

Linear codes invariant with respect to generalized shift operators

V G Labunets¹ and E Ostheimer²

¹Ural State Forest Engineering University, Sibirsky trakt 37, Ekaterinburg, Russia, 620100

²Capricat LLC, Pompano Beach, Florida, US

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 particular 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 Fourier transforms. The hope is that these more general structures will lead to larger classes of useful codes "good" properties.

1. Introduction

Let \mathbf{F} be a finite field. A *block code* of length N is a subset \mathbf{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* $\mathbf{C} \subset \mathbf{F}^N$ of length N over a finite field \mathbf{F} is a linear block code with the property that if $(c_0, c_1, \dots, c_{N-2}, c_{N-1}) \in \mathbf{C}$ then $(c_{N-1}, c_0, \dots, c_{N-3}, c_{N-2}) \in \mathbf{C}$.

It means that group of code symmetry of a cyclic code $\mathbf{C} \subset \mathbf{F}^N$ is $\text{Symm}\{\mathbf{C}\} \approx \mathbf{Z}_N$. Cyclic codes are studied from many points of view. One way is to view them as ideals of an algebra. Define $\rho: \mathbf{F}^N \rightarrow \mathbf{F}[x]/\langle x^N - 1 \rangle$ via $\rho: (c_0, c_1, \dots, c_{N-2}, c_{N-1}) \mapsto c_0 + c_1x + \dots + c_{N-2}x^{N-2} + c_{N-1}x^{N-1}$. It can be shown that ρ is an isomorphism. Let $\mathbf{C} \subset \mathbf{F}^N$ be cyclic block code. Then $\rho(\mathbf{C})$ is a subspace of the \mathbf{F} -vector space $\mathbf{F}[x]/\langle x^N - 1 \rangle$. Now the added condition of being cyclic translates to the following: if $\rho(c) \in \rho(\mathbf{C})$ then $x \cdot \rho(c) = x \cdot (c_0 + c_1x + \dots + c_{N-2}x^{N-2} + c_{N-1}x^{N-1}) = (c_{N-1} + c_0x + c_1x^2 + \dots + c_{N-2}x^{N-1}) \in \rho(\mathbf{C})$.

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

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 $Alg^N(\mathbf{F})[x]/\langle x^N + 1 \rangle$,
- constacyclic codes [12]- ideal of the ring $Alg^N(\mathbf{F})[x]/\langle x^N - \lambda \rangle$, where $\lambda \in Alg(\mathbf{F})$,
- polycyclic codes [3]- ideal of the ring $Alg^N(\mathbf{F})[x]/\langle f(x) \rangle$, where $f(x) \in Alg(\mathbf{F})[x]$.

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

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

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

Definition 2. For any integer $i \in \{0, 1, 2, \dots, N-1\}$, let $i = (i_{n-1}, i_{n-2}, \dots, i_1, i_0)$. Denote its radix-2 representation, where $i = i_{n-1}2^{n-1} + i_{n-2}2^{n-2} + \dots + i_12^1 + i_02^0 = \sum_{l=0}^{n-1} i_l 2^l$ and $i_l \in \{0, 1\}$ for $l = 0, 1, 2, \dots, n-1$.

Dyadic addition of two numbers i and j denoted by $i \oplus_2 j$ is defined by

$$\begin{aligned} k &= i \oplus_2 j = (i_{n-1}, i_{n-2}, \dots, i_1, i_0) \oplus_2 (j_{n-1}, j_{n-2}, \dots, j_1, j_0) = \\ &= (i_{n-1} \oplus j_{n-1}, i_{n-2} \oplus j_{n-2}, \dots, i_1 \oplus j_1, i_0 \oplus j_0) = (k_{n-1}, k_{n-2}, \dots, k_1, k_0) \end{aligned}$$

where $k_l = (i_l \oplus j_l) \bmod 2$, for $l = 0, 1, 2, \dots, n-1$. The dyadic shift, $m = 0, 1, 2, \dots, N-1$, of a vector $(c_0, c_1, \dots, c_{N-1})$ is the vector $(c_{0 \oplus_2 m}, c_{1 \oplus_2 m}, \dots, c_{(N-1) \oplus_2 m})$.

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 $m = 0, 1, 2, \dots, N-1$.

The class of dyadic codes is a special case of abelian group codes [13, 14-16] which is briefly discussed in the third. In this paper, we would like 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 particular 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 Fourier transforms. The hope is that these more general structures will lead to larger classes of useful codes "good" properties. The rest of the paper is organized as follows: in Section 2 and 3, the proposed method based on families of generalized shift operators (GSO) is explained.

2. Methods

2.1. Generalized shift operator

The purpose of this subsection is to introduce the mathematical representations of generalized shift operators associated with arbitrary orthogonal (or unitary) Fourier transforms (\mathbf{F} -transforms). For illustration, we also particularize our results for many transforms popular in coding and signal theories. The ordinary group shift operators $(T_t^\tau f)(t) = f(t + \tau)$ 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 $f(t):\Omega \rightarrow \mathbf{F}$ 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

$$L(\Omega, \mathbf{F}) := \{f(t) | f(t):\Omega \rightarrow \mathbf{F}\} \approx \mathbf{F}^{|\Omega|},$$

be vector space of \mathbf{F} -valued functions, where $|\Omega| = \text{card}(\Omega) = N^d$. The theory of generalized shift operators was initiated by Levitan [21]–[22]. According to Levitan the family of generalized shift operators (GSOs) $T_\tau[f(t)] := f(t(\tau))$ 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

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

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

$$T_\tau^r[T_\tau[f(t)]] = T_\tau[T_r[f(t)]], \text{ or } f(t(\tau(\mathbf{r}))) = f((t(\mathbf{r}))(\tau)), \text{ i.e., } T_\tau^r = T_\tau^r. \quad (2)$$

i. e., the GSOs are associative.

