Appl. Comput. Harmon. Anal. 55 (2021) 270–281

Contents lists available at ScienceDirect

Applied and Computational Harmonic Analysis

www.elsevier.com/locate/acha

On the construction of discrete orthonormal Gabor bases on finite dimensional spaces

Weiqi Zhou [1]

School of Mathematics and Statistics, Xuzhou University of Technology, Lishui Road 2, Yunlong District, Xuzhou, Jiangsu Province, 221111, China

ARTICLE INFO

Article history:
Received 1 August 2020
Received in revised form 26 May 2021
Accepted 3 June 2021
Available online 7 June 2021
Communicated by Bruno Torresani

MSC:
42C15
15B10
43A65

Keywords:
Discrete Gabor analysis
Orthonormal Gabor matrix
Discrete time-frequency analysis

ABSTRACT

We show that orthonormality of a discrete Gabor bases on $\mathbb{C}^n$ hinges heavily on the following pattern of its support set $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$: (i) Γ is itself a subgroup of order n, or (ii) Γ is the quotient of such a subgroup, i.e., there exists an order n subgroup $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ such that Γ takes precisely one element from each coset of H (i.e., $\mathbb{Z}_n \times \mathbb{Z}_n = H \times \Gamma$). If n is a prime number, then Γ satisfying (i) automatically implies that it satisfies (ii), and the condition is both sufficient and necessary. If n is a composite number, then (i) and (ii) do not necessarily imply each other, and the condition is sufficient (whether it is also necessary is unknown yet). Main contributions of this article are (a) necessity of the condition for prime n; (b) sufficiency of (i) for composite n; (c) the characterization that if Γ is an order n subgroup, then its corresponding discrete time-frequency shifts mutually commute.

1. Introduction

Gabor frames [1] are indispensable tools in modern time-frequency analysis. They are commonly used in science and engineering to decompose signals into localized building blocks on the time-frequency plane (see, e.g., [8,10,14–16,20]). Discrete Gabor systems are counterparts of Gabor frames on finite dimensional spaces, their rich structure has also attracted persistent research interest ever since their emergence (e.g., see [5–7,17,19]).

To understand the goal of this short note, let us first introduce relevant notions. On $\mathbb{C}^n$, define the discrete translation T and discrete modulation M to be

E-mail address: zwq@xzit.edu.cn.

[1] Part of this research (Theorem 1) was supported by the *Deutsche Forschungsgemeinschaft* (DFG) project 111001434 when the author resided in Germany.

https://doi.org/10.1016/j.acha.2021.06.001
1063-5203/

$$T = \begin{pmatrix} 0 & & & & 1 \\ 1 & \ddots & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}, \quad M = \begin{pmatrix} 1 & & & & \\ & \omega & & & \\ & & \ddots & & \\ & & & \omega^{n-2} & \\ & & & & \omega^{n-1} \end{pmatrix},$$

where $\omega = e^{\frac{2\pi i}{n}}$ is a primitive n-th root of unity. In particular, T acts on $\mathbb{C}^n$ as the circulant permutation $(x_1, x_2, \ldots, x_n)^T \mapsto (x_n, x_1, x_2 \ldots x_{n-1})^T$.

Discrete time frequency shifts are related through the discrete Fourier transform as

$$T = WM^*W^* = W^*MW, \tag{1}$$

where $*$ denotes the adjoint operation, and W with $W_{ij} = \omega^{(i-1)(j-1)}/\sqrt{n}$ is the Fourier matrix.

Just like their continuous counterparts, discrete time-frequency shifts also commute up to a phase factor ω:

$$MT = \omega TM, \tag{2}$$

and $\{\omega, M, T\}$ together under multiplication generates a representation of the finite Heisenberg group, see e.g., [9,12].

In various literature it is also customary to adopt following notations:

$$\pi(j,k) = M^j T^k,$$

and

$$\pi(H) = \{\pi(j,k) : \quad (j,k) \in H \subseteq \mathbb{Z}_n \times \mathbb{Z}_n\},$$

where $\mathbb{Z}_n$ is the additive cyclic group of n elements. It is easy to verify using (2) that $\pi(j,k)$ commutes with $\pi(j',k')$ if and only if

$$kj' \equiv jk' \mod n. \tag{3}$$

It is also worth mentioning that π is not a group homomorphism, thus $\pi(H)$ is not necessarily a group even if H is. For example, take H as the cyclic subgroup generated by $(1,1)$, then $\pi(1,1) = MT$, while its inverse $T^{-1}M^{-1} = \omega^{-1}M^{-1}T^{-1}$ is not in $\pi(H)$.

