ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 49, Number 1, 2019

GALOIS WAVELET TRANSFORMS OVER FINITE FIELDS

ARASH GHAANI FARASHAHI

ABSTRACT. In this article, we introduce the abstract notion of Galois wavelet groups over finite fields as the finite group of Galois dilations, and translations. We then present a unified theoretical linear algebra approach to the theory of Galois 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 Galois wavelet coefficients as well.

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 [**17, 19, 25**]. Discrete exponentiation can be quickly computed using techniques of fast exponentiation such as binary exponentiation within a finite field operations. In addition, in coding theory, many codes are constructed as subspaces of vector spaces over finite fields, see [**18, 21**] and the references therein.

Finite-dimensional data analysis and signal processing are the basis of digital signal processing, information theory and large scale data analysis. In data processing, time-frequency (respectively, time-scale) analysis comprises those techniques that analyze a vector in both time and frequency (respectively, time and scale) domains simultaneously, called time-frequency (respectively, time-scale) methods or representations, see [**4**] and the references therein. Commonly used coherent (structured) methods and techniques in such analyses are time-frequency analysis, which is sometimes called Gabor analysis [**5**], time-scale analysis, which is called wavelet analysis [**8, 14**] and scale-time-frequency analysis which, is mostly called wave packet methods, see

2010 AMS *Mathematics subject classification.* Primary 12E20, 42C40, Secondary 12F10, 13B05, 20G40, 81R05.

Keywords and phrases. Finite field, Galois wavelet group, Galois wavelet representation, Galois wavelet transform, Galois dilation operator, periodic (finite size) data, prime integer.

Received by the editors on February 21, 2017, and in revised form on July 21, 2018.

DOI:10.1216/RMJ-2019-49-1-79

[**9, 12, 13**] and the references therein. The theory of Gabor analysis is based on the modulations and translations of a given window vector, and the phase space has a unified group structure, see [**2, 3, 20**] and the references therein. Wavelet theory is based on the affine group as the group of dilations and translation, see [**1**] and the references therein. Wave packet analysis is a shrewd coherent state analysis which is an extension of the two most important and prominent coherent state methods, namely, wavelet and Gabor analysis [**6, 10, 11, 16**].

In this article, we introduce the notion of Galois wavelet groups associated to the finite field $\mathbb{F}$ as the group of Galois dilations and translations. We then present the abstract theory of Galois wavelet transform over $\mathbb{F}$. If $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ is a window vector, we define the Galois wavelet transform $W_{\mathbf{y}}$ as the voice transform defined on $\mathbb{C}^{\mathbb{F}}$ with complex values which are indexed in the finite Galois wavelet group. These techniques imply a unified group theoretical based Galois dilation, translation representations for vectors in $\mathbb{C}^{\mathbb{F}}$. It is shown that the Galois wavelet transform $W_{\mathbf{y}}$ as a windowed transform satisfies the isometric property and the inversion formula as well.

2. Preliminaries and notation. Let $\mathbb{H}$ be a finite-dimensional complex Hilbert space and $\dim \mathbb{H} = N$. A finite system (sequence) $\mathfrak{A} = \{\mathbf{y}_j : 0 \leq j \leq M-1\} \subset \mathbb{H}$ is called a *frame* (or *finite frame*) for $\mathbb{H}$, if there exist positive constants $0 < A \leq B < \infty$ such that

$$A\|\mathbf{x}\|^2 \leq \sum_{j=0}^{M-1} |\langle \mathbf{x}, \mathbf{y}_j \rangle|^2 \leq B\|\mathbf{x}\|^2 \quad \text{for all } \mathbf{x} \in \mathbb{H}. \tag{2.1}$$