Axiom 3. There exists an element $\tau_0 \in \Omega$ with $T_{\tau_0}[f(t)] \equiv f(t)$ 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

$$T_\tau^r[T_\tau[f(t)]] = T_\tau^r[T_r[f(t)]], \text{ or } f(t(\tau(\mathbf{r}))) = f((r(\tau))(\mathbf{r})), \text{ i.e., } T_\tau^r T_\tau^r = T_\tau^r T_\tau^r \quad (3)$$

We expand notion GSOs on the more complex signal space. Let $f(t):\Omega \rightarrow \text{Alg}(\mathbf{F})$ be a $\text{Alg}(\mathbf{F})$ -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 : $d = \dim(\Omega)$. The set $\text{Alg}(\mathbf{F})$ of values of the signal $f(t)$ is the *range* of the signal. About the range of the signal we assume, that $\text{Alg}(\mathbf{F})$ is a commutative algebra with aninvolution operation $a \rightarrow \bar{a}$, $\forall a \in \text{Alg}(\mathbf{F})$. In particular, if $\text{Alg}(\mathbf{F})$ 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

$$L(\Omega, \text{Alg}(\mathbf{F})) := \{f(t) | f(t):\Omega \rightarrow \text{Alg}(\mathbf{F})\} \approx \text{Alg}^{|\Omega|}(\mathbf{F}),$$

$$L(\Omega^*, \text{Alg}(\mathbf{F})) := \{F(\omega) | F(\omega):\Omega^* \rightarrow \text{Alg}(\mathbf{F})\} \approx \text{Alg}^{|\Omega^*|}(\mathbf{F})$$

be two vector spaces of $\text{Alg}(\mathbf{F})$ -valued functions. Here $|\Omega| = |\Omega^*| = N^d$. Let $\{\varphi_\omega(x)\}_{\omega \in \Omega^*}$ be an orthonormal system of functions in $L(\Omega, \text{Alg}(\mathbf{F}))$. Then for any function $f(t) \in L(\Omega, \text{Alg}(\mathbf{F}))$ there exists such a function $F(\omega) \in L(\Omega^*, \text{Alg}(\mathbf{F}))$, for which the following equations hold:

$$F(\omega) = (\mathbf{F}f)(\omega) = \sum_{t \in \Omega} f(t)\bar{\varphi}_\omega(t), \quad f(t) = (\mathbf{F}^{-1}F)(t) = \sum_{\omega \in \Omega^*} F(\omega)\varphi_\omega(t). \quad (4)$$

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

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

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

$$\begin{cases} T_t^\tau e^{j\omega t} = e^{j\omega(t+\tau)} = e^{j\omega\tau} e^{j\omega t} = \lambda_\omega(\tau) e^{j\omega t}, \\ \bar{T}_t^\tau e^{j\omega t} = e^{j\omega(t-\tau)} = e^{-j\omega\tau} e^{j\omega t} = \bar{\lambda}_\omega(\tau) e^{j\omega t} \end{cases}, \text{ and } \begin{cases} D_\omega^\nu e^{j\omega t} = e^{-j(\omega+\nu)t} = e^{-j\nu t} e^{-j\omega t} = \lambda_\nu(t) e^{-j\omega t}, \\ \bar{D}_\omega^\nu e^{j\omega t} = e^{-j(\omega-\nu)t} = e^{j\nu t} e^{-j\omega t} = \bar{\lambda}_\nu(t) e^{-j\omega t}, \end{cases} \quad (5)$$

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

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

$$\begin{aligned} (T_t^\tau \varphi_\omega)(t) &:= \varphi_\omega(\tau) \cdot \varphi_\omega(t) = \lambda_\omega(\tau) \varphi_\omega(t), \quad \forall \tau \in \Omega, \\ (\bar{T}_t^\tau \varphi_\omega)(t) &:= \bar{\varphi}_\omega(\tau) \cdot \varphi_\omega(t) = \bar{\lambda}_\omega(\tau) \varphi_\omega(t), \quad \forall \tau \in \Omega \end{aligned} \quad (6)$$

and

$$\begin{aligned} (D_\omega^\nu \bar{\varphi}_\omega)(t) &:= \bar{\varphi}_\nu(t) \cdot \bar{\varphi}_\omega(t) = \lambda_\nu(t) \cdot \bar{\varphi}_\omega(t), \quad \forall \nu \in \Omega^*, \\ (\bar{D}_\omega^\nu \bar{\varphi}_\omega)(t) &:= \varphi_\nu(t) \cdot \bar{\varphi}_\omega(t) = \bar{\lambda}_\nu(t) \cdot \bar{\varphi}_\omega(t), \quad \forall \nu \in \Omega^* \end{aligned} \quad (7)$$

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

For these operators we introduce the following designations:

$$\begin{aligned} (T_t^\tau \varphi_\omega)(t) &:= \varphi_\omega(t \oplus \tau), \quad (\bar{T}_t^\tau \varphi_\omega)(t) := \varphi_\omega(t' \tau), \quad \forall \tau \in \Omega, \\ (D_\omega^\nu \bar{\varphi}_\omega)(t) &:= \bar{\varphi}_{\omega \oplus \nu}(t), \quad (\bar{D}_\omega^\nu \bar{\varphi}_\omega)(t) := \bar{\varphi}_{\omega \$ \nu}(t), \quad \forall \nu \in \Omega^*, \end{aligned}$$

here, symbols “(, ⊕”, “(, \$ ” denote quasi-sums and quasi-differences, respectively. If $T_{t,\sigma}^\tau, \bar{T}_{t,\sigma}^\tau$ and $D_{\omega,\alpha}^\nu, \bar{D}_{\omega,\alpha}^\nu$ are matrix elements of operators $T_t^\tau = [T_{t,\sigma}^\tau]$, $\bar{T}_t^\tau = [\bar{T}_{t,\sigma}^\tau]$ and $D_{\omega,\alpha}^\nu = [D_{\omega,\alpha}^\nu]$, $\bar{D}_{\omega,\alpha}^\nu = [\bar{D}_{\omega,\alpha}^\nu]$, then

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

and

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

The expressions (8)–(9) are called *multiplication formulae* for basis functions $\{\varphi_\omega(t)\}_{\omega \in \Omega^*} \in L(\Omega, \text{Alg}(\mathbf{F}))$ and $\{\varphi_\omega(t)\}_{t \in \Omega} \in L(\Omega^*, \text{Alg}(\mathbf{F}))$. They show that the set of basis functions form two hypergroups with respect to multiplication rules (8) and (9), respectively. Consequently, two

spaces $L(\Omega, Alg(\mathbf{F}))$ and $L(\Omega^*, Alg(\mathbf{F}))$ form time and frequency algebras with structure constants $T_{t,\sigma}^\tau$ and $D_{\omega,\alpha}^v$, respectively.

