Banach J. Math. Anal. (2024) 18:51
https://doi.org/10.1007/s43037-024-00361-x

ORIGINAL PAPER

A Fuglede type conjecture for discrete Gabor bases

Weiqi Zhou[1]

Received: 7 January 2024 / Accepted: 28 May 2024

Abstract
This paper addresses the link between the characterization of spectral sets for orthogonal Fourier bases in $\mathbb{Z}_n^2$ and for discrete orthogonal Gabor bases in $\mathbb{Z}_n^2$. For Fourier bases there is a well known conjecture (i.e., the Fuglede conjecture) which states that a set is spectral if and only if it is a tile. This conjecture has been disproved for $d \geq 3$ (d for dimension) and remains open for $d = 1, 2$. A similar but stricter characterization for discrete orthogonal Gabor bases is conjectured here, which states that the support set shall not only be tiling but also either a subgroup of order n (i.e., a Lagrangian) or a tiling complement of such a subgroup. The additional requirement comes from restrictions on the window vector. The author has established this statement (in both directions) before for n being a prime number, the purpose of this paper is to extend this result to n being a prime square. As opposed to possible false first impressions, this is not a simple extension of the prime case, and actually relies heavily on several new techniques.

Keywords Discrete Gabor systems · Fuglede conjecture · Finite Heisenberg group · Symplectic modules

Mathematics Subject Classification 42A99 · 47G30

1 Introduction

Definition 1.1 A multiset is a collection of elements in which elements are allowed to be repeated. A simple set (i.e., a set in the usual sense) is then a special case of multisets in which every element has multiplicity 1.

Sets in this article are simple by default, multisets will only be used after specifications.

Communicated by Deguang Han.

✉ Weiqi Zhou
zwq@xzit.edu.cn

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

Published online: 08 June 2024

Let A, B be subsets of an additive finite Abelian group G, we use $A + B$ for the multiset formed by elements of form $a + b$ where a, b are enumerated from A, B respectively. We write $A \oplus B$ if $A + B$ is actually a simple set, and in such case we may also say that A, B are tiling complements of each other in $A \oplus B$.

Let

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}, \quad \widehat{\mathbb{Z}_n} = \left\{0, \frac{1}{n}, \dots, \frac{n-1}{n}\right\},$$

respectively be the additive cyclic group of n elements and its dual, $\mathbb{Z}_n$ is isomorphic to $\widehat{\mathbb{Z}_n}$ under the map $d \mapsto d/n$ $(d \in \mathbb{Z}_n)$. To better distinguish them, we will always use the hat symbol when talking about subsets in $\widehat{\mathbb{Z}_n}$, i.e., if $S \subseteq \mathbb{Z}_n$, then $\widehat{S} = \{s/n : s \in S\}$. We take $\widehat{\mathbb{Z}_n \times \mathbb{Z}_n} = \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}$, and will follow this convention consistently. If $x, y \in \mathbb{R}^d$, then we denote the Euclidean inner product of x, y by $x \cdot y$.

Definition 1.2 A subset A is said to be a tiling set (or a tile) in an additive finite Abelian group G, if there exists another subset B of G so that $A \oplus B = G$ (i.e., each element $g \in G$ can be uniquely decomposed as $g = a + b$ with $a \in A$ and $b \in B$). In such case we shall call (A, B) a tiling pair in G.

A subset A is said to be spectral in $\mathbb{Z}_n \times \mathbb{Z}_n$, if there is some $\widehat{S} \subseteq \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}$ such that $\{e^{2\pi i \hat{s} \cdot x}\}_{\hat{s} \in \widehat{S}}$ is an orthogonal bases on $L^2(A)$ with respect to the counting measure. In such case we shall call $(A, \widehat{S})$ a (Euclidean) spectral pair in $\mathbb{Z}_n \times \mathbb{Z}_n$. A famous and central problem concerning spectral sets and tiling sets is the Fuglede conjecture [10], which says that a set in $\mathbb{R}^d$ is spectral (in $\mathbb{R}^d$) if and only if it is a tile (in $\mathbb{R}^d$). Fuglede proved the statement for fundamental domains of lattices, and also showed that disks and triangles are not spectral. The conjecture is true for convex regions on all dimensions [31], but it is false in both directions for $d \geq 3$, see e.g. [9, 22, 23, 34, 45]. For lower dimensions it remains open.