If $\mathfrak{A} = \{\mathbf{y}_j : 0 \leq j \leq M-1\}$ is a frame for $\mathbb{H}$, the synthesis operator $F : \mathbb{C}^M \to \mathbb{H}$ is $F\{c_j\}_{j=0}^{M-1} = \sum_{j=0}^{M-1} c_j \mathbf{y}_j$ for all $\{c_j\}_{j=0}^{M-1} \in \mathbb{C}^M$. The adjoint (analysis) operator $F^* : \mathbb{H} \to \mathbb{C}^M$ is $F^*\mathbf{x} = \{\langle \mathbf{x}, \mathbf{y}_j \rangle\}_{j=0}^{M-1}$ for all $\mathbf{x} \in \mathbb{H}$. By composing F and F^*, we get the positive and invertible frame operator $S : \mathbb{H} \to \mathbb{H}$, given by

$$\mathbf{x} \longmapsto S\mathbf{x} = FF^*\mathbf{x} = \sum_{j=0}^{M-1} \langle \mathbf{x}, \mathbf{y}_j \rangle \mathbf{y}_j \quad \text{for all } \mathbf{x} \in \mathbb{H}, \tag{2.2}$$

In terms of the analysis operator we have $A\|\mathbf{x}\|_2^2 \leq \|F^*\mathbf{x}\|_2^2 \leq B\|\mathbf{x}\|_2^2$ for $\mathbf{x} \in \mathbb{H}$. If $\mathfrak{A}$ is a finite frame for $\mathbb{H}$, the set $\mathfrak{A}$ spans the complex Hilbert space $\mathbb{H}$, which implies $M \geq N$, where $M = |\mathfrak{A}|$. It should be

mentioned that each finite spanning set in $\mathbb{H}$ is a finite frame for $\mathbb{H}$. The ratio between M and N is called a *redundancy of the finite frame* $\mathfrak{A}$ (i.e., $\mathrm{red}_{\mathfrak{A}} = M/N$), where $M = |\mathfrak{A}|$. If $\mathfrak{A} = \{\mathbf{y}_j : 0 \leq j \leq M-1\}$ is a finite frame for $\mathbb{H}$, each $\mathbf{x} \in \mathbb{H}$ satisfies the following reconstruction formulae:

$$\mathbf{x} = \sum_{j=0}^{M-1} \langle \mathbf{x}, S^{-1}\mathbf{y}_j \rangle \mathbf{y}_j = \sum_{j=0}^{M-1} \langle \mathbf{x}, \mathbf{y}_j \rangle S^{-1}\mathbf{y}_j. \tag{2.3}$$

In this case, the complex numbers $\langle \mathbf{x}, S^{-1}\mathbf{y}_j \rangle$ are called *frame coefficients*, and the finite sequence $\mathfrak{A}^{\bullet} := \{S^{-1}\mathbf{y}_j : 0 \leq j \leq M-1\}$, which is a frame for $\mathbb{H}$ as well, is called the *canonical dual frame* of $\mathfrak{A}$. A finite frame $\mathfrak{A} = \{\mathbf{y}_j : 0 \leq j \leq M-1\}$ for $\mathbb{H}$ is called *tight* if we have $A = B$. If $\mathfrak{A} = \{\mathbf{y}_j : 0 \leq j \leq M-1\}$ is a tight frame for $\mathbb{H}$ with frame bound A, then the canonical dual frame $\mathfrak{A}^{\bullet}$ is exactly $\{A^{-1}\mathbf{y}_j : 0 \leq j \leq M-1\}$ and, for $\mathbf{x} \in \mathbb{H}$, we have

$$\mathbf{x} = \frac{1}{A} \sum_{j=0}^{M-1} \langle \mathbf{x}, \mathbf{y}_j \rangle \mathbf{y}_j. \tag{2.4}$$

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 $\|\cdot\|_2$-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 the 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

$g=(g_1,\ldots,g_d)\in G$ 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 to frequency representations. It is defined as a function on $\widehat{G}$ by

$$\mathcal{F}_G(\mathbf{x})(\ell)=\widehat{\mathbf{x}}(\ell)=\frac{1}{\sqrt{|G|}}\sum_{g\in G}\mathbf{x}(g)\overline{\ell(g)} \tag{2.5}$$

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

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

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 $\|\cdot\|_2$-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 $\mathbf{x}*\mathbf{y}(k)=1/\sqrt{|G|}\sum_{g\in G}\mathbf{x}(g)T_g\mathbf{y}(k)$ 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 $\|\cdot\|_1$-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