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

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

$$D_{\omega,\alpha}^v = \sum_{t \in \Omega} \bar{\varphi}_v(t) \bar{\varphi}_\omega(t) \varphi_\alpha(t), \quad D_{\omega,\alpha}^v = \sum_{t \in \Omega} \varphi_v(t) \bar{\varphi}_\omega(t) \varphi_\alpha(t). \quad (11)$$

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

$$\begin{aligned} T_x^\tau &= \mathbf{F}^{-1} \cdot \text{diag}\{\varphi_\omega(\tau)\} \cdot \mathbf{F}, \quad \bar{T}_t^\tau = \mathbf{F}^{-1} \cdot \text{diag}\{\bar{\varphi}_\omega(\tau)\} \cdot \mathbf{F}, \\ D_\omega^v &= \mathbf{F} \cdot \text{diag}\{\varphi_v(t)\} \cdot \mathbf{F}^{-1}, \quad \bar{D}_\omega^v = \mathbf{F} \cdot \text{diag}\{\bar{\varphi}_v(t)\} \cdot \mathbf{F}^{-1}, \end{aligned} \quad (12)$$

where $\text{diag}\{\varphi\}$ 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

$$\begin{aligned} T_t^{t_0} &= \mathbf{F}^{-1} \cdot \text{diag}\{\varphi_\omega(t_0)\} \cdot \mathbf{F} = \mathbf{F}^{-1} \cdot \text{diag}\{1\} \cdot \mathbf{F} = \mathbf{F}^{-1} \cdot \mathbf{F} = I, \\ \bar{T}_t^{t_0} &= \mathbf{F}^{-1} \cdot \text{diag}\{\bar{\varphi}_\omega(t_0)\} \cdot \mathbf{F} = \mathbf{F}^{-1} \cdot \text{diag}\{\bar{1}\} \cdot \mathbf{F} = \mathbf{F}^{-1} \cdot \mathbf{F} = I. \end{aligned} \quad (13)$$

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

$$\begin{aligned} \hat{D}_\omega^{\omega_0} &= \mathbf{F} \cdot \text{diag}\{\varphi_{\omega_0}(x)\} \cdot \mathbf{F}^{-1} = \mathbf{F} \cdot \text{diag}\{1\} \cdot \mathbf{F}^{-1} = \mathbf{F} \cdot \mathbf{F}^{-1} = I, \\ \bar{\hat{D}}_\omega^{\omega_0} &= \mathbf{F} \cdot \text{diag}\{\bar{\varphi}_{\omega_0}(x)\} \cdot \mathbf{F}^{-1} = \mathbf{F} \cdot \text{diag}\{\bar{1}\} \cdot \mathbf{F}^{-1} = \mathbf{F} \cdot \mathbf{F}^{-1} = I. \end{aligned}$$

We see also that two families of time and frequency GSOs form two hypergroups $\mathbf{HG} = \{T_t^\tau\}_{t \in \Omega}$ and $\mathbf{HG}^* = \{D_\omega^v\}_{v \in \Omega}$. By definition, functions $\{\varphi_\omega(t)\}_{\omega \in \Omega^*}$ and $\{\varphi_\omega(t)\}_{t \in \Omega}$ are eigenfunctions of GSOs. For this reason we can call them hypercharacters of hypergroups. For a signal $f(t) \in L(\Omega, Alg(\mathbf{F}))$ we define its shifted copies by

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

Analogously, for a spectrum $F(\omega) \in L(\Omega^*, Alg(\mathbf{F}))$

$$\begin{aligned} F(\omega \oplus v) &= (D_\omega^v F)(\omega) = D_\omega^v \left(\sum_{t \in \Omega} f(t) \bar{\varphi}_\omega(t) \right) = \sum_{t \in \Omega} f(t) (D_\omega^v \bar{\varphi}_\omega)(t) = \\ &= \sum_{t \in \Omega} f(t) \bar{\varphi}_v(t) \bar{\varphi}_\omega(t) = \sum_{t \in \Omega} (f(t) \bar{\varphi}_v(t)) \bar{\varphi}_\omega(t), \\ F(\omega \oplus \$ v) &= (\bar{D}_\omega^v F)(\omega) = \bar{D}_\omega^v \left(\sum_{t \in \Omega} f(t) \bar{\varphi}_\omega(t) \right) = \sum_{t \in \Omega} f(t) (\bar{D}_\omega^v \bar{\varphi}_\omega)(t) = \\ &= \sum_{t \in \Omega} f(t) \varphi_v(t) \bar{\varphi}_\omega(t) = \sum_{t \in \Omega} (f(t) \varphi_v(t)) \bar{\varphi}_\omega(t). \end{aligned} \quad (15)$$

We will need in the following modulation operators:

$$\begin{aligned} (M_t^\vee f)(t) &:= \varphi_\vee(t) f(t), & (\bar{M}_t^\vee f)(t) &:= \bar{\varphi}_\vee(t) f(t), \\ (M_\omega^\tau F)(\omega) &:= \varphi_\omega(\tau) F(\omega), & (\bar{M}_\omega^\tau F)(\omega) &:= \bar{\varphi}_\omega(\tau) F(\omega). \end{aligned}$$