An effective strategy for attacking this problem in $\mathbb{R}^d$ is to try to reduce it to finite Abelian groups. Counterexamples mentioned above in $\mathbb{R}^d$ for $d \geq 3$ are constructed via complex Hadamard matrices which arise from different tiling sets and spectral sets in finite Abelian groups. Standard statements as in [34, Proposition 2.1, Proposition 2.5] and [23, Theorem 4.1, Theorem 4.2] indicate that positivity of the conjecture in $\mathbb{R}^d$ always imply positivity of the conjecture in finite Abelian groups generated by d elements. The other direction is only established partially, the case of $d = 1$ is elaborated in [6, Theorem 1.3, Theorem 3.2] using rationality and periodicity results in [16, 21, 27], while for $d = 2$ even periodicity is only known on $\mathbb{Z}^2$ and on particular domains, see [2, 13, 14, 19, 35, 47]. Various results are available in finite Abelian groups with at most two generators, see e.g. [4, 7, 8, 18, 20, 24, 25, 28, 33, 41, 43, 44, 48, 49].

In this paper we formulate (and partially prove) the following characterization of orthogonal discrete Gabor bases that links its orthogonality to the tiling property of its support set, which gives the statement the same flavour of the Fuglede conjecture (but in a more restrictive way). To get started, a few concepts and notions shall be introduced first:

Definition 1.3 Let $\omega = e^{2\pi i/n}$ be a primitive n-th root of unity, and $(c_1, \dots, c_n)^T \in \mathbb{C}^n$ (the symbol T in the superscript means transpose). The discrete translation operator T and the discrete modulation operator M on $\mathbb{C}^n$ are respectively

$$T : (c_1, \dots, c_n)^T \mapsto (c_n, c_1, \dots, c_{n-1})^T;$$
$$M : (c_1, \dots, c_n)^T \mapsto (c_1, \omega c_2 \dots, \omega^{n-1} c_n)^T,$$

and a discrete time-frequency shift is denoted by

$$\pi(j,k) = M^j T^k, \quad \pi^*(j,k) = T^{-k} M^{-j}. \tag{1.1}$$

Let I be the identity operator on $\mathbb{C}^n$, since $T^n = M^n = I$, it is natural to consider $\pi(j,k)$ as induced by elements $(j,k) \in \mathbb{Z}_n \times \mathbb{Z}_n$ and use the notation $\pi(H)$ for the set of all discrete time-frequency shifts induced by $H \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$. Moreover, as

$$MT = \omega TM, \tag{1.2}$$

$\{\omega, M, T\}$ generates a representation of the finite Heisenberg group. It is also important to be aware that $\pi(\mathbb{Z}_n \times \mathbb{Z}_n)$ is not a representation of $\mathbb{Z}_n \times \mathbb{Z}_n$.

Definition 1.4 A discrete Gabor system on $\mathbb{C}^n$ consists of a support set $S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ and a window vector $\vec{c} \in \mathbb{C}^n$, it is defined and denoted by

$$\mathcal{G}(S, \vec{c}) = \{\pi(s)\vec{c} : \quad s \in S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n, \ \vec{c} \in \mathbb{C}^n\}.$$

The notation $G_S(\vec{c})$ will be used for the matrix formed by taking $\mathcal{G}(S, \vec{c})$ as its column vectors, the ordering of columns does not matter in this article.

Example 1.1 If $\vec{c} = (1, 0, \dots, 0)^T$, and $S = \{0\} \times \mathbb{Z}_n$, then $\mathcal{G}(S, \vec{c})$ is the Euclidean basis; Alternatively if $\vec{c} = n^{-1/2}(1, \dots, 1)^T$, and $S = \mathbb{Z}_n \times \{0\}$, then $\mathcal{G}(S, \vec{c})$ is the Fourier basis. They are both orthonormal bases on $\mathbb{C}^n$.

Gabor systems [11] in $L^2(\mathbb{R}^n)$ is a fundamental object in Gabor analysis, discrete Gabor systems [37, 38] are relatively new tools that can be viewed as counterparts of continuous Gabor systems. The exposition in [36] gives a good overview of them. A remarkable property is the full sparkness of such systems [30, 32].

Definition 1.5 Let $S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, we shall call S a discrete Gabor tile if it is either an order n subgroup (i.e., a Lagrangian, see Lemma 2.2 below), or is the tiling complement of an order n subgroup. If $\mathcal{G}(S, \vec{c})$ is actually an orthonormal system, then we shall call $\vec{c}$ a discrete Gabor spectrum of S.

It is clear that any orthogonal system $\mathcal{G}(S, \vec{c})$ can be turned into orthonormal by a scaling on $\vec{c}$, thus there is no harm by restricting ourselves to orthonormal systems only. It is also worth mentioning that CAZAC sequences [1] can be constructed out of such systems.

The author showed in [50] that

Theorem 1.1 *If $S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ is a discrete Gabor tile, then it has a discrete Gabor spectrum. If n is a prime number, then the converse (i.e., if S has a Gabor spectrum, then it is a discrete Gabor tile) is also true.*

The converse part for composite n is also conjectured but still seems to be difficult to prove. The statement of the theorem is very similar to the Fuglede conjecture even though the author is not able to provide a good reason for that at the moment. The tiling condition is stricter than the Fuglede conjecture, probably due to the fact that there is a stronger interaction between S and $\vec{c}$ (see Sect. 3.2 below).

