Journal of
Linear and Topological Algebra
Vol. 04*, No.* 04*,* 2015, 241- 257

Classical wavelet transforms over finite fields

A. Ghaani Farashahi*

Numerical Harmonic Analysis Group (NuHAG), Faculty of Mathematics,
University of Vienna.

Received 17 October 2015; Revised 23 January 2016; Accepted 31 January 2016.

Abstract. This article introduces a systematic study for computational aspects of classical wavelet transforms over finite fields using tools from computational harmonic analysis and also theoretical linear algebra. We present a concrete formulation for the Frobenius norm of the classical wavelet transforms over finite fields. It is shown that each vector defined over a finite field can be represented as a finite coherent sum of classical wavelet coefficients.

Keywords: Finite field, classical wavelet group, quasi-regular representation, classical wavelet transforms, dilation operators, periodic (finite size) data, prime integer.

2010 AMS Subject Classification: Primary 42C40, 12E20; Secondary 13B05, 12F10, 81R05, 20G40.

1. Introduction

The mathematical theory of finite fields has significant roles and applications in computer science, information theory, communication engineering, coding theory, cryptography, finite quantum systems and number theory [15, 24]. Discrete exponentiation can be computed quickly using techniques of fast exponentiation such as binary exponentiation within a finite field operations and also in coding theory, many codes are constructed as subspaces of vector spaces over finite fields, see [16, 17, 23] and references therein.

The finite dimensional data processing is the basis of information theory, and large scale data analysis. In data processing, time-scale analysis comprises those techniques that analyze a vector in both the time and scale domains simultaneously, called also wavelet methods, see [1, 2, 8, 9, 13, 22] and references therein. The wavelet theory is

*Corresponding author.
E-mail address: arash.ghaani.farashahi@univie.ac.at ; ghaanifarashahi@hotmail.com (A. Ghaani Farashahi).

Print ISSN: 2252-0201
Online ISSN: 2345-5934

http://jlta.iauctb.ac.ir

based on the affine group as the group of dilations and translation, see [1, 2, 22] and references therein. Wavelet analysis of periodic data rely on embedding the vector space of finite size data in the Hilbert space of all complex valued sequences with finite $\|.\|_2$-norm. Some different approaches to the wavelet analysis over finite fields studied in [5, 6, 12, 14].

In this article we present the notion of classical wavelet (affine) group $\mathrm{W}_{\mathbb{F}}$ associated to the finite field $\mathbb{F}$ as the group of dilation, translation and modulation and we present the abstract theory of classical wavelet transform over $\mathbb{F}$. If $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ is a window vector, we define the wavelet transform $W_{\mathbf{y}}$ as the voice transform defined on $\mathbb{C}^{\mathbb{F}}$ with complex values which are indexed in the classical wavelet group $\mathrm{W}_{\mathbb{F}}$. These techniques imply a unified group theoretical based time-scale (dilation and translation) representations for vectors in $\mathbb{C}^{\mathbb{F}}$. It is shown that the wavelet transform $W_{\mathbf{y}}$ as a windowed transform satisfies the isometric property and inversion formula as well, if the window vector satisfies an admissibility condition.

2. Preliminaries and Notations

For a finite group G, the finite dimensional complex vector space $\mathbb{C}^G = \{\mathbf{x} : G \to \mathbb{C}\}$ is a $|G|$-dimensional Hilbert space with complex vector entries indexed by elements in the finite group G. [1] The inner product of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{C}^G$ is $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{g \in G} \mathbf{x}(g)\overline{\mathbf{y}(g)}$, and the induced norm is the $\|.\|_2$-norm of $\mathbf{x}$, that is $\|\mathbf{x}\|_2 = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$. For $\mathbb{C}^{\mathbb{Z}_N}$, where $\mathbb{Z}_N$ denotes the cyclic group of N elements $\{0, \ldots, N-1\}$, we simply write $\mathbb{C}^N$ at times.

Time-scale analysis and time-frequency analysis on finite Abelian group G as modern computational harmonic analysis tools are based on three basic operations on $\mathbb{C}^G$. The translation operator $T_k : \mathbb{C}^G \to \mathbb{C}^G$ given by $T_k\mathbf{x}(g) = \mathbf{x}(g-k)$ with $g, k \in G$. The modulation operator $M_\ell : \mathbb{C}^G \to \mathbb{C}^G$ given by $M_\ell \mathbf{x}(g) = \overline{\ell(g)}\mathbf{x}(g)$ with $g \in G$ and $\ell \in \widehat{G}$, where $\widehat{G}$ is the character/dual group of G. As the fundamental theorem of finite Abelian groups provides a factorization of G into cyclic groups, that is, $G \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \ldots \times \mathbb{Z}_{N_d}$ as groups, which implies $\widehat{G} \cong G$, we can assume that the action of $\ell = (\ell_1, \ldots, \ell_d) \in \widehat{G}$ on $g = (g_1, ..., g_d) \in G$ is given by

$$\ell(g) = ((\ell_1, \ell_2, \ldots, \ell_d), (g_1, \ldots, g_d)) = \prod_{j=1}^{d} \mathbf{e}_{\ell_j}(g_j),$$

where $\mathbf{e}_{\ell_j}(g_j) = e^{2\pi i \ell_j g_j / N_j}$ for all $1 \leq j \leq d$. Thus

$$\ell(g) = ((\ell_1, \ell_2, \ldots, \ell_d), (g_1, \ldots, g_d)) = e^{2\pi i(\ell_1 g_1/N_1 + \ell_2 g_2/N_2 + \ldots + \ell_d g_d/N_d)}.$$

The character/dual group $\widehat{G}$ of any finite Abelian group G is isomorphic with G via the canonical group isomorphism $\ell \mapsto \mathbf{e}_\ell$, where the character $\mathbf{e}_\ell : G \to \mathbb{T}$ is given by $\mathbf{e}_\ell(g) = \ell(g)$ for all $g \in G$. The third fundamental operator is the discrete Fourier transform (DFT) $\mathcal{F}_G : \mathbb{C}^G \to \mathbb{C}^{\widehat{G}} = \mathbb{C}^G$ which allows us to pass from time representations

[1] $|G|$ denotes the order of the group G, or, more generally, the cardinality of a set G.

to frequency representations. It is defined as a function on $\widehat{G}$ by

$$\mathcal{F}_G(\mathbf{x})(\ell) = \widehat{\mathbf{x}}(\ell) = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mathbf{x}(g)\overline{\ell(g)} \tag{1}$$

for all $\ell \in \widehat{G}$ and $\mathbf{x} \in \mathbb{C}^G$. That is equivalently

$$\mathcal{F}_G(\mathbf{x})(\ell) = \widehat{\mathbf{x}}(\ell) = \frac{1}{\sqrt{|G|}} \sum_{g_1=0}^{N_1-1} \cdots \sum_{g_d=0}^{N_d-1} \mathbf{x}(g_1,\ldots,g_d)\overline{((\ell_1,\ldots,\ell_d),(g_1,\ldots,g_d))},$$

for all $\ell = (\ell_1,\ldots,\ell_d) \in \widehat{G}$ and $\mathbf{x} \in \mathbb{C}^G$. Translation, modulation, and the Fourier transform on the Hilbert space $\mathbb{C}^G = \mathbb{C}^{\widehat{G}}$ are unitary operators with respect to the $\|.\|_2$-norm. For $\ell, k \in G \cong \widehat{G}$ we have $(T_k)^* = (T_k)^{-1} = T_{-k}$ and $(M_\ell)^* = (M_\ell)^{-1} = M_{-\ell}$. The circular convolution of $\mathbf{x}, \mathbf{y} \in \mathbb{C}^G$ is defined by

$$\mathbf{x} * \mathbf{y}(k) = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mathbf{x}(g)\mathbf{y}(k-g), \quad \text{for } k \in G.$$