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

$$\begin{aligned} f(t \leftarrow \tau) &\xrightarrow{\mathbb{F}} F(\omega) \varphi_\omega(\tau), & f(t' \leftarrow \tau) &\xrightarrow{\mathbb{F}} F(\omega) \bar{\varphi}_\omega(\tau), \\ (T_t^\tau f)(t) &\xrightarrow{\mathbb{F}} (M_\omega^\tau F)(\omega), & (\bar{T}_t^\tau f)(t) &\xrightarrow{\mathbb{F}} (\bar{M}_\omega^\tau F)(\omega) \end{aligned}$$

and

$$\begin{aligned} F(\omega \oplus \vee) &\xrightarrow{\mathbb{F}} f(t) \bar{\varphi}_\vee(t), & F(\omega \$ \vee) &\xrightarrow{\mathbb{F}} f(t) \varphi_\vee(t) \\ (D_\omega^\vee F)(\omega) &\xrightarrow{\mathbb{F}} (M_t^\vee f)(t), & (\bar{D}_\omega^\vee F)(\omega) &\xrightarrow{\mathbb{F}} (\bar{M}_t^\vee f)(t). \end{aligned}$$

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*

$$y(t) := (h \diamond x)(t) = \sum_{\tau \in \Omega} h(\tau) x(t' \leftarrow \tau), \quad Y(\omega) := (H \heartsuit F)(\omega) = \sum_{\vee \in \Omega} H(\vee) F(\omega \$ \vee)$$

and

$$c(\tau) := (f \clubsuit g)(\tau) = \sum_{t \in \Omega} f(t) \bar{g}(t' \leftarrow \tau), \quad C(\vee) := (F \spadesuit G)(\vee) = \sum_{\omega \in \Omega} F(\omega) \bar{G}(\omega \$ \vee)$$

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

The spaces $L(\Omega, \text{Alg}(\mathbb{F}))$ and $L(\Omega^*, \text{Alg}(\mathbb{F}))$ equipped multiplications \diamond and \heartsuit form commutative signal and spectral convolution algebras $\langle L(\Omega, \text{Alg}(\mathbb{F})), \diamond \rangle$ and $\langle L(\Omega^*, \text{Alg}(\mathbb{F})), \heartsuit \rangle$, respectively.

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

$$y_1(t) = (h_1 \diamond x_1)(t) = \sum_{\tau \in \Omega} h_1(\tau) x_1(t' \leftarrow \tau) \quad \text{and} \quad Y_2(\omega) = (H_2 \heartsuit X_2)(\omega) = \sum_{\vee \in \Omega} H_2(\vee) F_2(\omega \$ \vee)$$

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

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

i.e.,

$$y_1(t) = (h_1 \diamond x_1)(t) \xrightarrow{\mathbb{F}} Y_1(\omega) = H_1(\omega) \cdot X_1(\omega), \quad y_2(t) = h_2(t) x_2(t) \xrightarrow{\mathbb{F}} Y_2(\omega) = (H_2 \heartsuit X_2)(\omega).$$

Theorem 2. *Let us take four triplets $c_1(t), f_1(t), g_1(t) \in L(\Omega, \text{Alg}(\mathbb{F}))$, $c_2(t), f_2(t), g_2(t) \in L(\Omega, \text{Alg}(\mathbb{F}))$ and $C_1(\omega), F_1(\omega), G_1(\omega) \in L(\Omega^*, \text{Alg}(\mathbb{F}))$, $C_2(\omega), F_2(\omega), G_2(\omega) \in L(\Omega^*, \text{Alg}(\mathbb{F}))$. Let*

$$c_1(\tau) = (f_1 \clubsuit g_1)(\tau) = \sum_{t \in \Omega} f_1(t) \bar{g}_1(t' \leftarrow \tau), \quad \text{and} \quad C_2(\omega) = (F_2 \spadesuit G_2)(\omega) = \sum_{\vee \in \Omega} F_2(\omega) \bar{G}_2(\omega \$ \vee),$$

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

$$\mathbb{F} \{c_1\} = \mathbb{F} \{f_1 \clubsuit g_1\} = \mathbb{F} \{f_1\} \cdot \mathbb{F} \{g_1\}, \quad \mathbb{F}^{-1} \{C_2\} := \mathbb{F}^{-1} \{F_2 \spadesuit G_2\} = \mathbb{F}^{-1} \{F_2\} \cdot \mathbb{F}^{-1} \{G_2\},$$

i.e.,

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

2.3. Codes invariant with respect to GSOs

We are going to consider block codes of length N as subsets $\mathbf{C} \subset L(\Omega, Alg(\mathbf{F}))$ and $\mathbf{C}^* \subset L(\Omega^*, Alg(\mathbf{F}))$, 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 $L(\Omega, Alg(\mathbf{F}))$ and $L(\Omega^*, Alg(\mathbf{F}))$, respectively. They generate two hypergroups \mathbf{HG} - and \mathbf{HG}^* .

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

$$(T_i^\tau c)(t) = c(t' \ \tau) \in \mathbf{C}, \quad \forall T_i^\tau \in \mathbf{HG} \text{ and } (D_\omega^\vee C)(\omega) = C(\omega \$ \vee) \in \mathbf{C}, \quad \forall D_\omega^\vee \in \mathbf{HG}^*, \text{ respectively.}$$

It means that \mathbf{HG} - and \mathbf{HG}^* - invariant block codes $\mathbf{C} \subset L(\Omega, Alg(\mathbf{F}))$ and $\mathbf{C}^* \subset L(\Omega^*, Alg(\mathbf{F}))$ have hypergroup symmetries $\text{Symm}\{\mathbf{C}\} \approx \mathbf{HG}$ and $\text{Symm}\{\mathbf{C}^*\} \approx \mathbf{HG}^*$.