There is a related research in [17] where discrete orthonormal Gabor systems on finite prime fields $\mathbb{Z}_p^d$ are studied. The essential difference between the theorem above and the result in [17], aside from the obvious part on the domain of the window vector ($\mathbb{Z}_n \times \mathbb{Z}_n$ vs. $\mathbb{Z}_p^d$), is that in [17] it is assumed that the support set decomposes into $S = A \times B$, where A is the support of the shift operator T and B is the support of the modulation operator M. We do not have such a restriction on S here in our theorem.

An analogous statement for continuous Gabor systems is to ask, for which set of translations and modulations can one find a window function g so that together they form an orthonormal Gabor bases. This is complicated even for simple g [12], see also [5, 26] and references therein.

The main purpose of this article is to establish the converse part of the above theorem for n being a prime square. As opposed to possible false first impressions, this is not a simple extension of the prime case, but requires much insights into structures of tiling sets and window vectors. We used symplectic methods to analyze the zero set of the characteristic polynomial (also called the mask polynomial in some literature) of S. The study of zero sets is a standard approach in the research of the Fuglede conjecture, but the application of symplectomorphisms is a new technique, it allows us to apply coordinate transforms for reductions.

2 Preliminaries

2.1 Symplectic tiling/spectral pairs

Let S be a subset of an additive Abelian group G, denote the difference set of S by

$$\Delta S = \{s - s' : \ s, s' \in S, \ s \neq s'\}.$$

Let A, B be subsets of an additive Abelian group G. Clearly $A + B = A \oplus B$ if and only if the map

$$(a, b) \mapsto a + b, \quad a \in A, b \in B,$$

is injective. This map is not injective if and only if there exist distinct $a, a' \in A$ and $b, b' \in B$ with $a + b = a' + b'$, i.e., $a - a' = b' - b$, which means

$$A + B = A \oplus B \quad \Leftrightarrow \quad \Delta A \cap \Delta B = \emptyset. \tag{2.1}$$

Definition 2.1 For $(j,k),(j',k')\in\mathbb{R}^2$, define the following symplectic bilinear form:

$$\langle (j,k),(j',k')\rangle_s = jk' - kj'.$$

Let $A\subseteq\mathbb{Z}_n\times\mathbb{Z}_n$, and $\widehat{S}\subseteq\widehat{\mathbb{Z}_n}\times\widehat{\mathbb{Z}_n}$, we shall call $(A,\widehat{S})$ a symplectic spectral pair in $\mathbb{Z}_n\times\mathbb{Z}_n$, if $\{e^{2\pi i\langle x,s\rangle_s}\}_{s\in\widehat{S}}$ is an orthogonal bases on $L^2(A)$ with respect to the counting measure. $\widehat{S}$ is then called the symplectic spectrum of A in such case.

If $s=(s_1,s_2)$, $s'=(s_2,-s_1)$, $x=(x_1,x_2)$ and

$$S'=\{(s_2,-s_1):(s_1,s_2)\in\widehat{S}\subseteq\widehat{\mathbb{Z}_n}\times\widehat{\mathbb{Z}_n}\},$$

then $\widehat{S}\to S'$ is a bijective map, and

$$\langle x,s\rangle_s = x_1s_2 - x_2s_1 = x\cdot s',$$

which shows that $(A,\widehat{S})$ is a symplectic spectral pair if and only if (A,S') is a Euclidean spectral pair.

Given a function f, define its zero set to be

$$Z(f)=\{t:f(t)=0\}.$$

Let A be a multiset with elements from $\mathbb{Z}_n\times\mathbb{Z}_n$, and set

$$F_A(s)=\sum_{a\in A}e^{2\pi i\langle a,s\rangle_s},\quad s\in\mathbb{R}^2.$$

If A is actually a simple set (i.e., a set in the usual sense), then it is easy to see that $(A,\widehat{S})$ is a symplectic spectral pair in $\mathbb{Z}_n\times\mathbb{Z}_n$ if and only if $(S,\widehat{A})$ is also a symplectic spectral pair in $\mathbb{Z}_n\times\mathbb{Z}_n$, which is equivalent to the condition that

$$\Delta\widehat{S}\subseteq Z(F_A),\quad |A|=|\widehat{S}|. \tag{2.2}$$

Moreover, if we set $z=e^{2\pi i/n}$ and consider $s\in\widehat{\mathbb{Z}_n}\times\widehat{\mathbb{Z}_n}$, then $F_A(s)$ is just a univariate polynomial of z with positive coefficients. On the other hand, it would be convenient to also consider F_A as induced by the polynomial

$$\tilde{F}_A(x,y)=\sum_{(a_1,a_2)\in A}x^{a_1}y^{a_2},$$

so that if $s=(s_1,s_2)$ then

$$F_A(s)=\tilde{F}_A(e^{2\pi i s_2},e^{-2\pi i s_1}),$$

and

$$F_A(0,0)=\tilde{F}_A(1,1)=|A|.$$

Consequently if $A, B \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, then (A, B) being a tiling pair is equivalent to

$$\Delta(\widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}) \subseteq Z(F_A) \cup Z(F_B), \quad |A| \cdot |B| = n^2. \tag{2.3}$$