In terms of the translation operators we have $\mathbf{x} * \mathbf{y}(k) = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \mathbf{x}(g) T_g \mathbf{y}(k)$ for $k \in G$. The circular involution or circular adjoint of $\mathbf{x} \in \mathbb{C}^G$ is given by $\mathbf{x}^*(k) = \overline{\mathbf{x}(-k)}$. The complex linear space $\mathbb{C}^G$ equipped with the $\|.\|_1$-norm, that is $\|\mathbf{x}\|_1 = \sum_{g\in G} |\mathbf{x}(g)|$, the circular convolution, and involution is a Banach $*$-algebra, which means that for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^G$ we have

$$\|\mathbf{x} * \mathbf{y}\|_1 \le \frac{1}{\sqrt{|G|}} \|\mathbf{x}\|_1 \|\mathbf{y}\|_1, \text{ and } \|\mathbf{x}^*\|_1 = \|\mathbf{x}\|_1.$$

The unitary DFT (1) satisfies

$$\widehat{T_k \mathbf{x}} = M_k \widehat{\mathbf{x}}, \quad \widehat{M_\ell \mathbf{x}} = T_{-\ell} \widehat{\mathbf{x}}, \quad \widehat{\mathbf{x}^*} = \overline{\widehat{\mathbf{x}}}, \quad \widehat{\mathbf{x} * \mathbf{y}} = \widehat{\mathbf{x}}.\widehat{\mathbf{y}},$$

for $\mathbf{x}, \mathbf{y} \in \mathbb{C}^G$, $k \in G$ and $\ell \in \widehat{G}$. See standard references of harmonic analysis such as [19, 25] and references therein.

3. Harmonic Analysis over Finite Fields

Throughout this section, we present a summary of basic and classical results concerning harmonic analysis over finite fields. For proofs we refer readers to see [15, 18, 20, 24] and references therein.

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of order q. Then there is a prime number p and an integer number $d \ge 1$ in which $q = p^d$. Every finite field of order $q = p^d$ is isomorphic as a field to every other field of order q. From now on, when it is necessary we denote any finite field of order $q = p^d$ by $\mathbb{F}_q$ otherwise we just denote it by $\mathbb{F}$. The prime number p is called the characteristic of $\mathbb{F}$, which means that

$$p.\tau = \sum_{k=1}^{p} \tau = 0 \quad \text{for all } \tau \in \mathbb{F}.$$

The absolute trace map $\mathbf{t} : \mathbb{F} \to \mathbb{Z}_p$ is given by $\tau \mapsto \mathbf{t}(\tau)$ where

$$\mathbf{t}(\tau) = \sum_{k=0}^{d-1} \tau^{p^k} \quad \text{for all } \tau \in \mathbb{F}.$$

The absolute trace map $\mathbf{t}$ is a $\mathbb{Z}_p$-linear transform from $\mathbb{F}$ onto $\mathbb{Z}_p$. It should be mentioned that in the case of prime fields, the trace map is readily the identity map.

There exists an irreducible polynomial $P \in \mathbb{Z}_p[t]$ of degree d and a root $\theta \in \mathbb{F}$ of P such that the set

$$\mathcal{B}_\theta := \{\theta^j : j = 0, ..., d-1\} = \{1, \theta, \theta^2, ..., \theta^{d-2}, \theta^{d-1}\},$$

is a linear basis of $\mathbb{F}$ over $\mathbb{Z}_p$. Then $\mathcal{B}_\theta$ is called as a polynomial basis of $\mathbb{F}$ over $\mathbb{Z}_p$ and θ is called as a defining element of $\mathbb{F}$ over $\mathbb{Z}_p$. Let $\mathbf{H} = \mathbf{H}_\theta \in \mathbb{Z}_p^{d\times d}$ be the $d \times d$ matrix with entries in the field $\mathbb{Z}_p$ given by $\mathbf{H}_{jk} := \mathbf{t}(\theta^{j+k})$ for all $0 \le j, k \le d-1$, which is invertible with the inverse $\mathbf{S} \in \mathbb{Z}_p^{d\times d}$. Then the dual polynomial basis

$$\widetilde{\mathcal{B}_\theta} := \{\Theta_k : k = 0, ..., d-1\}, \tag{2}$$

given by

$$\Theta_k = \sum_{j=0}^{d-1} \mathbf{S}_{kj}\theta^j, \tag{3}$$

satisfies the following orthogonality relation

$$\mathbf{t}(\theta^k \Theta_j) = \delta_{k,j}, \tag{4}$$

for all $j, k = 0, ..., d-1$.

Proposition 3.1 *Let $\mathbb{F}$ be a finite field of order $q = p^d$ with trace map $\mathbf{t} : \mathbb{F} \to \mathbb{Z}_p$. Then*

(1) For $\tau \in \mathbb{F}$ we have the following decompositions

$$\tau = \sum_{k=0}^{d-1} \tau_{(k)}\theta^k = \sum_{k=0}^{d-1} \tau_{[k]}\Theta_k,$$

where for all $k = 0, ..., d-1$ we have

$$\tau_{(k)} := \mathbf{t}(\tau\Theta_k), \qquad \tau_{[k]} := \mathbf{t}(\tau\theta^k).$$

(2) For $\tau \in \mathbb{F}$ the coefficients (components) $\{\tau_{(k)} : k = 0, ..., d-1\}$ and $\{\tau_{[k]} : k = 0, ..., d-1\}$ satisfy

$$\tau_{(k)} = \sum_{j=0}^{d-1} \mathbf{S}_{kj}\tau_{[j]}, \qquad \tau_{[k]} = \sum_{j=0}^{d-1} \mathbf{H}_{kj}\tau_{(j)},$$

for all $k = 0, ..., d-1$.

Let $\theta \in \mathbb{F}$ be a defining element of $\mathbb{F}$ over $\mathbb{Z}_p$. Then θ defines a $\mathbb{Z}_p$-linear isomorphism $J_\theta : \mathbb{F} \to \mathbb{Z}_p^d$ by

$$\gamma \mapsto J_\theta(\tau) := \tau_\theta = (\tau_{(k)})_{k=1}^d, \quad \text{for all } \tau \in \mathbb{F}. \tag{5}$$

Then the additive group of the finite field $\mathbb{F}$, $\mathbb{F}^+$, is isomorphic with the finite elementary group $\mathbb{Z}_p^d$ via J_θ. Thus, using classical dual theory on the ring $\mathbb{Z}_p^d$ we get

$$\mathbf{e}_{\tau_\theta}(\tau'_\theta) = \mathbf{e}_{1,p}\left(\tau_\theta.\tau'_\theta\right) = \mathbf{e}_{1,p}\left(\sum_{k=1}^{d} \tau_{(k)}\tau'_{(k)}\right), \quad \text{for all } \tau, \tau' \in \mathbb{F}.$$

Remark 1 *The dual (character) group of the finite elementary group $\mathbb{Z}_p^d$, that is $\widehat{\mathbb{Z}_p^d}$, is precisely*

$$\left\{\mathbf{e}_\ell : \ell = (\ell_1, ..., \ell_d) \in \mathbb{Z}_p^d\right\},$$

where the additive character $\mathbf{e}_\ell : \mathbb{Z}_p^d \to \mathbb{T}$ is given by

$$\mathbf{e}_\ell(g) = \mathbf{e}_{1,p}(\ell \cdot g) = \exp\left(\frac{2\pi i \ \ell \cdot g}{p}\right) = \prod_{k=1}^{d} \mathbf{e}_{\ell_k,p}(g_k) \quad \text{for all } g = (g_1, ..., g_d) \in \mathbb{Z}_p^d,$$

with $\ell \cdot g = \sum_{k=1}^d \ell_k g_k$.