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

$$\mathbf{m} = (m_0, m_1, \dots, m_{k-1}) \mapsto \mathbf{c}(t) = (c(0), c(1), \dots, c(N-1)), \quad Alg^k(\mathbf{F}) \rightarrow L(\Omega, Alg(\mathbf{F})) \quad (16)$$

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

$$\mathbf{m} = (m_0, m_1, \dots, m_{k-1}) \mapsto C(t) = (C(0), C(1), \dots, C(N-1)), \quad Alg^k(\mathbf{F}) \rightarrow L(\Omega^*, Alg(\mathbf{F}))$$

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

$$\mathbf{HG}\text{-RS}: Alg^k(\mathbf{F}) \rightarrow L(\Omega, Alg(\mathbf{F})), \quad \mathbf{HG}^*\text{-RS}: Alg^k(\mathbf{F}) \rightarrow L(\Omega^*, Alg(\mathbf{F}))$$

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

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

Hence, generator matrices for \mathbf{HG} - and \mathbf{HG}^* - invariant Reed-Solomon codes are the generalized Fourier matrices \mathbf{F} and \mathbf{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 these seminal papers of Forney [24] and Massey et al. [25].

Definition 8. \mathbf{HG} - and \mathbf{HG}^* - invariant convolutional codes of length N and dimension k are ideals $\langle \varphi h(t) \rangle$, $\langle G(\omega) \rangle$ of $\langle L(\Omega, Alg(\mathbf{F})), \diamond \rangle$ and $\langle L(\Omega^*, Alg(\mathbf{F})), \heartsuit \rangle$ having the following forms

$$c(t) = (h \diamond m)(t) = \sum_{\tau \in \Omega} h(t' \ \tau) m(\tau) \text{ and } C(\omega) = (G \heartsuit m)(\omega) = \sum_{\vee \in \Omega^*} G(\omega \$ \vee) m(\vee)$$

where

$$H(\omega) = (\mathbf{F}h)(\omega) = (H(0), H(1), \dots, H(k-1), 0, \dots, 0) \in \text{Alg}^k(\mathbf{F}),$$

$$g(\omega) = (\mathbf{F}^{-1}G)(t) = (g(0), g(1), \dots, g(k-1), 0, \dots, 0) \in \text{Alg}^k(\mathbf{F}).$$

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

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

3. Examples

Let \mathbf{H}_N be a finite Abelian group of order $N = N_1 N_2 \dots N_n$. The fundamental structure theorem for finite Abelian group implies that we may write \mathbf{H}_N as the direct sum of cyclic groups, $\mathbf{H}_N = \mathbf{Z}_{N_1} \times \mathbf{Z}_{N_2} \times \dots \times \mathbf{Z}_{N_n}$, where \mathbf{Z}_{N_i} identified with the ring of integers \mathbf{Z}_{N_i} under with respect to modulo N_i and an element $t \in \mathbf{H}_N$ is identified with a point $t = (t_1, t_2, \dots, t_n)$ of n D discrete torus. The addition of two elements $t, \tau \in \mathbf{H}_N$ is defined as $\sigma = t \oplus \tau = (\sigma_1, \sigma_2, \dots, \sigma_n) = (t_1 \oplus_{\mathbf{Z}_{N_1}} \tau_1, t_2 \oplus_{\mathbf{Z}_{N_2}} \tau_2, \dots, t_n \oplus_{\mathbf{Z}_{N_n}} \tau_n)$.

The Fourier transforms in the space of all functions, defined on the finite Abelian group $\mathbf{H}_N = \bigoplus_{i=1}^n \mathbf{Z}_{N_i}$, and with their values in the finite commutative ring (field) or some finite algebra \mathbf{A} has a great interest for digital signal processing. Denote this space as $L(\mathbf{H}_N, \text{Alg}(\mathbf{F}))$. Let ε_{N_i} a primitive N_i -th root in the algebra $\text{Alg}(\mathbf{F})$. Let us construct the following functions $\chi_{k_i}(t_i) = \varepsilon_{N_i}^{k_i t_i}$, $k_i = 0, 1, \dots, N_i - 1$. They form the set of characters of the cyclic group \mathbf{Z}_{N_i} . Then the set of all characters of the group \mathbf{H}_N can be describe by the following way

$$\chi_k(t) = \chi_{(k_1, k_2, \dots, k_n)}(t_1, t_2, \dots, t_n) = \varepsilon_{N_1}^{k_1 t_1} \varepsilon_{N_2}^{k_2 t_2} \dots \varepsilon_{N_n}^{k_n t_n}, \quad (16)$$

where $k = (k_1, k_2, \dots, k_n)$. The set of all characters $\{\chi_k(t)\}_{k \in \mathbf{H}_N^*}$ and the set of all indexes \mathbf{H}_N^* forms isomorphic multiplicative and additive groups, respectively, with respect to multiplication of characters and addition of indexes $\chi_k(t) \chi_m(t) = \chi_{k \oplus_{\mathbf{H}_N} m}(t) = \chi_l(t)$, where

$$l = k \oplus_{\mathbf{H}_N} m = (l_1, l_2, \dots, l_n) = (k_1 \oplus_{\mathbf{Z}_{N_1}} m_1, k_2 \oplus_{\mathbf{Z}_{N_2}} m_2, \dots, k_n \oplus_{\mathbf{Z}_{N_n}} m_n).$$

The following matrix $\mathbf{F} = [\chi_k(t)]_{t \in \mathbf{H}_N, k \in \mathbf{H}_N^*}$ forms Fourier transform on \mathbf{H}_N .

The set \mathbf{H}_N^* is called the dual group. It forms "frequency" domain. If initial group has the structure $\mathbf{H}_N = \mathbf{Z}_{N_1} \oplus \mathbf{Z}_{N_2} \oplus \dots \oplus \mathbf{Z}_{N_n}$ then the dual group has the same structure $\mathbf{H}_N^* = \mathbf{H}_N$. Let us embed finite groups \mathbf{H}_N and \mathbf{H}_N^* into two discrete segments $\Omega = [0, N-1]$ and $\Omega^* = [0, N-1]$

$$\mathbf{H}_N \rightarrow \Omega = [0, N-1], \quad \mathbf{H}_N^* \rightarrow \Omega^* = [0, N-1], \quad (17)$$

respectively. For this aim we briefly describe a mixed-radix number system now.