2.2 Symplectic basis

Definition 2.2 Given $A \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, let

$$A^{\perp} = \{h \in \mathbb{Z}_n \times \mathbb{Z}_n : \langle a, h \rangle_s = 0, \forall a \in A\}.$$

A is called isotropic if $A \subseteq A^{\perp}$ and Lagrangian if $A = A^{\perp}$.

$A^{\perp}$ is important since $\pi(A^{\perp})$ is precisely the set that commutates with $\pi(A)$ (see Eq. (2.5) below). We use $\gcd(a, b)$ for the greatest common divisor of a and b.

Lemma 2.1 *$\{h, h'\}$ is a pair of generators of $\mathbb{Z}_n \times \mathbb{Z}_n$ if and only if*

$$\gcd(\langle h, h' \rangle_s, n) = 1.$$

Proof For any element $h = (j, k) \in \mathbb{Z}_n \times \mathbb{Z}_n$, we have

$$\gcd(j, k) = \frac{n}{\operatorname{ord}(h)},$$

where $\operatorname{ord}(h)$ is the order of h in $\mathbb{Z}_n \times \mathbb{Z}_n$ (the smallest natural number m such that $\underbrace{h + \cdots + h}_{m \text{ items}} = 0$).

If $\operatorname{ord}(h) = n$, i.e., $\gcd(j, k) = 1$, then the Bézout identity shows that the solution to

$$jy - kx = 0$$

in $\mathbb{Z}$ is precisely $(x, y) = d(j, k)$ for any $d \in \mathbb{Z}$. Consequently it has exactly n solutions in $\mathbb{Z}_n \times \mathbb{Z}_n$, i.e., $\{h\}^{\perp}$ is the cyclic subgroup generated by h.

Now if h, h' is a pair of generators of $\mathbb{Z}_n \times \mathbb{Z}_n$, then $\operatorname{ord}(h) = \operatorname{ord}(h') = n$, and cyclic subgroups generated by h and h' intersect trivially. Suppose $\gcd(\langle h, h' \rangle_s, n) = d \neq 1$, then taking $c = n/d$ and $b = \langle h, h' \rangle_s / d$ we get

$$\langle h, ch' \rangle_s \equiv c \langle h, h' \rangle_s \equiv cdb \equiv nb \equiv 0 \pmod{n},$$

which is impossible since ch' is not in the cyclic subgroup generated by h.

Conversely if $h, h' \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfy $\gcd(\langle h, h' \rangle_s, n) = 1$, then there is some $k \in \mathbb{N}$ that is co-prime to n such that

$$k \langle h, h' \rangle_s \equiv 1 \pmod{n},$$

consequently

$$\mathrm{ord}(h) \equiv \mathrm{ord}(h)k\langle h, h'\rangle_s \equiv k\langle \mathrm{ord}(h)h, h'\rangle_s \equiv k\langle 0, h'\rangle_s \equiv 0 \pmod{n},$$

and

$$\mathrm{ord}(h') \equiv \mathrm{ord}(h')k\langle h, h'\rangle_s \equiv k\langle h, \mathrm{ord}(h)h'\rangle_s \equiv k\langle h, 0\rangle_s \equiv 0 \pmod{n},$$

which shows (since $\gcd(k, n) = 1$) that

$$\mathrm{ord}(h) = \mathrm{ord}(h') = n.$$

Thus they each generate a maximal cyclic subgroup. Let H, H' be maximal cyclic subgroups generated by h, h' respectively, and suppose $ah \in H'$, then we have

$$0 \equiv k\langle ah, h'\rangle_s \equiv ak\langle h, h'\rangle_s \equiv a \pmod{n},$$

which implies $a \equiv 0 \bmod n$, i.e., H, H' intersect trivially, consequently h, h' generate the full group $\mathbb{Z}_n \times \mathbb{Z}_n$. □

Lemma 2.2 *$H \subset \mathbb{Z}_n \times \mathbb{Z}_n$ is a Lagrangian if and only if H is an order n subgroup.*

Proof First consider an arbitrary subset H in $\mathbb{Z}_n \times \mathbb{Z}_n$. Observe that $0 \in H^\perp$, moreover, by the bilinearity of the symplectic form we have that $h \in H^\perp$ implies $-h \in H^\perp$, and $h, h' \in H^\perp$ implies $h + h' \in H^\perp$, therefore $H^\perp$ is a subgroup. Consequently Lagrangians must always be subgroups.