Let $\chi : \mathbb{F} \to \mathbb{T}$ be given by

$$\chi(\tau) := \exp\left(\frac{2\pi i \mathbf{t}(\tau)}{p}\right) = \mathbf{e}_{1,p}(\mathbf{t}(\tau)), \quad \text{for all } \tau \in \mathbb{F}.$$

Since the trace map is $\mathbb{Z}_p$-linear, we deduce that χ is a character on the additive group of $\mathbb{F}$ (i.e $\chi \in \widehat{\mathbb{F}^+}$).

Proposition 3.2 *Let $\mathbb{F}$ be a finite field of order $q = p^d$ with trace map $\mathbf{t} : \mathbb{F} \to \mathbb{Z}_p$. Then*

(1) For $\tau, \tau' \in \mathbb{F}$ we have

$$\mathbf{t}(\tau\tau') = \sum_{j=0}^{d-1}\sum_{k=0}^{d-1} \mathbf{H}_{jk}\tau_{(j)}\tau'_{(k)} = \sum_{j=0}^{d-1}\sum_{k=0}^{d-1} \mathbf{S}_{jk}\tau_{[j]}\tau'_{[k]} = \sum_{k=0}^{d-1} \tau_{(k)}\tau'_{[k]} = \sum_{k=0}^{d-1} \tau_{[k]}\tau'_{(k)}.$$

(2) For $\tau, \tau' \in \mathbb{F}$ we have

$$\chi(\tau\tau') = \mathbf{e}_{1,p}\left(\sum_{k=1}^{d} \tau_{(k)}\tau'_{[k]}\right) = \mathbf{e}_{1,p}\left(\sum_{k=1}^{d} \tau_{[k]}\tau'_{(k)}\right).$$

For $\gamma \in \mathbb{F}$, let $\chi_\gamma : \mathbb{F} \to \mathbb{T}$ be given by

$$\chi_\gamma(\tau) := \chi(\gamma\tau) = \exp\left(\frac{2\pi i \mathbf{t}(\gamma\tau)}{p}\right) = \mathbf{e}_{1,p}(\mathbf{t}(\gamma\tau)), \quad \text{for all } \tau \in \mathbb{F}.$$

Then χ_γ is a character on the additive group of $\mathbb{F}$ (i.e $\chi_\gamma \in \widehat{\mathbb{F}^+}$). For $\gamma = 1$ we get $\chi = \chi_1$.

If $\alpha \in \mathbb{F}^*$ the character χ_α is called as a non-principal character. The interesting property of non-principal characters is that any non-principal character can parametrize the full character group of the additive group of $\mathbb{F}$. In details, if $\alpha \in \mathbb{F}^*$, then we have

$$\widehat{\mathbb{F}^+} = \{\chi_{\alpha\gamma} \ : \ \gamma \in \mathbb{F}\}.$$

Thus, the mapping $\gamma \mapsto \chi_{\alpha\gamma}$ is group isomorphism of $\mathbb{F}$ onto $\widehat{\mathbb{F}^+}$. Then for $\alpha = 1$ we get

$$\widehat{\mathbb{F}^+} = \{\chi_\gamma \ : \ \gamma \in \mathbb{F}\}. \tag{6}$$

Then the Fourier transform of a vector $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$ at $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$ is

$$\widehat{\mathbf{x}}(\chi_\gamma) = \frac{1}{\sqrt{p^d}} \sum_{\tau\in\mathbb{F}} \mathbf{x}(\tau)\overline{\chi_\gamma(\tau)} = \frac{1}{\sqrt{p^d}} \sum_{\tau\in\mathbb{F}} \mathbf{x}(\tau)\overline{\mathbf{F}(\gamma,\tau)},$$

where the matrix $\mathbf{F} : \mathbb{F} \times \mathbb{F} \to \mathbb{C}$ is given by

$$\mathbf{F}(\gamma,\tau) := \chi(\gamma\tau) = \exp\left(\frac{2\pi i \mathbf{t}(\gamma\tau)}{p}\right), \quad \text{for all } \gamma,\tau \in \mathbb{F}.$$

Remark 2 *(i) For $\beta \in \mathbb{F}$, the translation operator $T_\beta : \mathbb{C}^{\mathbb{F}} \to \mathbb{C}^{\mathbb{F}}$ is*

$$T_\beta\mathbf{x}(\tau) := \mathbf{x}(\tau - \beta), \quad \text{for all } \tau \in \mathbb{F} \text{ and } \mathbf{x} \in \mathbb{C}^{\mathbb{F}}.$$

(ii) For $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$, the modulation operator $M_\gamma : \mathbb{C}^{\mathbb{F}} \to \mathbb{C}^{\mathbb{F}}$ is

$$M_\gamma\mathbf{x}(\tau) := \overline{\chi_\gamma(\tau)}\mathbf{x}(\tau), \quad \text{for all } \tau \in \mathbb{F} \text{ and } \mathbf{x} \in \mathbb{C}^{\mathbb{F}}.$$

4. Classical Wavelet Groups over Finite Fields

The abstract notion of wavelet groups over prime fields (finite Abelian groups of prime order) introduced in [7, 10–12] and extended for finite fields in [14].

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of order $q = p^d$. The finite multiplicative group

$$\mathbb{F}^* := \mathbb{F} - \{0\} = \{\alpha \in \mathbb{F} : \alpha \neq 0\}, \tag{7}$$

of nonzero elements of $\mathbb{F}$ is a finite cyclic group of order $q-1=p^d-1$. Any generator of the finite cyclic group $\mathbb{F}^*$ is called a primitive element or primitive root of $\mathbb{F}$ over $\mathbb{Z}_p$.

For $\alpha\in\mathbb{F}^*$, define the *dilation operator* $D_\alpha:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ by

$$D_\alpha\mathbf{x}(\tau):=\mathbf{x}(\alpha^{-1}\tau),$$

for all $\tau\in\mathbb{F}$ and $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$.

Hence we state basic algebraic properties of dilation operators.

Proposition 4.1 *Let $\mathbb{F}$ be a finite field. Then*

(1) For $(\alpha,\beta)\in\mathbb{F}^*\times\mathbb{F}$ we have $D_\alpha T_\beta=T_{\alpha\beta}D_\alpha$.
(2) For $\alpha,\alpha'\in\mathbb{F}^*$ we have $D_{\alpha\alpha'}=D_\alpha D_{\alpha'}$.
(3) For $(\alpha,\beta),(\alpha',\beta')\in\mathbb{F}^*\times\mathbb{F}$ we have $T_{\beta+\alpha\beta'}D_{\alpha\alpha'}=T_\beta D_\alpha T_{\beta'}D_{\alpha'}$.