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

The unitary DFT (2.5) satisfies

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

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 **[7, 23]**, and the 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, the reader is referred to **[15, 19, 22, 24, 25]**, and the 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 $d \geq 1$ 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 merely denote it by $\mathbb{F}$. The prime number p is called the *characteristic* of $\mathbb{F}$, which means that

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

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

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

is a linear basis of $\mathbb{F}$ over $\mathbb{Z}_p$. Then, $\mathcal{B}_\theta$ is called a *polynomial basis* of $\mathbb{F}$ over $\mathbb{Z}_p$ and θ is called 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 $0\leq j,k\leq d-1$, which is invertible with the inverse $\mathbf{S}\in\mathbb{Z}_p^{d\times d}$. Then, the dual polynomial basis

$$\widetilde{\mathcal{B}_\theta}:=\{\Theta_k:k=0,\ldots,d-1\},\tag{3.1}$$

given by

$$\Theta_k=\sum_{j=0}^{d-1}\mathbf{S}_{kj}\theta^j,\tag{3.2}$$

satisfies the following orthogonality relation

$$\mathbf{t}(\theta^k\Theta_j)=\delta_{k,j},\tag{3.3}$$

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

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*:

(i) *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 $k=0,\ldots,d-1$ we have

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

(ii) *for $\tau\in\mathbb{F}$ the coefficients (components) $\{\tau_{(k)}:k=0,\ldots,d-1\}$ and $\{\tau_{[k]}:k=0,\ldots,d-1\}$ 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 $k=0,\ldots,d-1$.

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

$$\gamma\longmapsto J_\theta(\tau):=\tau_\theta=(\tau_{(k)})_{k=1}^d,\quad \text{for all } \tau\in\mathbb{F}.\tag{3.4}$$

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

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

Remark 3.2. The dual (character) group of the finite elementary group $\mathbb{Z}_p^d$, that is, $\widehat{\mathbb{Z}_p^d}$, is precisely

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

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

$$\mathbf{e}_\ell(g) = \mathbf{e}_{1,p}(\ell \cdot g) = \exp\left(\frac{2\pi i\ \ell \cdot g}{p}\right) = \prod_{k=1}^{d} \mathbf{e}_{\ell_k,p}(g_k)$$

for all

$$g = (g_1, \ldots, g_d) \in \mathbb{Z}_p^d,$$

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

(i) *for* $\tau,\tau'\in\mathbb{F}$, *we have*

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

(ii) *for* $\tau,\tau'\in\mathbb{F}$, *we have*

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

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

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

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 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 $\mathbb{F}$. Specifically, 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 a group isomorphism of $\mathbb{F}$ onto $\widehat{\mathbb{F}^+}$. Then, for $\alpha=1$, we obtain

$$\widehat{\mathbb{F}^+}=\{\chi_\gamma:\gamma\in\mathbb{F}\}. \tag{3.5}$$

Remark 3.4. The characterization (3.5) for the character group of finite fields is a consequence of applying the trace map in duality theory

over finite fields. This characterization plays a significant role in the structure of dual action and hence wave packet groups over finite fields, see Section 4.

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

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

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 3.5.

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

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

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

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

and

$$\mathbf{x} \in \mathbb{C}^{\mathbb{F}}.$$

4. Galois wavelet groups over finite fields. Throughout this section, we shall present the abstract structure of Galois wavelet groups over finite fields.

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of order $q = p^d$. A bijective map $\sigma : \mathbb{F} \to \mathbb{F}$ is called a *Galois automorphism* of $\mathbb{F}$ over $\mathbb{Z}_p$, if

$$\sigma(\tau + \tau') = \sigma(\tau) + \sigma(\tau')$$

and

$$\sigma(\tau\tau') = \sigma(\tau)\sigma(\tau'),$$

for all $\tau,\tau'\in\mathbb{F}$, and also,

$$\sigma(k)=k,$$

for all $k\in\mathbb{Z}_p$.