It then follows from the proof (the second paragraph in the proof) of Lemma 2.1 that cyclic Lagrangians are precisely maximal cyclic subgroups.

Now let h, h' be a pair of generator of $\mathbb{Z}_n \times \mathbb{Z}_n$, and consider the subgroup H generated by ah, bh'. By Lemma 2.1 we see that n divides ab if and only if

$$0 \equiv \langle ah, bh'\rangle_s \equiv ab\langle h, h\rangle_s \pmod{n}.$$

Therefore if $ab = dn$ for some $d > 1$, then let $a = a'd_1$, $b = b'd_2$ with $d_1 d_2 = d$, clearly at least one of d_1, d_2 is greater than 1, say $d_1 > 1$ without loss of generality, then we have $\langle a'h, ah\rangle_s = 0$ and

$$\langle a'h, bh'\rangle_s \equiv \frac{ab}{d_1}\langle h, h'\rangle_s \equiv \frac{dn}{d_1}\langle h, h'\rangle_s \equiv d_2 n\langle h, h'\rangle_s \equiv 0 \pmod{n}.$$

Therefore $H^\perp$ contains the subgroup generated by $a'h$ and bh', which makes it larger than, instead of equal to, H. Consequently $H = H^\perp$ (i.e., H is a Lagrangian) if and only if $ab = n$, in which case the order of H is

$$\frac{n}{a} \cdot \frac{n}{b} = n.$$

□

Definition 2.3 $\{h, h'\}$ is said to be a symplectic basis of $\mathbb{Z}_n \times \mathbb{Z}_n$ if $\langle h, h' \rangle_s = 1$.

Definition 2.4 ψ is said to be a symplectomorphism on $\mathbb{Z}_n \times \mathbb{Z}_n$ if it keeps the symplectic form $\langle \cdot, \cdot \rangle_s$ invariant, i.e.,

$$\langle h, h' \rangle_s = \langle \psi(h), \psi(h') \rangle_s,$$

holds for any $h, h' \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Lemma 2.1 shows that if $\{h, h'\}$ is a symplectic basis, then they generate a tiling pair of cyclic Lagrangians in $\mathbb{Z}_n \times \mathbb{Z}_n$, therefore symplectomorphism are not only just change of symplectic basis but also group automorphisms. On the other hand, Lemma 2.3 below shows conversely that if H is a cyclic Lagrangian with generator h, then in each cyclic Lagrangian H' that intersects H trivially (which makes H' a tiling complement of H) one can always find some h' so that $\{h, h'\}$ is a symplectic basis. Thus by switching to the standard basis using proper symplectomorphisms (which changes neither tilingness nor spectrality), we are able to reduce the amount of cases to be analyzed. In contrast, such tools are not available with Euclidean inner products, since a tiling pair of cyclic Lagrangians need not contain a pair of orthogonal Euclidean basis.

Lemma 2.3 *If H, H' are cyclic Lagrangians such that $\mathbb{Z}_n \times \mathbb{Z}_n = H \oplus H'$, then there exists a symplectomorphism ψ with*

$$\psi(H) = \mathbb{Z}_n \times \{0\}, \quad \psi(H') = \{0\} \times \mathbb{Z}_n. \tag{2.4}$$

Proof Let h be a generator of H, and h' a generator of H'. If $a = \langle h, h' \rangle_s$, then by Lemma 2.1 we have $\gcd(a, n) = 1$, hence a is an element of the multiplicative group modulo n. Let a^{-1} be the inverse of a in the multiplicative group modulo n, clearly $\gcd(a^{-1}, n) = 1$ since a^{-1} is also a member of the multiplicative group modulo n, consequently $a^{-1}h'$ is still a generator of H'. Moreover, we have

$$\langle h, a^{-1}h' \rangle_s \equiv a^{-1} \langle h, h' \rangle_s \equiv a^{-1} \cdot a \equiv 1 \pmod{n},$$

which shows that $\{h, a^{-1}h'\}$ is a symplectic basis. Now we take ψ to be the group automorphism on $\mathbb{Z}_n \times \mathbb{Z}_n$ that maps h to $(1, 0)$ and $a^{-1}h'$ to $(0, 1)$, then Eq. (2.4) is satisfied. ψ is also a symplectomorphism since it is linear and maps the symplectic basis $\{h, a^{-1}h'\}$ to the symplectic basis $\{(1, 0), (0, 1)\}$. □

It is clear that

$$F_A(\hat{s}) = F_{\psi(A)}\left(\widehat{\psi(s)}\right),$$

holds for any symplectomorphism ψ, subsets $A \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, and element $\hat{s} \in \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}$. Therefore Eqs. (2.2) and (2.3) must hold or break simultaneously on A and $\psi(A)$, thus A is a tiling set (resp. a spectral set) in $\mathbb{Z}_n \times \mathbb{Z}_n$ if and only $\psi(A)$ is also a tiling set (resp. a spectral set) in $\mathbb{Z}_n \times \mathbb{Z}_n$.