We also introduce the notation $\pi^*(j,k)$ to denote the adjoint of $\pi(j,k)$, i.e.,

$$\pi^*(j,k) = T^{-k}M^{-j},$$

It follows immediately from (2) that

$$\pi(j',k')\pi(j,k) = \omega^{-jk'}\pi(j+j',k+k'), \tag{4}$$

and

$$\pi^*(j,k)\pi^*(j',k') = \omega^{jk'}\pi^*(j+j',k+k'). \tag{5}$$

A discrete Gabor system $(\Gamma, \vec{c})$ on $\mathbb{C}^n$ takes the form

$$(\Gamma, \vec{c}) = \{\pi(j,k)\vec{c}: \quad (j,k) \in \Gamma \subseteq \mathbb{Z}_n \times \mathbb{Z}_n,\ \vec{c} \in \mathbb{C}^n\}.$$

Here $\vec{c} \in \mathbb{C}^n$ is the window vector, $\Gamma \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ is the support of this system. It is called a Gabor matrix if written into the matrix form with $\pi(j,k)\vec{c}$ being its column vectors. The corresponding Gabor matrix is denoted as $G_\Gamma(\vec{c})$, the ordering of columns does not matter in this article.

$(\Gamma, \vec{c})$ is said to be a discrete Gabor frame if it forms a frame for $\mathbb{C}^n$, similarly it is called a discrete Gabor basis if it forms a basis for $\mathbb{C}^n$, two trivial examples of Gabor bases are

(i) $\big(\{0\} \times \mathbb{Z}_n, (1, 0, \dots, 0)^T\big)$. This consists of all circulant shifts on $(1, 0, \dots, 0)^T$ and is the usual Euclidean basis;
(ii) $\Big(\mathbb{Z}_n \times \{0\}, \frac{1}{\sqrt{n}}(1, 1, \dots, 1)^T\Big)$. This consists of all modulations on $\frac{1}{\sqrt{n}}(1, 1, \dots, 1)^T$ and is the Fourier basis, i.e., columns in the Fourier matrix.

And both of them are orthonormal bases on $\mathbb{C}^n$.

The purpose of this article is to establish following two relations:

Assertion 1 *(for prime numbers). If n is a prime number and $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$, then there exists $\vec{c} \in \mathbb{C}^n$ such that $(\Gamma, \vec{c})$ is an orthonormal basis for $\mathbb{C}^n$ if and only if there is a proper (and non-trivial) subgroup $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ so that Γ takes precisely one element from each coset of H, i.e., $|\Gamma| = n$ and*

$$\Gamma \times H = \mathbb{Z}_n \times \mathbb{Z}_n.$$

Assertion 2 *(for composite numbers). If $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$ satisfies one of the following two conditions:*

(I) $\Gamma \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is itself a subgroup of order n,
(II) there exists an order n subgroup $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ such that Γ takes precisely one element from each coset of H, i.e.,

$$\Gamma \times H = \mathbb{Z}_n \times \mathbb{Z}_n,$$

then one can find $\vec{c} \in \mathbb{C}^n$ such that $(\Gamma, \vec{c})$ is an orthonormal basis for $\mathbb{C}^n$.

If n is a prime number then Γ satisfying (I) in Assertion 2 automatically implies that it also satisfies (II). Indeed, in this case, any proper (and non-trivial) subgroups is cyclic, and takes one of the following form (by Sylow theorems):

$$H_s = \begin{cases} \{(ks, k)\}_{k \in \mathbb{Z}_n}, & s = 1, 2, \dots n-1, \\ \{(0, k)\}_{k \in \mathbb{Z}_n}, & s = 0, \\ \{(j, 0)\}_{j \in \mathbb{Z}_n}, & s = \infty, \end{cases} \tag{6}$$

they pairwise intersect trivially and jointly cover the whole group. Moreover, $\mathbb{Z}_n \times \mathbb{Z}_n = H_s \times H_0 = H_s \times H_\infty$ $(s = 1, 2, \dots, p-1)$ holds (i.e., if Γ is a proper and non-trivial subgroup, then it is at the same time also the quotient of another such subgroup), thus (I) is contained in (II) for prime n. There is also a geometric interpretation for (II), see the appendix.

Our result is novel in the following three aspects:

(i) The necessity of the condition in Assertion 1 has not been shown before;

(ii) The sufficiency of (I) in Assertion 2 is unknown before;
(iii) The sufficiency of (II) in Assertion 2 is partially known before (e.g., see [9]), but to the author's knowledge, previously H was only stated as a subgroup such that members in $\pi(H)$ mutually commute. We are now providing a better and clearer characterization that all subgroups of order n have this property.

We also give an explicit example of Γ (when n is a composite number) that satisfies (I) in Assertion 2 but not (II), which shows that these two conditions can not be combined as in Assertion 1, and produce the corresponding window vector $\vec{c}$ and unitary Gabor matrix $G_\Gamma(\vec{c})$.

2. Preliminaries

If $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup, and members in $\pi(H)$ mutually commute with each other, then H is called an isotropy subgroup in some literature (see e.g., [9] for relevant backgrounds from physics with respect to this name). This type of subgroups plays a central role in discrete time-frequency analysis, trivial examples of such subgroups (apply (3) to verify) include cyclic subgroups and lattice subgroups generated by $(a, 0)$ and $(0, b)$ where $ab = n$ (only exists if n is composite). It may not be immediately clear that actually all subgroups of order n have such a property, which is a simple consequence of [18, Theorem 1]:

Proposition 1. *If $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup of order n, then members in $\pi(H)$ mutually commute.*