Then, it can be shown that the distinct Galois automorphisms of $\mathbb{F}$ over $\mathbb{Z}_p$ are precisely the mappings $\{\sigma_j : 0\leq j\leq d-1\}$, where $\sigma_j:\mathbb{F}\to\mathbb{F}$ is defined by

$$\sigma_j(\tau)=\tau^{p^j},$$

for all $\tau\in\mathbb{F}$ and $0\leq j\leq d-1$.

The set of all Galois automorphisms of $\mathbb{F}$ over $\mathbb{Z}_p$ form a group under the composition of mappings, called the *Galois group* of $\mathbb{F}$ over $\mathbb{Z}_p$ and denoted by $\mathrm{Gal}(\mathbb{F}/\mathbb{Z}_p)$, or merely, $\mathrm{Gal}(\mathbb{F})$. The Galois group $\mathrm{Gal}(\mathbb{F})$ is a cyclic group of order d, generated by σ_1.

For $\sigma\in\mathrm{Gal}(\mathbb{F})$, define the *Galois dilation operator* $E_\sigma:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ by

$$E_\sigma\mathbf{x}(\tau):=\mathbf{x}(\sigma^{-1}\tau),$$

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

The following proposition states some properties of Galois dilation operators.

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

(i) *for $(\sigma,\beta)\in\mathrm{Gal}(\mathbb{F})\times\mathbb{F}$, we have $E_\sigma T_\beta=T_{\sigma\beta}E_\sigma$;*
(ii) *for $\sigma,\sigma'\in\mathrm{Gal}(\mathbb{F})$, we have $E_{\sigma\sigma'}=E_\sigma E_{\sigma'}$;*
(iii) *for $(\sigma,\beta),(\sigma',\beta')\in\mathrm{Gal}(\mathbb{F})\times\mathbb{F}$, we have $T_{\beta+\sigma\beta'}E_{\sigma\sigma'}=T_\beta E_\sigma T_{\beta'}E_{\sigma'}$.*

Proof. Let $\mathbb{F}$ be a finite field and $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then:

(i) for $(\sigma,\beta)\in\mathrm{Gal}(\mathbb{F})\times\mathbb{F}$ and $\tau\in\mathbb{F}$, we can write

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

(ii) For $\sigma,\sigma'\in\mathrm{Gal}(\mathbb{F})$ and $\tau\in\mathbb{F}$, we can write

$$E_{\sigma\sigma'}\mathbf{x}(\tau)=\mathbf{x}((\sigma\sigma')^{-1}\tau)=\mathbf{x}(\sigma'^{-1}\sigma^{-1}\tau)$$

$$= E_{\sigma'}\mathbf{x}(\sigma^{-1}\tau) = E_\sigma E_{\sigma'}\mathbf{x}(\tau).$$

(iii) It is straightforward from (i) and (ii). □

Next, we summarize analytic properties of Galois dilation operators.

Proposition 4.2. *Let $\mathbb{F}$ be a finite field and $\sigma \in \mathrm{Gal}(\mathbb{F})$. Then*:

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

Proof.

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

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

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

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

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

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

which implies $(E_\sigma\mathbf{x})^* = E_\sigma\mathbf{x}^*$.

(ii) Let $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$. Then, we can write

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

which implies that $E_\sigma:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ is unitary in $\|\cdot\|_2$-norm and also satisfies

$$(E_\sigma)^*=(E_\sigma)^{-1}=E_{\sigma^{-1}}.$$ □

In the remainder of this article, we use the explicit characterization of the character group given by (3.5). Using (3.5), 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*:

(i) *$M_\gamma:\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ is a unitary operator in $\|\cdot\|_2$-norm and satisfies $(M_\gamma)^*=(M_\gamma)^{-1}=M_{-\gamma}$;*
(ii) *for $\sigma\in\mathrm{Gal}(\mathbb{F})$, we have $E_\sigma M_\gamma=M_{\sigma^{-1}\gamma}E_\sigma$.*

Proof.

(i) It is straightforward, invoking the definition of modulation operators.