A number system is called a weighted number system if any number t can be uniquely expressed in the following form $t = \sum_i t_i w_i$ for some set of integers t_i , called digits, and w_i 's, called weights. If the weights are successive powers of the same number (for example, 2 or 10), the number system is called a *fixed-radix number system* (for example, *10-radix* or *2-radix*). Any number t in mixed-radix number system can be expressed in the form $t = \sum_{i=1}^n t_i \left(\prod_{j=i+1}^{n+1} N_j \right)$. Let $N_1, N_2, \dots, N_n, N_{n+1}$, where $N_{n+1} \equiv 1$ be a finite set of positive integers. Then, with respect to the mixed radixes above, any nonnegative integer $t \in [0, N-1]$, where $N = N_1 N_2 \dots N_n$, can be uniquely expressed as

$$t = (t_1, t_2, \dots, t_n) = t_1(N_2 N_3 \cdots N_{n-1} N_n) + \dots + t_{n-2}(N_{n-1} N_n) + t_{n-1}(N_n) + t_n = \sum_{i=0}^{n-1} t_{n-i} \left(\prod_{j=n+1}^{n-i+1} N_j \right),$$

where $t_1 \in [0, N_1 - 1]$, $t_2 \in [0, N_1 - 1]$, ..., $t_{n-1} \in [0, N_{n-1} - 1]$, $t_n \in [0, N_n - 1]$. The weights of t_i is $\prod_{j=n+1}^{n-i+1} N_j$.

The weight of t_n is unity ($N_{n+1} = 1$). The radix-2 representation is $t = t_{n-1} 2^{n-1} + t_{n-2} 2^{n-2} + \dots + t_1 2^1 + t_0 2^0 =$
 $= \sum_{i=0}^{n-1} t_{n-i} 2^i$. Let $t = (t_1, t_2, \dots, t_n) \in \mathbf{H}_N$ and $(\omega_1, \omega_2, \dots, \omega_n) \in \mathbf{H}_N^*$ then expressions $\omega = \sum_{i=0}^{n-1} \omega_{n-i} \left(\prod_{j=n+1}^{n-i+1} N_j \right)$,

$$k = \sum_{i=0}^{n-1} k_{n-i} \left(\prod_{j=n+1}^{n-i+1} N_j \right) \text{ define the maps (17).}$$

The following operators (with respect to which all characters are invariant eigenfunctions)

$$\begin{aligned} (T_t^\tau \chi_\omega)(t) &:= \chi_\omega(\tau) \cdot \chi_\omega(t) = \chi_\omega(t \oplus_{\mathbf{H}_N} \tau), \quad \forall \tau \in \Omega, \\ (\bar{T}_t^\tau \chi_\omega)(t) &:= \bar{\chi}_\omega(\tau) \cdot \chi_\omega(t) = \chi_\omega(t \otimes_{\mathbf{H}_N} \tau), \quad \forall \tau \in \Omega \end{aligned} \quad (18)$$

and

$$\begin{aligned} (D_\omega^v \bar{\chi}_\omega)(t) &:= \bar{\chi}_v(t) \cdot \bar{\chi}_\omega(t) = \bar{\chi}_{\omega \oplus_{\mathbf{H}_N} v}(t), \quad \forall v \in \Omega^*, \\ (\bar{D}_\omega^v \chi_\omega)(t) &:= \chi_v(t) \cdot \chi_\omega(t) = \bar{\chi}_{\omega \otimes_{\mathbf{H}_N} v}(t), \quad \forall v \in \Omega^* \end{aligned} \quad (19)$$

are called commutative $\mathbf{F}_{\mathbf{H}_N}$ -generalized "time"-shift and "frequency"-shift operators, induced an abelian group \mathbf{H}_N . It induces "exotic" shifts in segments $\mathbf{H}_N \rightarrow \Omega = [0, N - 1]$, $\mathbf{H}_N^* \rightarrow \Omega^* = [0, N - 1]$ too, which we will denote as

$$\begin{aligned} t \oplus_{\mathbf{H}_N} \tau &= (t_1 \oplus_{N_1} \tau_1, t_2 \oplus_{N_2} \tau_2, \dots, t_n \oplus_{N_n} \tau_n) \in \Omega = [0, N - 1], \\ k \oplus_{\mathbf{H}_N} m &= (k_1 \oplus_{N_1} m_1, k_2 \oplus_{N_2} m_2, \dots, k_n \oplus_{N_n} m_n) \in \Omega^* = [0, N - 1]. \end{aligned}$$

Instead of spaces $L(\mathbf{H}_N, \text{Alg}(\mathbf{F}))$ and $L(\mathbf{H}_N^*, \text{Alg}(\mathbf{F}))$ we will speak about spaces $L(\Omega, \text{Alg}(\mathbf{F}))$ and $L(\Omega^*, \text{Alg}(\mathbf{F}))$ and if necessary, in this designations we will distinguish groups, acting in intervals: $L(\Omega, \text{Alg}(\mathbf{F}) | \mathbf{H}_N)$ and $L(\Omega^*, \text{Alg}(\mathbf{F}) | \mathbf{H}_N^*)$.