Proof. A subgroup in $\mathbb{Z}_n \times \mathbb{Z}_n$ can be identified and visualized in the plane with sublattices of the lattice $\mathbb{Z}_n \times \mathbb{Z}_n$ ($1d$ lattice for cyclic subgroups and $2d$ lattice for other cases, see [18]). [18, Theorem 1] shows that if $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup of order n, then it can be generated by $(a, 0)$ and (s, b) with

$$ab = n, \quad s = \frac{ta}{\gcd(a, \frac{n}{b})}, \quad 0 \le t \le \gcd(a, \frac{n}{b}) - 1$$

for properly chosen a, b, t. It is cyclic if and only if

$$\gcd(\frac{n}{a}, \frac{n}{b}, \frac{ns}{ab}) = 1.$$

Consequently any two elements from $\pi(H)$ satisfy (3) and thus commute. □

Equip the matrix space $\mathbb{C}^{n\times n}$ with the inner product

$$\langle A, B\rangle = \operatorname{tr}(AB^*),$$

where tr is the trace. We provide a simpler proof for the following property repeated from [17]:

Proposition 2. *[17, Proposition 6.1 and Equation (6.7)]*

(i) $\frac{1}{\sqrt{n}}\pi(\mathbb{Z}_n \times \mathbb{Z}_n)$ is an orthonormal basis for $\mathbb{C}^{n\times n}$.
(ii) If $\{A_k\}_{k=1}^{n^2}$ is an orthonormal basis for $\mathbb{C}^{n\times n}$, then for any $\vec{c} \in \mathbb{C}^n$, $\{A_k\vec{c}\}_{k=1}^{n^2}$ is always a tight frame for $\mathbb{C}^n$ with frame constant $\|\vec{c}\|^2$. In particular, the full discrete Gabor system $(\mathbb{Z}_n \times \mathbb{Z}_n, \vec{c})$ is a tight frame with frame constant $n\|\vec{c}\|^2$.

Proof. (i) can be easily verified by direct computation. For (ii), take any $\vec{x} \in \mathbb{C}^n$, if $\{A_k\}_{k=1}^{n^2}$ is an orthonormal basis for $\mathbb{C}^{n\times n}$, then we have

$$\sum_{k=1}^{n^2} |\langle \vec{x}, A_k \vec{c}\rangle|^2 = \sum_{k=1}^{n^2} |\operatorname{tr}(\vec{x}\vec{c}^{\,*} A_k^*)|^2 = \sum_{k=1}^{n^2} |\langle \vec{x}\vec{c}^{\,*}, A_k\rangle|^2 = \|\vec{c}\|^2 \|\vec{x}\|^2,$$

which shows that it is a tight frame for $\mathbb{C}^n$ with frame constant $\|\vec{c}\|^2$. The rest follows from (i). □

For a vector $\vec{x} = (x_1, x_2, \dots, x_n)^T \in \mathbb{C}^n$, denote

$$P_{\vec{x}} = \vec{x}\vec{x}^*, \quad D_{\vec{x}} = \operatorname{diag}(x_1, x_2, \dots, x_n),$$

i.e., $P_{\vec{x}}$ is the (scaled) one dimensional projector onto the span of $\vec{x}$, and $D_{\vec{x}}$ is the diagonal matrix with elements in $\vec{x}$ lying on its main diagonal.

Denote $\circ$ as the matrix Hadamard product (i.e., $A \circ B = [A_{ij}B_{ij}]_{ij}$). For $j = 0, 1, \dots, n-1$, let $\vec{w}_j$ be the $(j+1)$-th column in the scaled Fourier matrix $\sqrt{n}W$, i.e.,

$$\vec{w}_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})^T.$$

For an arbitrary matrix $A \in \mathbb{C}^{n\times n}$, it is easy to verify (alternatively see [4, Chapter 5]) that

$$\pi(j,0)A\pi^*(j,0) = A \circ P_{\vec{w}_j}. \tag{7}$$

One may also check that if n is an odd prime, then eigenvectors of H_s (for $s = 0, 1, 2, \dots, n-1$) are columns in D^sW, where D is a diagonal matrix with the m-th entry on its main diagonal being $\omega^{m(m-1)/2}$. These eigenvectors are also examples of bi-unimodular sequences and CAZAC (constant amplitude zero auto correlation) sequences, as well as mutually unbiased bases, and are connected to so called cyclic n-roots. See e.g., [3,11,13]. We omit concrete formulas for other cases here since they are not directly related to our topic. In this article we only need the fact that discrete time-frequency shifts are diagonalizable by unitary matrices (In particular, they are unitary row scalings applied to the Fourier matrix).