(ii) Let $\sigma\in\mathrm{Gal}(\mathbb{F})$. Let $\mathbf{x}\in\mathbb{C}^{\mathbb{F}}$ and $\tau\in\mathbb{F}$. Then, we can write

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

which implies that $E_\sigma M_\gamma=M_{\sigma^{-1}\gamma}E_\sigma$. □

For $\sigma \in \mathrm{Gal}(\mathbb{F})$, let $\widehat{E}_\sigma : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ be given by

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

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 E_σ instead of $\widehat{E}_\sigma$ at times.

Then, we can present some analytic aspects of Galois dilation operators on the frequency domain as follows.

Proposition 4.4. *Let $\mathbb{F}$ be a finite field of order q and $\sigma \in \mathrm{Gal}(\mathbb{F})$. Then*:

(i) *$E_\sigma : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ is a $*$-isometric isomorphism of the Banach $*$-algebra $\mathbb{C}^{\widehat{\mathbb{F}^+}}$;*
(ii) *$E_\sigma : \mathbb{C}^{\widehat{\mathbb{F}^+}} \to \mathbb{C}^{\widehat{\mathbb{F}^+}}$ is unitary in the $\|\cdot\|_2$-norm and satisfies $(E_\sigma)^* = (E_\sigma)^{-1} = E_{\sigma^{-1}}$.*
(iii) *$\mathcal{F}_\mathbb{F} E_\sigma = \widehat{E}_{\sigma^{-1}} \mathcal{F}_\mathbb{F}$.*

Proof. (i) and (ii) are straightforward.

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

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

Replacing τ with $\sigma\tau$, we achieve

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

which implies $\mathcal{F}_\mathbb{F}(E_\sigma \mathbf{x}) = \widehat{E}_{\sigma^{-1}}(\mathcal{F}_\mathbb{F}\mathbf{x})$. □

The underlying set $\mathrm{Gal}(\mathbb{F})\times\mathbb{F}$, equipped with group operations given by

$$(\sigma,\beta)\rtimes(\sigma',\beta'):=(\sigma\sigma',\beta+\sigma(\beta')) \tag{4.1}$$

$$(\sigma,\beta)^{-1}:=(\sigma^{-1},\sigma^{-1}(-\beta)) \tag{4.2}$$

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

The next theorem shows that the group structure of the Galois wavelet group $\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$ canonically determines a group representation.

Theorem 4.5. *Let $\mathbb{F}$ be a finite field of order $q>2$. Then*:

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

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

$$(\sigma,\beta)\longmapsto\rho(\sigma,\beta):=T_\beta E_\sigma \tag{4.3}$$

for

$$(\sigma,\beta)\in\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F},$$

is a group representation of the finite Galois wavelet group $\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$ *on the finite-dimensional Hilbert space $\mathbb{C}^{\mathbb{F}}$.*

Proof. Let $\mathbb{F}$ be a finite field of order $q>2$. Then:

(i) It is straightforward from the group structure given in (4.1) that $\mathbb{F}$ is a normal Abelian subgroup and $\mathrm{Gal}(\mathbb{F})$ is a non-normal Abelian subgroup of $\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$.

(ii) It is easy to check that $\rho(1,0)=I$, and $\rho(\sigma,\beta):\mathbb{C}^{\mathbb{F}}\to\mathbb{C}^{\mathbb{F}}$ is a unitary operator for all $(\sigma,\beta)\in\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$. Now, let $(\sigma,\beta),(\sigma',\beta')\in\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$. Then, using Proposition 4.1, we can write

$$T_{\beta+\sigma(\beta')}D_{\sigma\sigma'}=T_\beta T_{\sigma(\beta')}D_\sigma D_{\sigma'}=T_\beta D_\sigma T_{\beta'}D_{\sigma'}.$$

Thus, we get

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

which implies that ρ is a group representation of the finite wavelet group $\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$ on the finite-dimensional Hilbert space $\mathbb{C}^{\mathbb{F}}$. □

Remark 4.6. In terms of abstract wavelet transforms over locally compact groups, the representation ρ mentioned in Theorem 4.5 is precisely the quasi-regular representation generated by the action of the multiplicative group $H = \mathrm{Gal}(\mathbb{F})$ on the finite additive group $K = \mathbb{F}$ on the Hilbert space $\mathbb{C}^{\mathbb{F}}$, see **[1, 8]** and the references therein.