2.3 Annihilation and complementation

For each $m \in \mathbb{N}$, let $\Phi_m(x)$ be the m-th cyclotomic polynomial (i.e., $\Phi_m(x) = \prod_i (x - \zeta_i)$ where ζ_i runs over all m-th primitive roots of unity).

Lemma 2.4 *Let $A \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ and $\hat{h}, \hat{h}' \in \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}$, if $\hat{h}, \hat{h}'$ generates the same cyclic subgroup, then $\hat{h} \in Z(F_A)$ implies $\hat{h}' \in Z(F_A)$.*

Proof Let m be the order of $\hat{h}$ in $\widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}$ and $\widehat{H}$ the cyclic subgroup generated by $\hat{h}$. Since both $\hat{h}$ and $\hat{h}'$ are generators of $\widehat{H}$, we must have $\hat{h}' = b\hat{h}$ for some b with $\gcd(b, m) = 1$. If we set $z = e^{2\pi i/m}$, then $F_A(\hat{h})$ is a polynomial of z divisible by $\Phi_m(z)$, which we write as $f_A(z)$, then we have

$$F_A(\hat{h}') = F_A(b\hat{h}) = f_A(z^b) = 0,$$

therefore all generators of $\widehat{H}$ are contained in $Z(F_A)$. □

Lemma 2.5 *If H is a subgroup in $\mathbb{Z}_n \times \mathbb{Z}_n$, then*

$$(\widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n}) \cap Z(F_H) = \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n} \setminus \widehat{H^\perp}.$$

Proof There are two cases:

- H is cyclic: By Lemma 2.3 it suffices to consider H generated by $(a, 0)$ for some $a \in \mathbb{Z}_n$, other cases will follow by applying a proper symplectomorphism. Let $b = n/a$, and $H' = \{0\} \times b\mathbb{Z}_a$, the cyclic subgroup generated by $(0, b)$, notice that

$$H^\perp = \mathbb{Z}_n \times b\mathbb{Z}_a = (\mathbb{Z}_n \times \{0\}) \oplus H'.$$

  Thus if $\hat{s} \in \widehat{H^\perp}$, then

$$F_H(\hat{s}) = |H| \neq 0,$$

  while if $\hat{s} \in \widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n} \setminus \widehat{H^\perp}$, then it can be written as $\hat{s} = (j/n, k/n)$ for some $j \in \mathbb{Z}_n$ and $k \in \mathbb{Z}_n \setminus b\mathbb{Z}_a$, consequently

$$F_H(\hat{s}) = \sum_{t=0}^{b-1} e^{2\pi i \frac{kta}{n}} = \sum_{t=0}^{b-1} e^{2\pi i \frac{kt}{b}} = 0,$$

  which shows that $\widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n} \setminus \widehat{H^\perp} = Z(F_H) \cap (\widehat{\mathbb{Z}_n} \times \widehat{\mathbb{Z}_n})$.
- H is not cyclic: Again by Lemma 2.3 it suffices to consider H generated by $(a, 0)$ and $(0, b)$ for some $a, b \in \mathbb{Z}_n$, other cases will follow by applying a proper symplectomorphism. Let A, B denote cyclic subgroups generated by $(a, 0)$ and $(0, b)$ respectively, then $H = A \oplus B$ and thus

$$H^\perp = A^\perp \cap B^\perp, \quad Z(F_H) = Z(F_A) \cup Z(F_B),$$

the result then follows from the cyclic case.

□

Lemma 2.6 *Let H be a subgroup in $\mathbb{Z}_n \times \mathbb{Z}_n$, then $C \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$ is a tiling complement of H in $\mathbb{Z}_n \times \mathbb{Z}_n$ if and only if $|C| = n/|H|$ and*

$$\Delta\widehat{H^{\perp}} \subseteq Z(F_C).$$

Proof Combine Eq. (2.3) and Lemma 2.5. □

2.4 Centralizer and projector

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

$$\langle A, B\rangle = \mathrm{tr}(AB^*), \quad A, B \in \mathbb{C}^{n\times n},$$

where tr is the trace and B^* is the adjoint of B. With this setting it is easy to verify that $n^{-1/2}\pi(\mathbb{Z}_n \times \mathbb{Z}_n)$ is an orthonormal basis for $\mathbb{C}^{n\times n}$.