Next, we establish the sufficiency of (II) for all n as Proposition 3 below, this result is already shown in [9], but the proof we are giving here is relatively more elementary, and it relies on two technical lemmas:

Lemma 1. *Let $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ be a subgroup of order n, let V be an eigenmatrix that simultaneously diagonalizes members of $\pi(H)$. If $\vec{v}$ is a column in V, then*

(i) $P_{\vec{v}} \in \operatorname{span}(\pi(H))$.
(ii) *If $(a,b) \notin H$, then $P_{\vec{v}} \perp \pi(a,b)$.*

Proof. Suppose members in $\pi(H)$ are diagonalized as $VD_{\vec{a}_1}V^*, VD_{\vec{a}_2}V^*, \dots, VD_{\vec{a}_n}V^*$ where without loss of generality we may arrange V properly so that $\vec{v}$ is the first column of V, then a linear combination will result in

$$x_1VD_{\vec{a}_1}V^* + x_2VD_{\vec{a}_2}V^* + \ldots + x_nVD_{\vec{a}_n}V^* = VD_{\vec{y}}V^*,$$

where

$$\vec{y} = x_1\vec{a}_1 + x_2\vec{a}_2 + \ldots + x_n\vec{a}_n.$$

Recall from Proposition 2 that $\pi(\mathbb{Z}_n \times \mathbb{Z}_n)$ forms a basis for $\mathbb{C}^{n\times n}$, thus members in $\pi(H)$ must be linearly independent, which from the above equation implies that $\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n$ must also be linearly independent. Consequently there exist coefficients $x_1, x_2, \dots, x_n$ that yields $\vec{y} = (1, 0, \dots, 0)$, which is also the linear combination that gives $P_{\vec{v}}$. This establishes (i).

If $(a,b) \notin H$, then again by Proposition 2, $\pi(a,b) \perp \pi(H)$, hence by (i) it is also perpendicular to $P_{\vec{v}}$, and (ii) follows. $\square$

If n is a prime number, then the following lemma is just a trivial statement following from the orbit-stabilizer theorem. If n is a composite number, then it is not immediate that H is (instead of being a subgroup of) the stabilizer subgroup for $\vec{v}$. We thus provide a quick proof:

Lemma 2. *Let $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ be a subgroup of order n, let V be an eigenmatrix that simultaneously diagonalizes members of $\pi(H)$. If $\vec{v}$ is a column in V, then each coset of H uniquely maps $\vec{v}$ to a distinct column (up to the difference of a unit phase factor $e^{i\theta}$ for some θ) in V.*

Proof. Let $(j,k) \in H$ be arbitrary, and denote the eigenvalue of $\pi(j,k)$ for $\vec{v}$ as λ (obviously $|\lambda| = 1$ since $\pi(j,k)$ is unitary), then for any $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ we have

$$\pi(j,k)\pi(a,b)\vec{v} = \omega^{jb-ka}\pi(a,b)\pi(j,k)\vec{v} = \lambda\, \omega^{jb-ka}\pi(a,b)\vec{v},$$

which shows $\pi(a,b)\vec{v}$ is also a shared unit eigenvector for members of $\pi(H)$. Now if (a,b) and (a',b') belong to different cosets of H, i.e., $(a-a', b-b') \notin H$, then we have

$$|\langle \pi(a,b)\vec{v}, \pi(a',b')\vec{v}\rangle| = |\langle \pi(a-a', b-b')\vec{v}, \vec{v}\rangle| = |\langle \pi(a-a', b-b'), P_{\vec{v}}\rangle| = 0,$$

where the last equality follows from Lemma 1. This orthogonality shows their distinctness. $\square$

Proposition 3 *(Sufficiency of (II) in Assertion 2, [9]). Let $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ be a subgroup of order n, if Γ consists of precisely one element from each coset of H, i.e., $|\Gamma| = n$ and*

$$\mathbb{Z}_n \times \mathbb{Z}_n = \Gamma \times H,$$

then there exists $\vec{c} \in \mathbb{C}^n$ such that $(\Gamma, \vec{c})$ forms an orthonormal basis for $\mathbb{C}^n$.

Proof. Let V be an eigenmatrix that simultaneously diagonalizes members of $\pi(H)$, it suffices to take an arbitrary column in V as the window vector $\vec{c}$, then by Lemma 2, $G_\Gamma(\vec{c})$ differs from V by at most a column permutation and a unitary column scaling, consequently it is also unitary, thus $(\Gamma, \vec{c})$ is an orthonormal basis for $\mathbb{C}^n$. $\square$

Now Define the difference set $\Delta\Gamma$ of Γ to be

$$\Delta\Gamma = \{(j-j', k-k') : \quad (j,k), (j',k') \in \Gamma, (j,k) \neq (j',k')\},$$

if $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup, then clearly $(j-j', k-k') \in H$ if and only if they lie in the same coset of H, therefore if $|\Gamma| = n$, then

$$\Delta\Gamma \cap H = \emptyset \quad \Leftrightarrow \quad \mathbb{Z}_n \times \mathbb{Z}_n = \Gamma \times H. \tag{8}$$

Lemma 3. *Take $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$ with $|\Gamma| = n$ and $\vec{c} \in \mathbb{C}^n$ with unit norm, then*

$$(\Gamma, \vec{c}) \textit{ is orthonormal} \quad \Leftrightarrow \quad P_{\vec{c}} \perp \pi(\Delta\Gamma).$$