5. Galois wavelet transforms over finite fields. In this section, we present an 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 $W_{\mathbf{y}}\mathbf{x}:\mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}\to\mathbb{C}$, given by

$$W_{\mathbf{y}}\mathbf{x}(\sigma,\beta) := \sum_{\tau\in\mathbb{F}}\mathbf{x}(\tau)\overline{\mathbf{y}(\sigma^{-1}(\tau-\beta))}, \tag{5.1}$$

for all $(\sigma,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}$. 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 (5.1) and using inner product terms, we can write

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

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

$$\langle\mathbf{x},\rho(\sigma,\beta)\mathbf{y}\rangle = \langle\mathbf{x},T_\beta E_\sigma\mathbf{y}\rangle = \langle T_{-\beta}\mathbf{x},E_\sigma\mathbf{y}\rangle, \tag{5.2}$$

for

$$(\sigma,\beta)\in \mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}.$$

The next proposition gives us a Fourier (respectively, 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 $(\sigma,\beta)\in \mathrm{Gal}(\mathbb{F})\rtimes\mathbb{F}$. Then*:

(i) $W_{\mathbf{y}}\mathbf{x}(\sigma,\beta)=\sqrt{q}\mathcal{F}_q(\widehat{\mathbf{x}}\cdot\overline{\widehat{E_\sigma\mathbf{y}}})(-\beta)$.
(ii) $W_{\mathbf{y}}\mathbf{x}(\sigma,\beta)=\mathbf{x}*E_\sigma\mathbf{y}^*(\beta)$.

Proof. Let $\mathbf{x},\mathbf{y}\in\mathbb{C}^{\mathbb{F}}$ and $(\sigma,\beta)\in\mathbb{F}^*\rtimes\mathbb{F}$.

(i) Using the Plancherel formula, we have

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

(ii) Similarly, using the Plancherel formula, we can write

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

□

The following theorem presents a concrete formulation for the $\|\cdot\|_2$-norm of the Galois wavelet transform $\mathcal{W}_{\mathbf{y}}\mathbf{x}$.

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*

$$\|W_{\mathbf{y}}\mathbf{x}\|_2^2 = q\sum_{\gamma\in\mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2\Big). \tag{5.3}$$

Proof. Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a window function, $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$ and $\sigma \in \mathrm{Gal}(\mathbb{F})$. Using Proposition 5.1, we have

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

Therefore, we can write

$$\begin{aligned}&\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})}\sum_{\beta\in\mathbb{F}} |\langle \mathbf{x}, \rho(\sigma,\beta)\mathbf{y}\rangle|^2 \\ &= q\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})}\sum_{\gamma\in\mathbb{F}} \Big|\widehat{\mathbf{x}}(\chi_\gamma)\cdot\overline{\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)}\Big|^2 \\ &= q\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})}\sum_{\gamma\in\mathbb{F}} \Big|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot|\overline{\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)}\Big|^2 \\ &= q\sum_{\gamma\in\mathbb{F}}\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})} \Big|\widehat{\mathbf{x}}(\chi_\gamma)|^2\cdot|\overline{\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)}\Big|^2 \\ &= q\sum_{\gamma\in\mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})} |\overline{\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)}|^2\Big) \\ &= q\sum_{\gamma\in\mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in\mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2\Big).\end{aligned}$$

Then, we deduce that

$$\|W_{\mathbf{y}}\mathbf{x}\|_2^2 = q\sum_{\gamma\in\mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2\Big). \qquad \square$$

Let $\mathbb{F}$ be a finite field of order $q = p^d$. A nonzero window vector/signal $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ is called *Galois admissible* if and only if

$$|\widehat{\mathbf{y}}(k)|^2 = d^{-1} \cdot \sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{\mathbf{y}}(\chi_{\sigma(\gamma)})|^2, \tag{5.4}$$

for all $\gamma \in \mathbb{F} - \mathbb{Z}_p$ and $k \in \mathbb{Z}_p$.