Definition 9. \mathbf{H}_N - and \mathbf{H}_N^* - invariant block codes $\mathbf{C} \subset L(\Omega, \text{Alg}(\mathbf{F}) | \mathbf{H}_N)$ and $\mathbf{C}^* \subset L(\Omega^*, \text{Alg}(\mathbf{F}) | \mathbf{H}_N^*)$ are linear block codes with the property that if $c(t) \in \mathbf{C}$ and $C(\omega) \in \mathbf{C}^*$ then

$$(T_t^\tau c)(t) = c(t \oplus_{\mathbf{H}_N} \tau) \in \mathbf{C}, \quad \forall \tau \in \Omega \text{ and } (D_\omega^v C)(\omega) = C(\omega \oplus_{\mathbf{H}_N} v) \in \mathbf{C}, \quad \forall v \in \Omega^*,$$

respectively

It means that \mathbf{H}_N - and \mathbf{H}_N^* - invariant block codes have ordinary group symmetries $\text{HypSym}\{\mathbf{C}\} \square \mathbf{H}_N$ and $\text{HypSym}\{\mathbf{C}^*\} \square \mathbf{H}_N^*$. The subclass of codes are called the *abelian group codes* [13, 14-16]. Special cases of abelian group codes are 1) a cyclic code, when $\mathbf{H}_N = \mathbf{Z}_{N_1} \times \mathbf{Z}_{N_2} \times \dots \times \mathbf{Z}_{N_n} \equiv \mathbf{Z}_N$ is a cyclic group, 2) a dyadic code, when $\mathbf{H}_{2^n} = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \dots \times \mathbf{Z}_2$. In the first case $\mathbf{F} = \left[\varepsilon_N^{t\omega} \right]_{t \in \mathbf{Z}_N, \omega \in \mathbf{Z}_N^*}$ is the ordinary Fourier transform, where ε_N a primitive N -th root in the algebra $\text{Alg}(\mathbf{F})$ and in the second one $\mathbf{F} = \left[(-1)^{\langle t | \omega \rangle} \right]_{t \in \mathbf{H}_{2^n}, \omega \in \mathbf{H}_{2^n}^*}$ is the Walsh transform, where $\langle t | \omega \rangle$ is

the scalar products of two vectors $t = (t_1, t_2, \dots, t_n) \in \mathbf{H}_N$ and $(\omega_1, \omega_2, \dots, \omega_n) \in \mathbf{H}_N^* : \langle t | \omega \rangle = \sum_{i=1}^n t_i \omega_i$.

Let $\mathbf{F} = \left[\varepsilon_{2N}^t \varepsilon_N^{t\omega} \right]_{t,\omega=0}^{N-1} = \left[\varepsilon_{2N}^{t(2\omega+1)} \right]_{t,\omega=0}^{N-1}$. Then

$$F(\omega) = (\mathbf{F}f)(\omega) = \sum_{t \in \Omega} f(t) \varepsilon_{2N}^{-t} \varepsilon_N^{-t\omega}, \quad f(t) = (\mathbf{F}^{-1}F)(t) = \sum_{\omega \in \Omega^*} F(\omega) \varepsilon_{2N}^t \varepsilon_N^{t\omega}$$

is direct and inverse modulation Fourier transform, where ε_{2N} is a primitive $2N$ -th root in the algebra $\text{Alg}(\mathbf{F})$. According to definition 4 for $\varphi_\omega(t) = \varepsilon_{2N}^t \varepsilon_N^{t\omega}$ we have

$$\begin{aligned} \hat{T}_t^\tau \{ \varphi_\omega(t) \} &= \varphi_\omega(t(\tau)) = \varphi_\omega(\tau) \cdot \varphi_\omega(t) = \varepsilon_{2N}^{(2\omega+1)\tau} \varepsilon_{2N}^{(2\omega+1)t} = \varepsilon_{2N}^{(2\omega+1)(t+\tau)}, \\ \overline{\hat{T}}_n^\tau \{ \varphi_\omega(t) \} &= \varphi_\omega(t'(\tau)) = \overline{\varphi}_\omega(\tau) \cdot \varphi_\omega(t) = \varepsilon_{2N}^{-(2\omega+1)\tau} \varepsilon_{2N}^{(2\omega+1)t} = \varepsilon_{2N}^{(2\omega+1)(t-\tau)}. \end{aligned}$$

But $\varepsilon_{2N}^{(2\omega+1)(t+N)} = \varepsilon_{2N}^{(2\omega+1)N} \varepsilon_{2N}^{(2\omega+1)t} = \varepsilon_{2N}^{(2\omega+1)} \varepsilon_{2N}^{(2\omega+1)t} = (-1)^{(2\omega+1)} \varepsilon_{2N}^{(2\omega+1)t} = -\varepsilon_{2N}^{(2\omega+1)t}$. Hence, \hat{T}_t^τ and $\overline{\hat{T}}_n^\tau$ are negacyclic (skew-cyclic) GSOs:

$$\hat{T}_t^\tau \{ c(t) \} = (c_{0(\tau)}, c_{1(\tau)}, \dots, c_{(N-1)(\tau)}) = (c_\tau, c_{\tau+1}, \dots, c_{N-2}, c_{N-1}, \underbrace{-c_0, -c_1, \dots, -c_{\tau-1}}_\tau),$$

$$\overline{\hat{T}}_n^\tau \{ c(t) \} = (c_{0'(\tau)}, c_{1'(\tau)}, \dots, c_{(N-1)'(\tau)}) = (\underbrace{-c_{N-\tau}, \dots, -c_{N-2}, -c_{N-1}}_\tau, c_0, c_1, \dots, c_{N-(\tau-1)}).$$

They generate negacyclic (skew-cyclic) codes. Let $\mathbf{F} = \left[\varepsilon_{mN}^t \varepsilon_N^{t\omega} \right]_{t,\omega=0}^{N-1} = \left[\varepsilon_{mN}^{(m\omega+1)t} \right]_{t,\omega=0}^{N-1}$. Then

$$F(\omega) = (\mathbf{F}f)(\omega) = \sum_{t \in \Omega} f(t) \varepsilon_{mN}^{-t} \varepsilon_N^{-t\omega}, \quad f(t) = (\mathbf{F}^{-1}F)(t) = \sum_{\omega \in \Omega^*} F(\omega) \varepsilon_{mN}^t \varepsilon_N^{t\omega}$$

is direct and inverse ε_{mN}^{-t} -modulation Fourier transform, where ε_{mN} is a primitive mN -th root in the algebra $\text{Alg}(\mathbf{F})$. According to definition 4 for $\varphi_\omega(t) = \varepsilon_{mN}^t \varepsilon_N^{t\omega}$ we have