Proof. Observe that the inner product of any two distint vectors $\pi(j,k)\vec{c}$ and $\pi(j',k')\vec{c}$ in $(\Gamma,\vec{c})$ is of form $\omega^h\langle\pi(j-j',k-k')\vec{c},\vec{c}\rangle$ where h can be computed using (3). Therefore $(\Gamma,\vec{c})$ is orthonormal if and only if

$$0=|\omega^h\langle\pi(j-j',k-k')\vec{c},\vec{c}\rangle|=|\,\mathrm{tr}\,(\pi(j-j',k-k')P_{\vec{c}})\,|=|\langle\pi(j-j',k-k'),P_{\vec{c}}\rangle|,$$

i.e., $P_{\vec{c}}\perp\pi(\Delta\Gamma)$. □

3. The case of prime numbers

Lemma 4. *Let p be a prime number, $\vec{c}\in\mathbb{C}^p$ and $\Gamma\subset\mathbb{Z}_p\times\mathbb{Z}_p$ with $|\Gamma|=p$. For any proper (and non-trivial) subgroup $H_s\lhd\mathbb{Z}_n\times\mathbb{Z}_n$, if $(\Gamma,\vec{c})$ is an orthonormal basis for $\mathbb{C}^p$, but $\Delta\Gamma\cap H_s\neq\emptyset$, then $(H_s,\vec{c})$ is also an orthonormal basis for $\mathbb{C}^p$.*

Proof. Recall the form of H_s from (6), to make our discussion easier we shall first look at $s=0,1,2\dots,p-1$.

Denote elements in Γ as $(j_1,k_1),(j_2,k_2),\dots,(j_p,k_p)$, and consider the concatenated matrix

$$G=\left[\quad G_{(j_1,k_1)+H_s}(\vec{c})\quad\middle|\quad G_{(j_2,k_2)+H_s}(\vec{c})\quad\middle|\quad\dots\quad\middle|\quad G_{(j_p,k_p)+H_s}(\vec{c})\quad\right].$$

Rearranging columns in G we will get the following concatenated matrix

$$\left[\quad G_{(s,1)+\Gamma}(\vec{c})\quad\middle|\quad G_{(2s,2)+\Gamma}(\vec{c})\quad\middle|\quad\dots\quad\middle|\quad G_{(ps,p)+\Gamma}(\vec{c})\quad\right].$$

After a unitary column scaling due to (4) it can be further written as

$$\left[\quad \pi(s,1)G_\Gamma(\vec{c})\quad\middle|\quad \pi(2s,2)G_\Gamma(\vec{c})\quad\middle|\quad\dots\quad\middle|\quad \pi(ps,p)G_\Gamma(\vec{c})\quad\right].$$

Each $\pi(ks,k)$ is unitary, and by our assumption $G_\Gamma(\vec{c})$ is also unitary, hence the above is just p unitary matrices concatenated together. Therefore

$$GG^*=pI,$$

where $I\in\mathbb{C}^{p\times p}$ is the identity matrix.

On the other hand, $(j_i,k_i)+H_s$ is a coset of H_s, recall that such a representation of a coset is not unique, in particular, for each $i=1,2,\dots,p$, there exists an a_i so that

$$(j_i,k_i)+H_s=(a_i,0)+H_s, \tag{9}$$

since one may verify that

$$\mathbb{Z}_p\times\mathbb{Z}_p=H_s\times H_\infty,\quad s=0,1,2,\dots,p-1,$$

also holds. Consequently we may rewrite G as

$$G=\left[\quad G_{(a_1,0)+H_s}(\vec{c})\quad\middle|\quad G_{(a_2,0)+H_s}(\vec{c})\quad\middle|\quad\dots\quad\middle|\quad G_{(a_p,0)+H_s}(\vec{c})\quad\right].$$

If we denote

$$A_s=G_{H_s}(\vec{c})G^*_{H_s}(\vec{c}),$$

and combine all above equations together, then we get

$$pI = GG^* = \sum_{i=1}^{p} \pi(a_i, 0) A_s \pi^*(a_i, 0) = A_s \circ (\sum_{i=1}^{p} P_{\vec{w}_{a_i}}), \tag{10}$$

where the last equality follows from (7).

Now let us inspect the part $\sum_{i=1}^{p} P_{\vec{w}_{a_i}}$. Obviously its main diagonal is pI, thus comparing both sides of (10) we conclude that the main diagonal of A_s must be I; Each off diagonal element in $\sum_{i=1}^{p} P_{\vec{w}_{a_i}}$ is a polynomial of ω with non-negative integer coefficients, i.e., they are of form

$$c_0 + c_1\omega + \ldots + c_{p-1}\omega^{p-1},$$

with

$$c_0, c_1, \ldots, c_{p-1} \in \mathbb{N} \cup \{0\}, \quad c_0 + c_1 + \ldots + c_{p-1} = p. \tag{11}$$

Recall the assumption that $\Gamma \cap H_s \neq \emptyset$, i.e., Γ does not consist of precisely one element from each coset of H_s, having duplication simply means that there exist some distinct i, j with $\vec{w}_{a_i} = \vec{w}_{a_j}$, i.e., at least one of $c_0, c_1, \ldots, c_{p-1}$ is 0. But for a prime number p, the minimum polynomial of ω over $\mathbb{Q}$ is the p-th cyclotomic polynomial $1 + \omega + \ldots + \omega^{p-1}$ (see e.g. [2, p.299]), therefore the only set of coefficients that produces $c_0 + c_1\omega + \ldots + c_{p-1}\omega^{p-1} = 0$ while satisfying (11) is $c_0 = c_1 = \ldots = c_{p-1} = 1$. Consequently off diagonal elements in $\sum_{i=1}^{p} P_{\vec{w}_{a_i}}$ can not be 0. It then requires all off diagonal elements in A_s to be 0 for (10) to hold.