Then, equivalently, $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ is Galois admissible if and only if

$$|\widehat{\mathbf{y}}(k)|^2 = d^{-1} \cdot \sum_{j=0}^{d-1} |\widehat{\mathbf{y}}(\chi_{\gamma^{p^j}})|^2, \tag{5.5}$$

for all $\gamma \in \mathbb{F} - \mathbb{Z}_p$ and $k \in \mathbb{Z}_p$.

In this case,

$$c_{\mathbf{y}} := d \cdot |\widehat{\mathbf{y}}(k)|^2 = \sum_{j=0}^{d-1} |\widehat{\mathbf{y}}(\gamma^{p^j})|^2,$$

is called a *Galois wavelet* constant of $\mathbf{y}$.

Theorem 5.3. *Let $\mathbb{F}$ be a finite field of order $q = p^d$. Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a Galois admissible window vector. Then, for $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$, we have*

$$\|W_{\mathbf{y}}\mathbf{x}\|_2^2 = q \cdot c_{\mathbf{y}} \cdot \|\mathbf{x}\|_2^2.$$

Proof. Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a Galois admissible window vector with the Galois wavelet constant $c_{\mathbf{y}}$. Also, let $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$. Then, using (5.3), we have

$$\begin{aligned}
\|W_{\mathbf{y}}\mathbf{x}\|_2^2 &= q \cdot \sum_{\gamma\in\mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2 \Big) \\
&= q \cdot \Big(\sum_{k\in\mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_k)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_k)|^2 \Big) \\
&\quad + \sum_{\gamma\in\mathbb{F}-\mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2 \Big) \Big) \\
&= q \cdot \Big(\sum_{k\in\mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_k)|^2 \cdot \Big(\sum_{\sigma\in \mathrm{Gal}(\mathbb{F})} |\widehat{\mathbf{y}}(\chi_{\sigma^{-1}(k)})|^2 \Big)
\end{aligned}$$

$$
\begin{aligned}
&\quad + \sum_{\gamma \in \mathbb{F} - \mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2 \right) \Bigg) \\
&= q \cdot \Bigg(\sum_{k \in \mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_k)|^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F})} |\widehat{\mathbf{y}}(\chi_k)|^2 \right) \\
&\quad + \sum_{\gamma \in \mathbb{F} - \mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2 \right) \Bigg) \\
&= q \cdot \Bigg(d \cdot \sum_{k \in \mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_k)|^2 |\widehat{\mathbf{y}}(\chi_k)|^2 \\
&\quad + \sum_{\gamma \in \mathbb{F} - \mathbb{Z}_p} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \cdot \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F})} |\widehat{E_\sigma \mathbf{y}}(\chi_\gamma)|^2 \right) \Bigg) \\
&= q \cdot c_{\mathbf{y}} \cdot \left(\sum_{\gamma \in \mathbb{F}} |\widehat{\mathbf{x}}(\chi_\gamma)|^2 \right) \\
&= q \cdot c_{\mathbf{y}} \cdot \|\widehat{\mathbf{x}}\|_2^2 = q \cdot c_{\mathbf{y}} \cdot \|\mathbf{x}\|_2^2. \qquad \square
\end{aligned}
$$

We then conclude with the following inversion formula.

Corollary 5.4. *Let $\mathbb{F}$ be a finite field of order $q = p^d$. Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a Galois admissible window vector. Then, each $\mathbf{x} \in \mathbb{C}^{\mathbb{F}}$ satisfies the following reconstruction formula:*

$$\mathbf{x}(\tau) = d^{-1} \cdot c_{\mathbf{y}}^{-1} \cdot \sum_{\sigma \in \mathrm{Gal}(\mathbb{F})} \sum_{\beta \in \mathbb{F}} W_{\mathbf{y}} \mathbf{x}(\sigma, \beta) T_\beta E_\sigma \mathbf{y}(\tau),$$

for all $\tau \in \mathbb{F}$.

The following theorem summarizes our recent results in terms of frame theory.