For an element $g \in \mathbb{Z}_n \times \mathbb{Z}_n$, let

$$P_g A = \pi(g)A\pi^*(g), \quad A \in \mathbb{C}^{n\times n},$$

be the simultaneous conjugation by $\pi(g)$. Similarly for a subset $S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, let

$$P_S A = \frac{1}{|S|}\sum_{s\in S} P_s A, \quad A \in \mathbb{C}^{n\times n}.$$

These operators commute, i.e., $P_S P_H = P_H P_S$ for any two subsets $S, H \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$.

It follows from Eq. (1.2) that

$$\pi(h)\pi(h') = \omega^{\langle h,h'\rangle_s}\pi(h')\pi(h), \tag{2.5}$$

which shows that $\pi(S^{\perp})$ is the centralizer of $\pi(S)$, more importantly Eq. (2.5) leads to

$$P_S\pi(h) = \frac{1}{|S|}F_S(\hat{h})\pi(h). \tag{2.6}$$

Corollary 2.1 *Let $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ be a subgroup, then P_H is the orthogonal projection onto the span of $\pi(H^{\perp})$.*

Proof Combine Eq. (2.6) with Lemma 2.5. □

For a vector $\vec{c} \in \mathbb{C}^n$ let

$$P_{\vec{c}} = \vec{c}\vec{c}^*,$$

be the (scaled) projector onto the span of $\vec{c}$.

The frame operator of a discrete Gabor system $\mathcal{G}(S, \vec{c})$ is then simply

$$G_S(\vec{c})G_S^*(\vec{c}) = |S| P_S P_{\vec{c}}.$$

Moreover, by looking at the Gram matrix $G_S^*(\vec{c})G_S(\vec{c})$ we can easily see that

$$\mathcal{G}(S, \vec{c}) \text{ is an orthogonal system} \Leftrightarrow P_{\vec{c}} \perp \pi(\Delta S). \tag{2.7}$$

For a vector $\vec{c} \in \mathbb{C}^n$, set

$$Z(P_{\vec{c}}) = \{h \in \mathbb{Z}_n \times \mathbb{Z}_n : \langle P_{\vec{c}}, \pi(h)\rangle = 0\},$$

and

$$\text{supp}(P_{\vec{c}}) = \{h \in \mathbb{Z}_n \times \mathbb{Z}_n : \langle P_{\vec{c}}, \pi(h)\rangle \neq 0\}.$$

Lemma 2.7 *If $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a Lagrangian, V is a unitary matrix that simultaneously diagonalizes $\pi(H)$, and $\vec{c}$ is a column in V, then* $\text{supp}(P_{\vec{c}}) \subseteq H$.

Proof Each element in $\pi(H)$ is unitary, thus normal and can be diagonalized. H being Lagrangian implies that elements in $\pi(H)$ mutually commute, therefore they can indeed be simultaneously diagonalized. Since they are linearly independent, their spectrums (viewed as vectors) are also linearly independent and thus form a basis of $\mathbb{C}^n$. Consequently there exists linear combinations of them that produces matrices with spectrums $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)$, each of which is an instance of $P_{\vec{c}}$. □

Lemma 2.8 *Let $S \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, $\vec{c} \in \mathbb{C}^n$, if $\mathcal{G}(S, \vec{c})$ is an orthonormal basis of $\mathbb{C}^n$, then we have*

$$\widehat{\text{supp}(P_{\vec{c}})} \setminus \{(0, 0)\} \subseteq Z(F_S).$$

Conversely if $h \in \mathbb{Z}_n \times \mathbb{Z}_n \setminus \{(0, 0)\}$ and $\hat{h} \notin Z(F_S)$, then

$$h \in Z(P_{\vec{c}}).$$

Proof If $\mathcal{G}(S, \vec{c})$ is an orthonormal basis of $\mathbb{C}^n$, then $G_S(\vec{c})$ is unitary and we have for its frame operator that

$$n P_S P_{\vec{c}} = G_S(\vec{c})G_S^*(\vec{c}) = I,$$

Take a cyclic Lagrangian $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ and let h be its generator, then by Corollary 2.1, P_H is the orthogonal projection onto the span of $\pi(H)$, thus

$$I = n P_H P_S P_{\vec{c}} = n P_S P_H P_{\vec{c}}$$

$$= nP_S\left(\sum_{k=0}^{n-1} c_k\pi(kh)\right)$$
$$= I + n\sum_{k=1}^{n-1} c_k P_S\pi(hk).$$

where $c_k = \langle P_{\vec{c}}, \pi(kh)\rangle/n$. Therefore for the equation to hold c_k has to be 0 if $P_S\pi(kh) \neq 0$, similarly $P_S\pi(kh)$ has to be 0 if $c_k \neq 0$, and this is valid for all cyclic Lagrangians (which jointly cover $\mathbb{Z}_n \times \mathbb{Z}_n$), thus the conclusion follows from Eq. (2.6). □

It is shown in [30, 32] that if S is an order n subset in $\mathbb{Z}_n \times \mathbb{Z}_n$, then the set of vectors $\vec{c}$ that makes $\mathcal{G}(S, \vec{c})$ a basis of $\mathbb{C}^n$ is open dense in $\mathbb{C}^n$. Below is a shorter proof for the particular case when S is a Lagrangian, in the proof such window vectors are also characterized.