Proof. Let $\mathbb{F}$ be a finite field and $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then (1) For $(\alpha,\beta)\in\mathbb{F}^*\times\mathbb{F}$ and $\tau\in\mathbb{F}$, we can write

$$\begin{aligned}D_\alpha T_\beta\mathbf{x}(\tau)&=T_\beta\mathbf{x}(\alpha^{-1}\tau)\\&=\mathbf{x}(\alpha^{-1}\tau-\beta)\\&=\mathbf{x}(\alpha^{-1}\tau-\alpha^{-1}\alpha\beta)\\&=\mathbf{x}(\alpha^{-1}(\tau-\alpha\beta))\\&=D_\alpha\mathbf{x}(\tau-\alpha\beta)=T_{\alpha\beta}D_\alpha\mathbf{x}(\tau).\end{aligned}$$

(2) For $\alpha,\alpha'\in\mathbb{F}^*$ and $\tau\in\mathbb{F}$, we can write

$$\begin{aligned}D_{\alpha\alpha'}\mathbf{x}(\tau)&=\mathbf{x}((\alpha\alpha')^{-1}\tau)\\&=\mathbf{x}(\alpha'^{-1}\alpha^{-1}\tau)\\&=D_{\alpha'}\mathbf{x}(\alpha^{-1}\tau)=D_\alpha D_{\alpha'}\mathbf{x}(\tau).\end{aligned}$$

(3) It is straightforward from (1) and (2). ■

Next proposition summarizes analytic properties of dilation operators.

Proposition 4.2 *Let $\mathbb{F}$ be a finite field and $\alpha\in\mathbb{F}^*$. Then*

(1) $D_\alpha:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ is a $*$-isometric isomorphism of the Banach $*$-algebra $\mathbb{C}^{\mathbb{F}}$
(2) $D_\alpha:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ is unitary in $\|.\|_2$-norm and satisfies $(D_\alpha)^*=(D_\alpha)^{-1}=D_{\alpha^{-1}}$.

Proof. (1) Let $\mathbf{x},\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ and $\tau\in\mathbb{F}$. Then we have

$$D_\alpha(\mathbf{x}*\mathbf{y})(\tau)=\mathbf{x}*\mathbf{y}(\alpha^{-1}\tau)=\frac{1}{\sqrt{q}}\sum_{\tau'\in\mathbb{F}}\mathbf{x}(\tau')\mathbf{y}(\alpha^{-1}\tau-\tau').$$

Replacing τ' with $\alpha^{-1}\tau'$ we get

$$\begin{aligned}\frac{1}{\sqrt{q}}\sum_{\tau'\in\mathbb{F}}\mathbf{x}(\tau')\mathbf{y}(\alpha^{-1}\tau-\tau') &= \frac{1}{\sqrt{q}}\sum_{\tau'\in\mathbb{F}}\mathbf{x}(\alpha^{-1}\tau')\mathbf{y}(\alpha^{-1}\tau-\alpha^{-1}\tau') \\ &= \frac{1}{\sqrt{q}}\sum_{\tau'\in\mathbb{F}}\mathbf{x}(\alpha^{-1}\tau')\mathbf{y}(\alpha^{-1}(\tau-\tau')) \\ &= \frac{1}{\sqrt{q}}\sum_{\tau'\in\mathbb{F}}D_\alpha\mathbf{x}(\tau')D_\alpha\mathbf{y}(\tau-\tau') = (D_\alpha\mathbf{x})*(D_\alpha\mathbf{y})(\tau),\end{aligned}$$

which implies that $D_\alpha(\mathbf{x}*\mathbf{y}) = (D_\alpha\mathbf{x})*(D_\alpha\mathbf{y})$.
We can also write

$$\begin{aligned}(D_\alpha\mathbf{x})^*(\tau) &= \overline{D_\alpha\mathbf{x}(-\tau)} \\ &= \overline{\mathbf{x}(-\alpha^{-1}\tau))} \\ &= \mathbf{x}^*(\alpha^{-1}\tau) = D_\alpha\mathbf{x}^*(\tau),\end{aligned}$$

which guarantees $(D_\alpha\mathbf{x})^* = D_\alpha\mathbf{x}^*$.
(2) Let $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then we can write

$$\begin{aligned}\|D_\alpha\mathbf{x}\|_2^2 &= \sum_{\tau\in\mathbb{F}}|D_\alpha\mathbf{x}(\tau)|^2 \\ &= \sum_{\tau\in\mathbb{F}}|\mathbf{x}(\alpha^{-1}\tau)|^2 \\ &= \sum_{\tau\in\mathbb{F}}|\mathbf{x}(\tau)|^2 = \|\mathbf{x}\|_2^2,\end{aligned}$$

which implies that $D_\alpha : \mathbb{C}^{\mathbb{F}} \to \mathbb{C}^{\mathbb{F}}$ is unitary in $\|.\|_2$-norm and satisfies

$$(D_\alpha)^* = (D_\alpha)^{-1} = D_{\alpha^{-1}}.$$

■

In the remainder of this article, we use the explicit characterization of the character group given by (6). Using (6), which can be considered as a consequence of analytic and algebraic properties of the trace map, the finite field $\mathbb{F}$ parametrizes the full character group $\widehat{\mathbb{F}^+}$. This parametrization implies a unified labeling on the character group $\widehat{\mathbb{F}^+}$ with $\mathbb{F}$.

Then we can present the following proposition.

Proposition 4.3 *Let $\mathbb{F}$ be a finite field and $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$. Then*

(1) $M_\gamma : \mathbb{C}^{\mathbb{F}} \to \mathbb{C}^{\mathbb{F}}$ is a unitary operator in $\|.\|_2$-norm and satisfies $(M_\gamma)^* = (M_\gamma)^{-1} = M_{-\gamma}$.
(2) For $\alpha\in\mathbb{F}^*$ we have $D_\alpha M_\gamma = M_{\alpha^{-1}\gamma}D_\alpha$.
(3) For $\beta\in\mathbb{F}$ we have $T_\beta M_\gamma = \chi_\gamma(\beta)M_\gamma T_\beta$.

Proof. (1) This statement is evident invoking definition of modulation operators.

(2) Let $\alpha \in \mathbb{F}^*$. Let $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$ and $\tau \in \mathbb{F}$. Then we can write

$$\begin{aligned} D_\alpha M_\gamma \mathbf{x}(\tau) &= M_\gamma \mathbf{x}(\alpha^{-1}\tau) \\ &= \overline{\chi_\gamma(\alpha^{-1}\tau)}\mathbf{x}(\alpha^{-1}\tau) \\ &= \overline{\chi(\gamma\alpha^{-1}\tau)}\mathbf{x}(\alpha^{-1}\tau) \\ &= \overline{\chi(\alpha^{-1}\gamma\tau)}\mathbf{x}(\alpha^{-1}\tau) \\ &= \overline{\chi_{\alpha^{-1}\gamma}(\tau)}\mathbf{x}(\alpha^{-1}\tau) \\ &= \overline{\chi_{\alpha^{-1}\gamma}(\tau)}D_\alpha\mathbf{x}(\tau) = M_{\alpha^{-1}\gamma}D_\alpha\mathbf{x}(\tau), \end{aligned}$$

which implies $D_\alpha M_\gamma = M_{\alpha^{-1}\gamma}D_\alpha$.