Together we obtain that $A_s = I$, i.e., $G_{H_s}(\vec{c})$ is unitary, and thus $(H_s, \vec{c})$ is an orthonormal basis for $\mathbb{C}^p$.

The case $s = \infty$ is essentially proved in the same way as above, we repeat all steps till (9), which we now replace with

$$(j_i, k_i) + H_\infty = (0, b_i) + H_\infty,$$

then (10) becomes

$$pI = \sum_{i=1}^{p} \pi(0, b_i) A_\infty \pi^*(0, b_i),$$

where A_∞ is defined in the same way, i.e., $A_\infty = G_{H_\infty}(\vec{c}) G^*_{H_\infty}(\vec{c})$.

Applying (1) to diagonalize $\pi(0, b_i)$ and $\pi^*(0, b_i)$, and conjugating both sides by W simultaneously we get

$$pI = \sum_{i=1}^{p} \pi(b_i, 0) W A_\infty W^* \pi^*(b_i, 0),$$

which again brings us back to the same form as in (10), thus with same arguments we can conclude that $WA_\infty W^* = I$, i.e., $A_\infty = I$, which further implies that $G_{H_\infty}(\vec{c})$ is unitary, and thus $(H_\infty, \vec{c})$ is also an orthonormal basis for $\mathbb{C}^p$. □

Theorem 1. *Let p be a prime number and $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$, then there exists $\vec{c} \in \mathbb{C}^p$ such that $(\Gamma, \vec{c})$ forms an orthonormal basis for $\mathbb{C}^p$ if and only if there is a proper (and non-trivial) subgroup $H_s \lhd \mathbb{Z}_n \times \mathbb{Z}_n$, so that Γ consists of precisely one element from each coset of H_s, i.e., $|\Gamma| = n$ and*

$$\mathbb{Z}_n \times \mathbb{Z}_n = \Gamma \times H_s.$$

Proof. As argued, the sufficiency follows from Proposition 3. For the necessity, assume the contrary that $(\Gamma, \vec{c})$ is an orthonormal basis for $\mathbb{C}^p$, but there is no proper and non-trivial subgroup H_s that satisfies the condition $\mathbb{Z}_p \times \mathbb{Z}_p = \Gamma \times H_s$. By (8), this means

$$\Delta\Gamma \cap H_s \neq \emptyset,$$

for all H_s. Then by Lemma 4, this implies $(H_s, \vec{c})$ is also an orthonormal basis for $\mathbb{C}^p$, consequently by Lemma 3 we obtain

$$P_{\vec{c}} \perp \pi(\Delta H_s),$$

and this holds for all s. Now since H_s is a group, its difference set is simply

$$\Delta H_s = H_s \setminus \{(0,0)\}.$$

Recall that since p is a prime number, H_s for $s = 0, 1, \ldots, p, \infty$ intersect trivially and jointly cover the whole group, therefore

$$\bigcup_s \Delta H_s = \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0,0)\},$$

and thus

$$P_{\vec{c}} \perp \pi\left(\mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0,0)\}\right).$$

Now by Proposition 2, $\pi(\mathbb{Z}_p \times \mathbb{Z}_p)$ is an orthogonal basis for the matrix space $\mathbb{C}^{p\times p}$, which left us with

$$P_{\vec{c}} \in \operatorname{span}\left(\pi(0,0)\right),$$

i.e., it is a constant multiple of the identity matrix I, but

$$\operatorname{rank}(P_{\vec{c}}) = 1 \neq p = \operatorname{rank}(I),$$

which is a contradiction. □

4. The case of composite numbers

Lemma 5. *If $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup of order n, and P_H is the average of simultaneous conjugations by members in $\pi(H)$, i.e.,*

$$P_H(A) = \frac{1}{n} \sum_{(j,k)\in H} \pi(j,k) A \pi^*(j,k), \quad A \in \mathbb{C}^n,$$

then P_H is the orthogonal projection of A onto the span of $\pi(H)$.

Proof. For any two $(j,k), (j',k') \in H$, we have by (4), (5) that

$$\pi(j',k')\pi(j,k)A\pi^*(j,k)\pi^*(j',k') = \pi(j+j',k+k')A\pi^*(j+j',k+k'),$$

consequently since H is a group we obtain

$$P_H^2(A) = \frac{1}{n^2} \sum_{(j',k'),(j,k)\in H} \pi(j+j', k+k') A \pi^*(j+j', k+k') = \frac{1}{n} \sum_{(j,k)\in H} \pi(j,k) A \pi^*(j,k) = P_H(A),$$

which shows it is a projection.

