Delphine, B. Coding with skew polynomial rings / B. Delphine, U. Felix // Adv. Math. Commun. – 2008. – Vol. 3(3). – P. 2543-276.

[7] Hai, Q.D. Negacyclic codes of length 2s over Galois rings / Q.D. Hai // IEEE Trans. Inform. Theory. – 2005. – Vol. 51(12). – P. 4252-4262.

[8] Hai, Q.D. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions / / Q.D. Hai // Finite Fields Appl. – 2008. – Vol. 14(1). – P. 22-40.

[9] Hai, Q.D. On the structure of cyclic and negacyclic codes over finite chain rings / Q.D. Hai, R.L. Sergio, S. Szabo // Codes over rings. Vol. 16. World Scientific Publishing, 2009. – N.J.: Co. Pte.

[10] Hai, Q.D. Cyclic and negacyclic codes over finite chain rings / Q.D. Hai, R.L. Sergio // IEEE Trans. Inform. Theory. – 2004. – Vol. 50(8). – P. 1728-1744.

[11] Hakan, O. A note on negacyclic and cyclic codes of length *p^s* over a finite field of characteristic *p* / O. Hakan, O. Ferruh // Adv. Math. Commun. – 2009. – Vol. 3(3). – P. 265-271.

[12] Hai, Q. Dinh. Structure of some classes of repeated-root constacyclic codes over integers modulo 2m / Q. Hai // Groups, rings and group rings. Vol. 248 Lect. Notes Pure Appl. Math. – Boca Raton: Chapman & Hall/CRC, 2006. – P. 105-117.

[13] Sundar, R.B. Transform Domain Characterization of Abelian codes / R.B. Sundar, M.U. Siddigi // IEEE Trans. Inform. Theory. – 1994. – Vol. 40. – P.2082-2090.

[14] Berman, S.D. Semi-simple cyclic and abelian codes / S.D. Berman // Kibernetica. – 1967. – Vol. 3. – P.20-30.

[15] Camion, P. Abelian codes / P. Camion // Tech. Rep. – University of Wisconsin, 1970. – Vol. 1059.

[16] MacWilliams, F.J. Binary codes which are ideals in the group algebra of an abelian group / F.J. MacWilliams // BSTJ. – 1970. – Vol. 49. – P. 987-1011.

[17] Marty, F. Sur une generalization de la notion de groupe / F. Marty // Sartryckur Forhandlingar Via Altonde Skandinavioka Matematiker kongresseni. – 1934. – P. 45-49.

[18] Marty, F. Role de la notion d'hypergroupedansl'etude des groupes non abelians / F. Marty // Computes Rendus de l'Academie des Sciences. – 1937. – Vol. 201. – P. 636-638

[19] Wall, H.S. Hypergroups / H.S. Wall //Bulletin of the American Mathematical Socity. –Vol.41. – P. 36-40.

[20] Wall, H.S. Hypergroups / H.S. Wall // American Journal of Mathematics. – 1937. – Vol. 59. – P. 77-98.

[21] Levitan, B.M. The application of generalized displacement operators to linear differential equations of second order / B.M. Levitan // Uspechi Math. Nauk. – 1949. – Vol. 4(29). – P. 3-112.

[22] Levitan, B.M. Generalized translation operators / B.M. Levitan // Israel Program for Scientific Translations, Jerusalem, 1964.

[23] Reed, I.S. Polynomial Codes Over Certain Finite Fields / I.S. Reed, G. Solomon // SIAM Journal of Applied Math. – 1960. – Vol. 3. – P. 300-304.

[24] Forney, G.D. Convolutional codes I: Algebraic structure / G.D. Forney // IEEE Trans. Inform. Theory. – 1970. – Vol. 16. – P. 720-738.

[25] Massey, J.L. Codes, automata, and continuous systems: Explicit Interconnections / J.L. Massey, M.K. Sain // IEEE Trans. Aut. Contr. – 1967. – AC-12. –P. 644-650.