(3) Let $\beta \in \mathbb{F}$. Let $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$ and $\tau \in \mathbb{F}$. Then we have

$$\begin{aligned} T_\beta M_\gamma \mathbf{x}(\tau) &= M_\gamma \mathbf{x}(\tau - \beta) \\ &= \overline{\chi_\gamma(\tau-\beta)}\mathbf{x}(\tau-\beta) \\ &= \overline{\chi_\gamma(-\beta)\chi_\gamma(\tau)}\mathbf{x}(\tau-\beta) \\ &= \overline{\chi_\gamma(-\beta)\chi_\gamma(\tau)}T_\beta\mathbf{x}(\tau) = \chi_\gamma(\beta)M_\gamma T_\beta\mathbf{x}(\tau), \end{aligned}$$

which implies $T_\beta M_\gamma = \chi_\gamma(\beta)M_\gamma T_\beta$. ■

For $\alpha \in \mathbb{F}^*$, let $\widehat{D}_\alpha : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ be given by

$$\widehat{D}_\alpha\mathbf{x}(\chi_\gamma) := \mathbf{x}(\chi_{\alpha^{-1}\gamma}),$$

for all $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$ and $\mathbf{x} \in \mathbb{C}^{\widehat{\mathbb{F}}}$. Since $\mathbb{F}$ and $\widehat{\mathbb{F}^+}$ are isomorphic as finite Abelian groups, we may use D_α instead of $\widehat{D}_\alpha$ at times.

The following proposition presents some analytic properties of dilation operators on the frequency domain.

Proposition 4.4 *Let $\mathbb{F}$ be a finite field and $\alpha \in \mathbb{F}^*$. Then*

(1) $D_\alpha : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ is a $*$-isometric isomorphism of the Banach $*$-algebra $\mathbb{C}^{\widehat{\mathbb{F}^+}}$

(2) $D_\alpha : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ is unitary in $\|.\|_2$-norm and satisfies $(D_\alpha)^* = (D_\alpha)^{-1} = D_{\alpha^{-1}}$.

Next result states analytic properties of dilation operators and also connections with the Fourier transform.

Proposition 4.5 *Let $\mathbb{F}$ be a finite field of order q. Then*

(1) For $\beta \in \mathbb{F}$ we have $\mathcal{F}_{\mathbb{F}}T_\beta = M_\beta\mathcal{F}_{\mathbb{F}}$.

(2) For $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$ we have $\mathcal{F}_{\mathbb{F}}M_\gamma = T_{-\gamma}\mathcal{F}_{\mathbb{F}}$.

(3) For $\alpha \in \mathbb{F}^*$ we have $\mathcal{F}_{\mathbb{F}}D_\alpha = \widehat{D}_{\alpha^{-1}}\mathcal{F}_{\mathbb{F}}$.

Proof. (1) Let $\beta \in \mathbb{F}$ and $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$. Then for $\gamma \asymp \chi_\gamma \in \widehat{\mathbb{F}^+}$ we have

$$\mathcal{F}_{\mathbb{F}}(T_\beta\mathbf{x})(\chi_\gamma) = \frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}} T_\beta\mathbf{x}(\tau)\overline{\chi_\gamma(\tau)} = \frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau-\beta)\overline{\chi_\gamma(\tau)}.$$

Replacing τ with $\tau+\beta$ we get

$$\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau-\beta)\overline{\chi_\gamma(\tau)}=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\chi_\gamma(\tau+\beta)}=\frac{\overline{\chi_\gamma(\beta)}}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\chi_\gamma(\tau)}.$$

Then we can write

$$\begin{aligned}\mathcal{F}_{\mathbb{F}}(T_\beta\mathbf{x})(\chi_\gamma)&=\overline{\chi_\gamma(\beta)}\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\chi_\gamma)\\&=\overline{\chi_\gamma(\beta)}\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\chi_\gamma)=\overline{\chi_\beta(\gamma)}\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\chi_\gamma),\end{aligned}$$

implying $\mathcal{F}_{\mathbb{F}}T_\beta=M_\beta\mathcal{F}_{\mathbb{F}}$.

(2) Let $\gamma\asymp\chi_\gamma\in\widehat{\mathbb{F}^+}$ and $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then for all $\gamma'\asymp\chi_{\gamma'}\in\widehat{\mathbb{F}^+}$ we have

$$\begin{aligned}\mathcal{F}_{\mathbb{F}}(M_\gamma\mathbf{x})(\gamma')&=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}M_\gamma\mathbf{x}(\tau)\overline{\chi_\gamma(\tau)}\\&=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\chi_\gamma(\tau)\mathbf{x}(\tau)\overline{\chi_{\gamma'}(\tau)}\\&=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\chi_{\gamma+\gamma'}(\tau)}\\&=\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\gamma+\gamma')=T_{-\gamma}\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\gamma').\end{aligned}$$

(3) Let $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$ and $\gamma\asymp\chi_\gamma\in\widehat{\mathbb{F}^+}$. Then we have

$$\mathcal{F}_{\mathbb{F}}(D_\alpha\mathbf{x})(\gamma)=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}D_\alpha\mathbf{x}(\tau)\overline{\chi_\gamma(\tau)}=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\alpha^{-1}\tau)\overline{\chi_\gamma(\tau)}.$$

Replacing τ with $\alpha\tau$ we achieve

$$\begin{aligned}\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\alpha^{-1}\tau)\overline{\chi_\gamma(\tau)}&=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\chi_\gamma(\alpha\tau)}\\&=\frac{1}{\sqrt{q}}\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\chi_{\alpha\gamma}(\tau)}=\mathcal{F}_{\mathbb{F}}(\mathbf{x})(\alpha\gamma),\end{aligned}$$

which implies $\mathcal{F}_{\mathbb{F}}(D_\alpha\mathbf{x})=\widehat{D}_{\alpha^{-1}}(\mathcal{F}_{\mathbb{F}}\mathbf{x})$. ■

The underlying set $\mathbb{F}^*\times\mathbb{F}$ equipped with group operations given by

$$(\alpha,\beta)\rtimes(\alpha',\beta'):=(\alpha\alpha',\beta+\alpha\beta') \tag{8}$$

$$(\alpha,\beta)^{-1}:=(\alpha^{-1},\alpha^{-1}.(-\beta)) \tag{9}$$

for all $(\alpha,\beta),(\alpha',\beta')\in\mathbb{F}^*\times\mathbb{F}$, is a finite non-Abelian group of order $q\cdot(q-1)$ which is denoted by $\mathrm{W}_{\mathbb{F}}=\mathbb{F}^*\rtimes\mathbb{F}$. The group $\mathbb{F}^*\rtimes\mathbb{F}$ is called as **classical wavelet group** over the finite field $\mathbb{F}$. Since any two field of order $q=p^d$ are isomorphic as finite field, we deduce that the notion of $\mathbb{F}^* \rtimes \mathbb{F}$ just depends on q. In details, if $\mathbb{F}$ and $\mathbb{K}$ are two finite field of order q, then the groups $\mathbb{F}^* \rtimes \mathbb{F}$ and $\mathbb{K}^* \rtimes \mathbb{K}$ are isomorphic as finite groups of order $q \cdot (q-1)$.

Next theorem guarantees that the group structure of the wavelet group $\mathbb{F}^* \rtimes \mathbb{F}$ is canonically connected with a group representation.