Now for any $(j,k) \in H$, the fact that it commutes with any member in $\pi(H)$ implies that

$$P_H(A)\pi^*(j,k) = P_H\left(A\pi^*(j,k)\right),$$

while the cyclic invariance of the trace shows that

$$\operatorname{tr}\left(P_H\left(A\pi^*(j,k)\right)\right) = \operatorname{tr}\left(A\pi^*(j,k)\right),$$

i.e., the range of $I - P_H$ (I is the identity operator) is orthogonal to the range of P_H since

$$\operatorname{tr}\left((A - P_H(A))\pi^*(j,k)\right) = 0,$$

which shows the orthogonality of P_H. □

The following commutativity relation is established for lattice subgroups generated by $(a,0)$ and $(0,b)$ with $ab = n$ in [17, Proposition 6.2], using Proposition 1 and Lemma 5 we can generalize it to all order n subgroups:

Corollary 1. *If $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a subgroup of order n, then the frame operator of $(H, \vec{c})$ commutes with $\pi(j,k)$ for any $(j,k) \in H$.*

Proof. The frame operator is $G_H(\vec{c})G_H^*(\vec{c})$, which can also be written as $nP_H(P_{\vec{c}})$, then by Lemma 5, it is a linear combination of members in $\pi(H)$, thus of course commutes with $\pi(j,k)$ for any $(j,k) \in H$ since by Proposition 1 members in $\pi(H)$ mutually commute. □

Theorem 2. *If $\Gamma \subset \mathbb{Z}_n \times \mathbb{Z}_n$ satisfies one of the following two conditions:*

(I) $\Gamma \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is itself a subgroup of order n,
(II) there exists an order n subgroup $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ such that Γ takes precisely one element from each coset of H, i.e.,

$$\Gamma \times H = \mathbb{Z}_n \times \mathbb{Z}_n,$$

then one can find $\vec{c} \in \mathbb{C}^n$ such that $(\Gamma, \vec{c})$ is an orthonormal basis on $\mathbb{C}^n$.

Proof. (II) is simply Proposition 3, thus it suffices to consider only (I).

If Γ is a subgroup of order n, then we take some $\vec{d} \in \mathbb{C}^n$ such that $G_\Gamma(\vec{d})$ is non-singular. The main result of [19] indicates that such $\vec{d}$ not only exists but also forms an open dense subset of $\mathbb{C}^n$. Denote $S = G_\Gamma(\vec{d})G_\Gamma^*(\vec{d})$ as the frame operator of $(\Gamma, \vec{d})$, it is easy to verify that the matrix $S^{-\frac{1}{2}}G_\Gamma(\vec{d})$ is unitary (i.e., the polar decomposition). By Corollary 1, S commutes with $\pi(j,k)$ for any $(j,k) \in \Gamma$, thus

$$S^{-\frac{1}{2}}G_\Gamma(\vec{d}) = G_\Gamma(S^{-\frac{1}{2}}\vec{d}),$$

i.e., $(\Gamma, S^{-\frac{1}{2}}\vec{d})$ is an orthonormal basis on $\mathbb{C}^n$. □

Below is a simple example in which Γ satisfies (I) but not (II):

Take $n = 4$, and $\Gamma = \{(0,0),(2,0),(0,2),(2,2)\} \lhd \mathbb{Z}_4 \times \mathbb{Z}_4$, i.e., Γ is isomorphic to the Klein four group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Clearly for any subgroup $H \lhd \mathbb{Z}_4 \times \mathbb{Z}_4$, we always have $\mathbb{Z}_2 \times \mathbb{Z}_2 \times H \neq \mathbb{Z}_4 \times \mathbb{Z}_4$, otherwise it would contradict the fundamental theorem of finite Abelian groups. This shows Γ satisfies (I) but not (II). An explicit choice of the window vector in this case is $\vec{c} = (1,1,0,0)^T/\sqrt{2}$, so that

$$G_\Gamma(\vec{c}) = (\vec{c}, \pi(2,0)\vec{c}, \pi(0,2)\vec{c}, \pi(2,2)\vec{c}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix},$$

which is unitary. Moreover, $G_\Gamma(\vec{c})$ has a block diagonal structure, i.e.,

$$G_\Gamma(\vec{c}) = \begin{pmatrix} W & 0 \\ 0 & W \end{pmatrix},$$

where W is the 2×2 Fourier matrix.

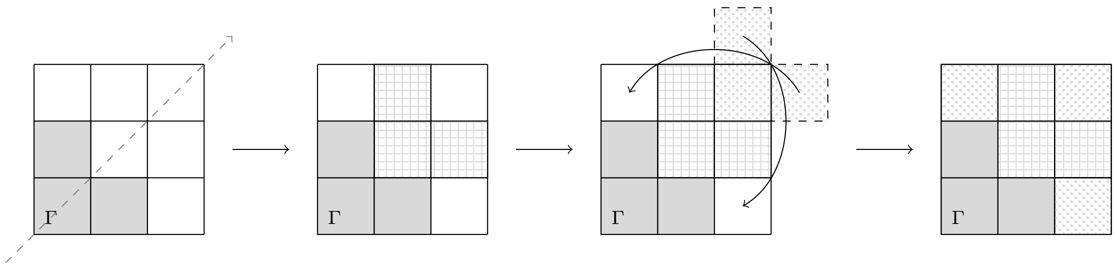
In general, one can derive in a similar way that if $n = m^2$ for some natural number $m \geq 2$, and Γ is the subgroup generated by $(0,m)$ and $(m,0)$, then choosing $\vec{c} = \frac{1}{\sqrt{m}}(\underbrace{1,\dots,1}_{m \text{ items}}, 0, \dots, 0)^T$ leads to the unitary block diagonal matrix $G_\Gamma(\vec{c}) = \mathrm{diag}(\underbrace{W,\dots,W}_{m \text{ items}})$ where W is the $m \times m$ Fourier matrix. In particular, Γ satisfies (I) but not (II) in such cases.