Theorem 5.5. *Let $\mathbb{F}$ be a finite field of order $q = p^d$. Let $\mathbf{y} \in \mathbb{C}^{\mathbb{F}}$ be a Galois admissible window vector. Then*

$$\left\{ T_\beta E_\sigma \mathbf{y} : (\sigma, \beta) \in \mathrm{Gal}(\mathbb{F}) \rtimes \mathbb{F} \right\},$$

constitutes a tight frame for $\mathbb{C}^{\mathbb{F}}$.

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

ENDNOTES

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

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** (2009), 541–552.

2. A. Arefijamaal and E. Zekaee, *Signal processing by alternate dual Gabor frames*, Appl. Comp. Harmon. Anal. **35** (2013), 535–540.

3. ———, *Image processing by alternate dual Gabor frames*, Bull. Iranian Math. Soc. **42** (2016), 1305–1314.

4. L. Cohen, *Time-frequency analysis*, Prentice-Hall, New York, 1995.

5. H.G. Feichtinger, W. Kozek and F. Luef, *Gabor analysis over finite Abelian groups*, Appl. Comp. Harmon. Anal. **26** (2009), 230–248.

6. K. Flornes, A. Grossmann, M. Holschneider and B. Torrésani, *Wavelets on discrete fields*, Appl. Comp. Harmon. Anal. **1** (1994), 137–146.

7. G.B. Folland, *A course in abstract harmonic analysis*, CRC Press, Boca Raton, 1995.

8. H. Führ, *Abstract harmonic analysis of continuous wavelet transforms*, Springer-Verlag, Berlin, 2005.

9. A. Ghaani Farashahi, *Cyclic wave packet transform on finite Abelian groups of prime order*, Int. J. Wavelets Multiresolut. Inf. Proc. **12** (2014), 1450041.

10. ———, *Wave packet transform over finite fields*, Electr. J. Lin. Alg. **30** (2015), 507–529.

11. ———, *Classical coherent state transforms over finite fields*, Inter. J. Math. Game Th. Alg. **25** (2016), 273–297.

12. ———, *Wave packet transforms over finite cyclic groups*, Lin. Alg. Appl. **489** (2016), 75–92.

13. ———, *Theoretical frame properties of wave-packet matrices over prime fields*, Lin. Multilin. Alg. **65** (2017), 2508–2529.

14. ———, *Structure of finite wavelet frames over prime fields*, Bull. Iranian Math. Soc. **43** (2017), 109–120.

15. G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, New York, 1979.

16. C.P. Johnston, *On the pseudodilation representations of Flornes, Grossmann, Holschneider, and Torrésani*, J. Fourier Anal. Appl. **3** (1997), 377–385.

17. J.B. Lima and R.M. Campello de Souza, *Fractional cosine and sine transforms over finite fields*, Lin. Alg. Appl. **438** (2013), 3217–3230.

18. R.J. McEliece, *Finite fields for computer scientists and engineers*, Springer Inter. Eng. Comp. Sci. (1987).

19. G.L. Mullen and D. Panario, *Handbook of finite fields*, Discr. Math. Appl., Chapman and Hall/CRC, 2013.

20. G. Pfander, *Gabor frames in finite dimensions, Finite frames, theory and applications*, in *Finite frames, Applied and numerical harmonic analysis*, Birkhauser, Boston, 2013.

21. O. Pretzel, *Error-correcting codes and finite fields*, Oxford Appl. Math. Comp. Sci. (1996).

22. D. Ramakrishnan and R.J. Valenza, *Fourier analysis on number fields*, Springer-Verlag, New York, 1999.

23. R. Reiter and J.D. Stegeman, *Classical harmonic analysis*, Oxford University Press, New York, 2000.

24. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, 1994.

25. A. Vourdas, *Harmonic analysis on a Galois field and its subfields*, J. Fourier Anal. Appl. **14** (2008), 102–123.

Johns Hopkins University, Whiting School of Engineering, Laboratory for Computational Sensing and Robotics (LCSR), Baltimore, MD 21218
Email address: arash.ghaanifarashahi@jhu.edu, ghaanifarashahi@outlook.com