Theorem 4.6 *Let $\mathbb{F}$ be a finite field of order $q > 2$. Then*

(1) $\mathbb{F}^* \rtimes \mathbb{F}$ is a non-Abelian group of order $q \cdot (q-1)$ which contains $\mathbb{F}$ as a normal Abelian subgroup and $\mathbb{F}^*$ as a non-normal cyclic subgroup.

(2) The map $\rho : \mathbb{F}^* \rtimes \mathbb{F} \to \mathcal{U}(\mathbb{C}^{\mathbb{F}}) \cong \mathbf{U}_{q\times q}(\mathbb{C})$ defined by

$$(\alpha, \beta) \mapsto \rho(\alpha, \beta) := T_\beta D_\alpha \quad \text{for } (\alpha, \beta) \in \mathbb{F}^* \rtimes \mathbb{F}, \tag{10}$$

is a group representation of the finite classical wavelet group $\mathbb{F}^* \rtimes \mathbb{F}$ on the finite dimensional Hilbert space $\mathbb{C}^{\mathbb{F}}$.

Proof. Let $\mathbb{F}$ be a finite field of order $q > 2$. Then
(1) It is straightforward from the group structure given in (8) that $\mathbb{F}$ is a normal Abelian subgroup and $\mathbb{F}^*$ is a non-normal Abelian subgroup of $\mathbb{F}^* \rtimes \mathbb{F}$.
(2) It is evident to check that $\rho(1, 0) = I$ and $\rho(\alpha, \beta) : \mathbb{C}^{\mathbb{F}} \to \mathbb{C}^{\mathbb{F}}$ is a unitary operator for all $(\alpha, \beta) \in \mathbb{F}^* \rtimes \mathbb{F}$. Now let $(\alpha, \beta), (\alpha', \beta') \in \mathbb{F}^* \rtimes \mathbb{F}$. Then using Proposition 4.1, we can write

$$T_{\beta+\alpha\beta'} D_{\alpha\alpha'} = T_\beta T_{\alpha\beta'} D_\alpha D_{\alpha'} = T_\beta D_\alpha T_{\beta'} D_{\alpha'}.$$

Thus, we get

$$\begin{aligned}\rho\left((\alpha, \beta) \rtimes (\alpha', \beta')\right) &= \rho(\alpha\alpha', \beta + \alpha\beta') \\ &= T_{\beta+\alpha\beta'} D_{\alpha\alpha'} \\ &= T_\beta D_\alpha T_{\beta'} D_{\alpha'} = \rho(\alpha, \beta)\rho(\alpha', \beta'),\end{aligned}$$

which implies that ρ is a group representation of the finite wavelet group $\mathbb{F}^* \rtimes \mathbb{F}$ on the finite dimensional Hilbert space $\mathbb{C}^{\mathbb{F}}$. ∎

Remark 3 *In terms of abstract wavelet transforms over locally compact groups, the representation ρ mentioned in Theorem 4.6 is precisely the quasi regular representation generated by the action of the multiplicative group $H = \mathbb{F}^*$ on the finite additive group $K = \mathbb{F}$ on the Hilbert space $\mathbb{C}^{\mathbb{F}}$, see [1–3] and references therein.*

5. Classical Wavelet Transforms over Finite Fields

In this section we present the abstract theory of classical wavelet transforms over finite fields and we study analytic properties of this transform. Throughout this section, it is still assumed that $\mathbb{F}$ is a finite field of order $q = p^d$.

Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a window vector/signal and $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$. The wavelet transform of $\mathbf{x}$ with respect to $\mathbf{y}$ is $W_{\mathbf{y}}\mathbf{x} : \mathbb{F}^* \rtimes \mathbb{F} \to \mathbb{C}$ given by

$$W_{\mathbf{y}}\mathbf{x}(\alpha, \beta) := \sum_{\tau\in\mathbb{F}} \mathbf{x}(\tau)\overline{\mathbf{y}(\alpha^{-1}(\tau - \beta))}, \tag{11}$$

for all $(\alpha,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}$. Then $W_{\mathbf{y}}:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}^*\rtimes\mathbb{F}}$ given by $\mathbf{x}\mapsto W_{\mathbf{y}}\mathbf{x}$ is a linear transformation.

By definition (11) and using inner product terms, we can write

$$\begin{aligned}W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)&=\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\mathbf{y}(\alpha^{-1}(\tau-\beta))}\\&=\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{D_\alpha\mathbf{y}(\tau-\beta)}\\&=\sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{T_\beta D_\alpha\mathbf{y}(\tau)}\\&=\langle\mathbf{x},T_\beta D_\alpha\mathbf{y}\rangle=\langle\mathbf{x},\rho(\alpha,\beta)\mathbf{y}\rangle.\end{aligned}$$

Also, invoking properties of the dilation and translation operators we get

$$\langle\mathbf{x},\rho(\alpha,\beta)\mathbf{y}\rangle=\langle\mathbf{x},T_\beta D_\alpha\mathbf{y}\rangle=\langle T_{-\beta}\mathbf{x},D_\alpha\mathbf{y}\rangle,\quad\text{for }(\alpha,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}.\tag{12}$$

The following proposition gives us a Fourier (resp. convolution) representation for the wavelet matrix.

Proposition 5.1 *Let $\mathbb{F}$ be a finite field of order q. Let $\mathbf{x},\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ and $(\alpha,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}$. Then,*

(1) $W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)=\sqrt{q}\mathcal{F}_q(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}})(\beta)$.
(2) $W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)=\mathbf{x}*D_\alpha\mathbf{y}^*(\beta)$.

Proof. Let $\mathbf{x},\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ and $(\alpha,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}$. (1) Using the Plancherel formula we have

$$\begin{aligned}W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)&=\langle\mathbf{x},\rho(\alpha,\beta)\mathbf{y}\rangle\\&=\langle\mathbf{x},T_\beta D_\alpha\mathbf{y}\rangle\\&=\langle\widehat{\mathbf{x}},\widehat{T_\beta D_\alpha\mathbf{y}}\rangle\\&=\sum_{\gamma\in\widehat{\mathbb{F}^+}}\widehat{\mathbf{x}}(\gamma)\overline{\widehat{T_\beta D_\alpha}\mathbf{y}(\gamma)}\\&=\sum_{\gamma\in\widehat{\mathbb{F}^+}}\widehat{\mathbf{x}}(\gamma)\overline{M_\beta\widehat{D_\alpha\mathbf{y}}(\gamma)}\\&=\sum_{\gamma\in\widehat{\mathbb{F}^+}}\widehat{\mathbf{x}}(\gamma)\overline{\widehat{D_\alpha\mathbf{y}}(\gamma)}\chi_\beta(\gamma)\\&=\sum_{\gamma\in\widehat{\mathbb{F}^+}}\left(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}}\right)(\gamma)\overline{\chi_\gamma(-\beta)}=\sqrt{q}\mathcal{F}_q(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}})(-\beta).\end{aligned}$$

(2) Similarly using the Plancherel formula we can write

$$\begin{aligned}
W_{\mathbf{y}}\mathbf{x}(\alpha,\beta) &= \langle \mathbf{x}, \rho(\alpha,\beta)\mathbf{y}\rangle \\
&= \sum_{\gamma\in\widehat{\mathbb{F}^+}} \widehat{\mathbf{x}}(\gamma)\overline{\widehat{D_\alpha\mathbf{y}}(\gamma)}\chi_\beta(\gamma) \\
&= \sum_{\gamma\in\widehat{\mathbb{F}^+}} \widehat{\mathbf{x}}(\gamma)(\widehat{D_\alpha\mathbf{y})}^*(\gamma)\chi_\beta(\gamma) \\
&= \sum_{\gamma\in\widehat{\mathbb{F}^+}} \widehat{\mathbf{x}}(\gamma)(\widehat{D_\alpha\mathbf{y}^*})(\gamma)\chi_\beta(\gamma) = \sum_{\gamma\in\widehat{\mathbb{F}^+}} \widehat{\mathbf{x}*D_\alpha}\mathbf{y}^*(\gamma)\chi_\beta(\gamma) = \mathbf{x}*D_\alpha\mathbf{y}^*(\beta).
\end{aligned}$$

∎

In the following theorem we present an analytic formulation for the Frobenius norm of the wavelet transform $W_{\mathbf{y}}\mathbf{x}$.