$$\begin{aligned} \hat{T}_t^\tau \{ \varphi_\omega(t) \} &= \varphi_\omega(t(\tau)) = \varphi_\omega(\tau) \cdot \varphi_\omega(t) = \varepsilon_{mN}^{(m\omega+1)\tau} \varepsilon_{mN}^{(2m+1)t} = \varepsilon_{mN}^{(m\omega+1)(t+\tau)}, \\ \overline{\hat{T}}_n^\tau \{ \varphi_\omega(t) \} &= \varphi_\omega(t'(\tau)) = \overline{\varphi}_\omega(\tau) \cdot \varphi_\omega(t) = \varepsilon_{mN}^{-(m\omega+1)\tau} \varepsilon_{mN}^{(m\omega+1)t} = \varepsilon_{mN}^{(m\omega+1)(t-\tau)}. \end{aligned}$$

But $\varepsilon_{mN}^{(m\omega+1)(t+N)} = \varepsilon_{mN}^{(m\omega+1)N} \varepsilon_{mN}^{(m\omega+1)t} = \varepsilon_{mN}^{(m\omega+1)} \varepsilon_{2N}^{(2\omega+1)t} = \varepsilon_m \varepsilon_{mN}^{(m\omega+1)t}$. Hence, \hat{T}_t^τ and $\overline{\hat{T}}_n^\tau$ are constacyclic GSOs:

$$\hat{T}_t^\tau \{ c(t) \} = (c_{0(\tau)}, c_{1(\tau)}, \dots, c_{(N-1)(\tau)}) = (c_\tau, c_{\tau+1}, \dots, c_{N-2}, c_{N-1}, \underbrace{\varepsilon_m c_0, \varepsilon_m c_1, \dots, \varepsilon_m c_{\tau-1}}_\tau),$$

$$\overline{\hat{T}}_n^\tau \{ c(t) \} = (c_{0'(\tau)}, c_{1'(\tau)}, \dots, c_{(N-1)'(\tau)}) = (\underbrace{\varepsilon_m c_{N-\tau}, \dots, \varepsilon_m c_{N-2}, \varepsilon_m c_{N-1}}_\tau, c_0, c_1, \dots, c_{N-(\tau-1)}).$$

They generate constacyclic codes codes.

4. 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 Fourier transforms.

5. References

- [1] Berlekamp E R 1969 Negacyclic codes for the Lee metric *Combinatorial Mathematics and its Applications* 298-316
- [2] Berlekamp E R 1984 *Algebraic coding theory* (New York: Aegean Park Press)
- [3] Sergio R L P and Benigno R 2009 Dual generalizations of the concept of cyclicity of codes *Adv. Math. Commun.* **3(3)** 227-234

- [4] Boucher D, Geiselmann W and Ulmer F 2007 Skew-cyclic codes *Appl. Algebra Eng. Comm. Comput.* **184** 379-389
- [5] Delphine B, Patrick S and Felix U 2008 Skew constacyclic codes over Galois rings *Adv. Math. Commun.* **23** 273-292
- [6] Delphine B and Felix U 2008 Coding with skew polynomial rings *Adv. Math. Commun.* **33** 254-276
- [7] Hai Q D 2005 Negacyclic codes of length $2s$ over Galois rings *IEEE Trans. Inform. Theory IT* **51(12)** 4252-4262
- [8] Hai Q D 2008 On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions *Finite Fields Appl.* **14** 1 22-40
- [9] Hai Q D, Sergio R L and Szabo S On the structure of cyclic and negacyclic codes over finite chain rings *Codes over rings* **6**
- [10] Hai Q D and Sergio R L 2004 Cyclic and negacyclic codes over finite chain rings *IEEE Trans. Inform. Theory* **50(8)** 1728-1744
- [11] Hakan O and Ferruh O 2009 A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p *Adv. Math. Commun.* **3(3)** 265-271
- [12] Hai Q 2006 Structure of some classes of repeated-root constacyclic codes over integers modulo $2m$ *Groups, rings and group rings Lect. Notes Pure Appl. Math.* **248** 105-117
- [13] Sundar R B and Siddigi M U 1994 Transform Domain Characterization of Abelian codes *IEEE Trans. Inform. Theory* **40** 2082-2090
- [14] Berman S D 1967 Semi-simple cyclic and abelian codes *Kibernetika* **3** 20-30
- [15] Camion P 1970 Abelian codes *Tech. Rep.* 1059
- [16] MacWilliams F J 1970 Binary codes which are ideals in the group algebra of an abelian group *BSTJ* **49** 987-1011
- [17] Marty F 1934 Sur une generalization de la notion de groupe *Sartryckur Forhandlingar Via Altonde Skandinavioka Matematiker kongresseni* 45-49
- [18] Marty F 1937 Role de la notion d'hypergroupes dans l'etude des groupes non abeliens *Comptes Rendus de l'Academie des Sciences* **201** 636-638
- [19] Wall H S 1934 Hypergroups *Bulletin of the American Mathematical Society* **41** 36-40
- [20] Wall H S 1937 Hypergroups *American Journal of Mathematics* **59** 77-98
- [21] Levitan B M 1949 The application of generalized displacement operators to linear differential equations of second order *Uspechi Math. Nauk* **4(1)** 3-112
- [22] Levitan B M 1964 Generalized translation operators *Israel Program for Scientific Translations*
- [23] Reed I S and Solomon G 1960 Polynomial Codes Over Certain Finite Fields *SIAM Journal of Applied Math* **3** 300-304
- [24] Forney G D 1970 Convolutional codes Part I: Algebraic structure *IEEE Trans. Inform. Theory. It* **16** 720-738
- [25] Massey J L and Sain M K 1967 Codes, automata, and continuous systems: Explicit Interconnections *IEEE Trans. Aut. Contr. AC* **12** 644-650

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".