There are little clues concerning whether the necessity holds for composite n as well, yet from a purely aesthetic perspective, the author tends to conjecture that such a symmetric statement (Γ is either a subgroup of order n or the quotient of such a subgroup) should be true.

Appendix. Shapes of support sets

Finally we provide an interesting interpretation of the condition in Theorem 1 and condition (II) in Theorem 2. Plot $\mathbb{Z}_n \times \mathbb{Z}_n$ on an $n \times n$ grid with (j,k) mapped to the corresponding cell (orientation of coordinates does not matter). Because of the group structure, opposite edges are identifiable with each other, thus we obtain a torus. Each support set Γ now occupies a number of cells in the grid, and $\Gamma \times H_s$ can be visualized as shifting Γ along the line of slope s. The condition $\Gamma \times H_s = \mathbb{Z}_n \times \mathbb{Z}_n$ means that it tiles up the whole grid on the torus.

Below is an example for $\Gamma = \{(0,0),(1,0),(0,1)\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$, which consists of precisely one element from each coset of H_1, and it tiles up the grid when shifted along the subgroup H_1.



Now regions of certain shapes will always admit orthonormal Gabor bases. For instance, consider $\{(0,0),(0,1),\dots,(0,k)\} \cup \{(1,0),(2,0),\dots,(n-k-1,0)\} \subset \mathbb{Z}_n \times \mathbb{Z}_n$ where k is a fixed number between 1 and $n-2$. We may call it an L-shaped region, the name is self-explanatory. It is easy to verify that $\Delta\Gamma \cap H_1 = \emptyset$ holds for any L-shaped region Γ, therefore orthonormal Gabor bases always exist on L-shaped regions.

References

[1] D. Gabor, Theory of communication part 1: the analysis of information, J. Inst. Electr. Eng., Part 3, Radio Commun. Eng. 93 (26) (1946) 429–441.
[2] T. Hungerford, Algebra, Springer, 1974.
[3] G. Björck, R. Fröberg, A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots, J. Symb. Comput. 12 (3) (1991) 329–336.
[4] R. Horn, Topics in Matrix Analysis, Cambridge University Press, 1991.
[5] S. Qiu, H. Feichtinger, Discrete Gabor structures and optimal representations, IEEE Trans. Signal Process. 43 (10) (1995) 2258–2268.
[6] S. Qiu, Discrete Gabor transforms: the Gabor-Gram matrix approach, J. Fourier Anal. Appl. 4 (1) (1998) 1–17.
[7] J. Lawrence, G. Pfander, D. Walnut, Linear independence of Gabor systems in finite dimensional vector spaces, J. Fourier Anal. Appl. 11 (6) (2005) 715–726.
[8] D. Tse, P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005.
[9] S. Howard, A. Calderbank, W. Moran, The finite Heisenberg-Weyl groups in radar and communications, EURASIP J. Appl. Signal Process. 1 (12) (2006).
[10] G. Pfander, D. Walnut, Measurement of time-variant linear channels, IEEE Trans. Inf. Theory 52 (11) (2006) 4808–4820.
[11] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices, arXiv preprint, arXiv:0803.2629, 2008.
[12] H. Krovi, M. Rötteler, An efficient quantum algorithm for the hidden subgroup problem over Weyl-Heisenberg groups, in: Mathematical Methods in Computer Science, Springer, 2008, pp. 70–88.
[13] T. Durt, B. Englert, I. Bengtsson, K. Zyczkowski, On mutually unbiased bases, Int. J. Quantum Inf. 8 (4) (2010) 535–640.
[14] G. Matz, F. Hlawatsch, Fundamentals of time-varying communication channels, in: Wireless Communications over Rapidly Time-Varying Channels, Elsevier, 2011, pp. 1–63.
[15] K. Gröchenig, Foundations of Time-Frequency Analysis, Springer, 2013.
[16] G. Matz, H. Bolcskei, F. Hlawatsch, Time-frequency foundations of communications: concepts and tools, IEEE Signal Process. Mag. 30 (6) (2013) 87–96.
[17] G. Pfander, Gabor frames in finite dimensions, in: Finite Frames, Springer, 2013, pp. 193–239.
[18] M. Hampejs, N. Holighaus, L. Tóth, C. Wiesmeyr, Representing and counting the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$, J. Numbers (2014).
[19] R. Malikiosis, A note on Gabor frames in finite dimensions, Appl. Comput. Harmon. Anal. 38 (2) (2015) 318–330.
[20] G. Pfander, D.F. Walnut, Sampling and reconstruction of operators, IEEE Trans. Inf. Theory 62 (1) (2016) 435–458.