Theorem 5.2 Let $\mathbb{F}$ be a finite field of order q. Let $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ be a window vector and $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then

$$\|W_{\mathbf{y}}\mathbf{x}\|_{\mathrm{Fr}}^2 = q\left((q-1)|\widehat{\mathbf{x}}(0)|^2|\widehat{\mathbf{y}}(0)|^2 + \left(\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\right)\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_\alpha)|^2\right)\right). \qquad (13)$$

Proof. Let $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ be a window function, $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$, and $\alpha\in\mathbb{F}^*$. Using Proposition 5.1 we have

$$\begin{aligned}
\sum_{\beta\in\mathbb{F}}|\langle \mathbf{x},\rho(\alpha,\beta)\mathbf{y}\rangle|^2 &= q\sum_{\beta\in\mathbb{F}}\left|\mathcal{F}_q(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}})(-\beta)\right|^2 \\
&= q\sum_{\beta\in\mathbb{F}}\left|\mathcal{F}_q(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}})(\beta)\right|^2 \\
&= q\sum_{\gamma\in\mathbb{F}}\left|(\widehat{\mathbf{x}}.\overline{\widehat{D_\alpha\mathbf{y}}})(\chi_\gamma)\right|^2 = q\sum_{\gamma\in\mathbb{F}}\left|\widehat{\mathbf{x}}(\chi_\gamma).\overline{\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)}\right|^2.
\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}^*}\sum_{\beta\in\mathbb{F}}|\langle\mathbf{x},\rho(\alpha,\beta)\mathbf{y}\rangle|^2 &= q\sum_{\alpha\in\mathbb{F}^*}\sum_{\gamma\in\mathbb{F}}\left|\widehat{\mathbf{x}}(\chi_\gamma).\overline{\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)}\right|^2\\ &= q\sum_{\alpha\in\mathbb{F}^*}\sum_{\gamma\in\mathbb{F}}\left|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot|\overline{\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)}\right|^2\\ &= q\sum_{\gamma\in\mathbb{F}}\sum_{\alpha\in\mathbb{F}^*}\left|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot|\overline{\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)}\right|^2\\ &= q\sum_{\gamma\in\mathbb{F}}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot\left(\sum_{\alpha\in\mathbb{F}^*}|\overline{\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)}|^2\right)\\ &= q\sum_{\gamma\in\mathbb{F}}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)|^2\right).\end{aligned}$$

Now we have

$$\begin{aligned}\sum_{\gamma\in\mathbb{F}}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)|^2\right) &= |\widehat{\mathbf{x}}(0)|^2\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(0)|^2\right)\\ &\quad+\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_{\alpha\gamma})|^2\right).\end{aligned}$$

Replacing α with $\gamma^{-1}\alpha$ we have

$$\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_{\alpha\gamma})|^2=\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_\alpha)|^2,$$

which implies

$$\begin{aligned}&\sum_{\gamma\in\mathbb{F}}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{D_\alpha\mathbf{y}}(\chi_\gamma)|^2\right)\\ &=|\widehat{\mathbf{x}}(0)|^2\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(0)|^2\right)+\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_{\alpha\gamma})|^2\right)\\ &=(q-1)|\widehat{\mathbf{x}}(0)|^2|\widehat{\mathbf{y}}(0)|^2+\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_{\alpha\gamma})|^2\right)\\ &=(q-1)|\widehat{\mathbf{x}}(0)|^2|\widehat{\mathbf{y}}(0)|^2+\left(\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\right)\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_\alpha)|^2\right).\end{aligned}$$

Hence, we get

$$\|W_{\mathbf{y}}\mathbf{x}\|_{\mathrm{Fr}}^2 = q\left((q-1)|\widehat{\mathbf{x}}(0)|^2|\widehat{\mathbf{y}}(0)|^2 + \left(\sum_{\gamma\in\mathbb{F}^*}|\widehat{\mathbf{x}}(\chi_\gamma)|^2\right)\left(\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_\alpha)|^2\right)\right).$$

■

Then we conclude the following results.

Corollary 5.3 *Let* $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ *be a window vector with* $\widehat{\mathbf{y}}(0)\neq 0$ *and* $\|\widehat{\mathbf{y}}\|_0\geq 2$. *The classic wavelet transform* $W_{\mathbf{y}}$ *is a multiple of an isometric transform if and only if* $\mathbf{y}$ *satisfies* $\|\mathbf{y}\|_{\mathbf{Fr}}=\sqrt{q}|\widehat{\mathbf{y}}(0)|$. *In this case,*

$$\|W_{\mathbf{y}}\mathbf{x}\|_{\mathbf{Fr}}^2 = c_{\mathbf{y}}\|\mathbf{x}\|_{\mathbf{Fr}}^2,\quad \text{for all } \mathbf{x}\in\mathbb{C}^{\mathbb{F}}, \tag{14}$$

where

$$c_{\mathbf{y}} := (q-1)\left|\sum_{\tau\in\mathbb{F}}\mathbf{y}(\tau)\right|^2 = q\cdot(q-1)\cdot|\widehat{\mathbf{y}}(0)|^2 = q\sum_{\alpha\in\mathbb{F}^*}|\widehat{\mathbf{y}}(\chi_\alpha)|^2. \tag{15}$$

From now on, a vector $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ with $\widehat{\mathbf{y}}(0)\neq 0$ and $\|\widehat{\mathbf{y}}\|_0\geq 2$ is called **admissible**, if $\mathbf{y}$ satisfies $\|\mathbf{y}\|_{\mathbf{Fr}}=\sqrt{q}|\widehat{\mathbf{y}}(0)|$. In this case, the constant $c_{\mathbf{y}}$ is called as **classic wavelet constant** of $\mathbf{y}$.

Next result states an inversion formula for the windowed transform given in (11).

Theorem 5.4 *Let* $\mathbb{F}$ *be a finite field of order* $q=p^d$. *Let* $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ *be an admissible window vector and* $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. *Then*

$$\mathbf{x}(\tau) = c_{\mathbf{y}}^{-1}\cdot\sum_{\alpha\in\mathbb{F}^*}\sum_{\beta\in\mathbb{F}}W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)T_\beta D_\alpha\mathbf{y}(\tau),\quad \text{for } \tau\in\mathbb{F}. \tag{16}$$

Proof. For $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$ and a non-zero window vector $\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$, define

$$\widetilde{\mathbf{x}}(\tau) := \sum_{\alpha\in\mathbb{F}^*}\sum_{\beta\in\mathbb{F}}W_{\mathbf{y}}\mathbf{x}(\alpha,\beta)T_\beta D_\alpha\mathbf{y}(\tau),\quad \text{for } \tau\in\mathbb{F}.$$

Let $\mathbf{z} \in \mathbb{C}^{\mathbb{F}}$ be given. Using (14) we have

$$\begin{aligned}
\langle \widetilde{\mathbf{x}}, \mathbf{z} \rangle_{\mathbb{C}^{\mathbb{F}}} &= \sum_{\tau \in \mathbb{F}} \widetilde{\mathbf{x}}(\tau)\overline{\mathbf{z}(\tau)} \\
&= \sum_{\tau \in \mathbb{F}} \left(\sum_{\alpha \in \mathbb{F}^*} \sum_{\beta \in \mathbb{F}} W_{\mathbf{y}}\mathbf{x}(\alpha,\beta) T_\beta D_\alpha \mathbf{y}(\tau) \right) \overline{\mathbf{z}(\tau)} \\
&= \sum_{\alpha \in \mathbb{F}^*} \sum_{\beta \in \mathbb{F}} W_{\mathbf{y}}\mathbf{x}(\alpha,\beta) \left(\sum_{\tau \in \mathbb{F}} \overline{\mathbf{z}(\tau)} T_\beta D_\alpha \mathbf{y}(\tau) \right) \\
&= \sum_{\alpha \in \mathbb{F}^*} \sum_{\beta \in \mathbb{F}} W_{\mathbf{y}}\mathbf{x}(\alpha,\beta) \left(\sum_{\tau \in \mathbb{F}} \mathbf{z}(\tau) T_\beta D_\alpha \overline{\mathbf{y}}(\tau) \right)^{-} \\
&= \sum_{\alpha \in \mathbb{F}^*} \sum_{\beta \in \mathbb{F}} W_{\mathbf{y}}\mathbf{x}(\alpha,\beta) \overline{W_{\mathbf{y}}\mathbf{z}(\alpha,\beta)} \\
&= \langle W_{\mathbf{y}}\mathbf{x}, W_{\mathbf{y}}\mathbf{z} \rangle_{\mathbb{C}^{\mathrm{W}_{\mathbb{F}}}} = c_{\mathbf{y}} \cdot \langle \mathbf{x}, \mathbf{z} \rangle_{\mathbb{C}^{\mathbb{F}}},
\end{aligned}$$

implying

$$\mathbf{x}(\tau) = c_{\mathbf{y}}^{-1} \cdot \widetilde{\mathbf{x}}(\tau), \quad \text{for } \tau \in \mathbb{F},$$

which guarantees (16). ■

Acknowledgement

The author would like to express his deepest gratitude to Prof. Hans G. Feichtinger for his valuable comments.

References

[1] A. Arefijamaal and R.A. Kamyabi-Gol. *On the square integrability of quasi regular representation on semidirect product groups*, J. Geom. Anal., 19 (3), (2009), 541-552.
[2] A. Arefijamaal and R.A. Kamyabi-Gol. *On construction of coherent states associated with semidirect products*, Int. J. Wavelets Multiresolut. Inf. Process. 6 (5), (2008), 749-759.
[3] A. Arefijamaal and R.A. Kamyabi-Gol, *A Characterization of square integrable representations associated with CWT*, J. Sci. Islam. Repub. Iran 18 (2), (2007), 159-166.
[4] G. Caire, R.L. Grossman, and H. Vincent Poor. Wavelet transforms associated with finite cyclic groups. *IEEE Transaction On Information Theory* 39 (4), (1993), 113-119.
[5] F. Fekri, R.M. Mersereau, and R.W. Schafer. Theory of wavelet transform over finite fields. *Proceedings of International Conference on Acoustics, Speech, and Signal Processing.*, 3, (1999), 1213-1216.
[6] K. Flornes, A. Grossmann, M. Holschneider, and B. Torrésani. Wavelets on discrete fields. *Appl. Comput. Harmon. Anal.*, 1, (1994), 137-146.
[7] A. Ghaani Farashahi, *Structure of finite wavelet frames over prime fields*, Bull. Iranian Math. Soc., to appear 2016.
[8] A. Ghaani Farashahi, *Wave packet transforms over finite cyclic groups*, Linear Algebra Appl., 489 (2016), 75-92.
[9] A. Ghaani Farashahi, *Wave packet transform over finite fields*, Electronic Journal of Linear Algebra, Volume 30 (2015), 507-529.
[10] A. Ghaani Farashahi. *Cyclic wavelet systems in prime dimensional linear vector spaces*, Wavelets and Linear Algebra 2 (1), (2015), 11-24.
[11] A. Ghaani Farashahi. Cyclic wave packet transform on finite Abelian groups of prime order. *Int. J. Wavelets Multiresolut. Inf. Process.*, 12 (6), (2014), 1450041 (14 pages).

[12] A. Ghaani Farashahi and M. Mohammad-Pour. A unified theoretical harmonic analysis approach to the cyclic wavelet transform (CWT) for periodic signals of prime dimensions., Sahand Commun. Math. Anal., 1 (2), (2014), 1-17.

[13] A. Ghaani Farashahi and R. Kamyabi-Gol. Gabor transform for a class of non-abelian groups., *Bull. Belg. Math. Soc. Simon Stevin.*, 19 (4), (2012), 683-701.

[14] C.P. Johnston. On the pseudodilation representations of flornes, grossmann, holschneider, and torrésani. *J. Fourier Anal. Appl.*, 3 (4), (1997), 377-385.

[15] G.L. Mullen and D. Panario. *Handbook of Finite Fields.*, Series: Discrete Mathematics and Its Applications, Chapman and Hall/CRC, 2013.

[16] R.J. McEliece. *Finite Fields for Computer Scientists and Engineers.*, The Springer International Series in Engineering and Computer Science, 1987.

[17] O. Pretzel. *Error-Correcting Codes and Finite Fields.*, Oxford Applied Mathematics and Computing Science Series, 1996.

[18] D. Ramakrishnan and R.J. Valenza. *Fourier Analysis on Number Fields.*, Springer-Verlag, New York, 1999.

[19] R. Reiter and J.D. Stegeman. *Classical Harmonic Analysis.*, 2nd Ed, Oxford University Press, New York, 2000.

[20] H. Riesel. *Prime Numbers and Computer Methods for Factorization.*, (second edition), Boston: Birkhauser, 1994.

[21] S. Sarkar and H. Vincent Poor. Cyclic wavelet transforms for arbitrary finite data lengths. *Signal Processing* 80 (2000), 2541-2552.

[22] G. Strang and T. Nguyen. *Wavelets and Filter Banks*, Wellesley-Cambridge Press, Wellesley, 1996.

[23] S. A. Vanstone and P. C. Van Oorschot. *An Introduction to Error Correcting Codes with Applications.*, The Springer International Series in Engineering and Computer Science, 1989.

[24] A. Vourdas. Harmonic analysis on a Galois field and its subfields. *J. Fourier Anal. Appl.*, 14 (1), (2008), 102-123.

[25] M.W. Wong. *Discrete Fourier Analysis.* Pseudo-differential Operators Theory and applications Vol. 5, Springer-Birkhauser, 2010.