Lemma 2.9 *For a Lagrangian $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$, let V be a unitary matrix that simultaneously diagonalizes $\pi(H)$, then $\mathcal{G}(H, \vec{c})$ has rank m if and only if $\vec{c}$ is orthogonal to precisely $n - m$ columns in V.*

Proof Denote the k-th column in V by $\vec{v}_k$. Suppose

$$\vec{c} = \sum_{k=1}^{n} c_k\vec{v}_k,$$

and the simultaneous diagonalization of elements in $\pi(H)$ is

$$\pi(h) = VD_hV^*, \quad h \in H.$$

Write $D_{\vec{c}} = \mathrm{diag}(c_1, \dots, c_n)$, and $\vec{d}^{(h)}$ the vectorization of D_h so that

$$D_h = \mathrm{diag}(d^{(h)}).$$

With these notations we have

$$\pi(h)\vec{c} = VD_hV^*V\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = VD_h\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = VD_{\vec{c}}\,\vec{d}^{(h)}.$$

Now enumerate elements in H as $h_1, \dots, h_n$, then

$$V^*G_H(\vec{c}) = D_{\vec{c}}\left(\vec{d}^{(h_1)}, \vec{d}^{(h_2)}, \dots, \vec{d}^{(h_n)}\right). \tag{2.8}$$

Clearly $\{\vec{d}^{(h)}\}_{h\in H}$ is a linearly independent set since elements in $\pi(H)$ are mutually orthogonal in $\mathbb{C}^{n\times n}$, thus the rank of $G_H(\vec{c})$ equals the number of non-zero entries in $c_1, \dots, c_n$, which is the desired result. □

In particular, $\mathcal{G}(H, \vec{c})$ is a basis of $\mathbb{C}^n$ if and only if $\vec{c}$ is not orthogonal to any column in V.

3 Structures in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

3.1 A counting lemma

Given a prime number p, let us recall the structure of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ and agree on the following notations: The unique subgroup formed by all order p elements will be denoted by K. Counting the number of generators, it is easy to see that there are $p+1$ number of proper and non-trivial subgroups in K, each of them is cyclic and they mutually intersect trivially. The subgroup generated by $(ap, bp) \in K$ will be denoted by $K_{b/a}$ (with the convention $b/a = \infty$ if $a = 0$) so that $K_0, K_1, \ldots, K_{p-1}, K_\infty$ is the list of all proper, non-trivial subgroups in K. Similar arguments indicate that there are $p^2 + p$ cyclic Lagrangians in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, we will denote them by $H_{j,k}$ with $j \in \mathbb{Z}_p$, $k \in \{0, 1, \ldots, p-1, \infty\}$, where $H_{j,k}$ is generated by

$$h_{j,k} = \begin{cases} (1, jp+k) & k \in \{0, 1, \ldots, p-1\}, \\ (jp, 1) & k = \infty. \end{cases}$$

We shall call $\{0, 1, \ldots, p-1, \infty\}$ the index set in the rest part of this paper, and with these notations we have

$$H_{j,k} \cap H_{j',k'} = \begin{cases} \emptyset & \text{if } k \neq k', \\ K_k & \text{if } k = k'. \end{cases}$$

For each $k \in \{0, 1, \ldots, p-1, \infty\}$, we shall write

$$H_k = \bigcup_{j \in \mathbb{Z}_p} H_{j,k} \cup K = K_k^{\perp},$$

and further use

$$\tilde{K}_k = \Delta K_k, \quad \tilde{H}_{j,k} = H_{j,k} \setminus K_k,$$

as the set of all generators in K_k, $H_{j,k}$ respectively. For convenience we also take

$$\tilde{H}_k = \bigcup_{j \in \mathbb{Z}_p} \tilde{H}_{j,k}.$$

The following two pictures may help to build intuitions behind these notations (Figs. 1, 2).

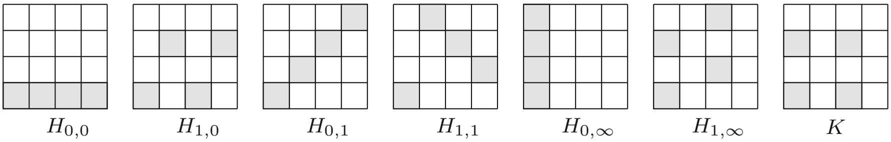

Fig. 1 Lagrangians in $\mathbb{Z}_4 \times \mathbb{Z}_4$

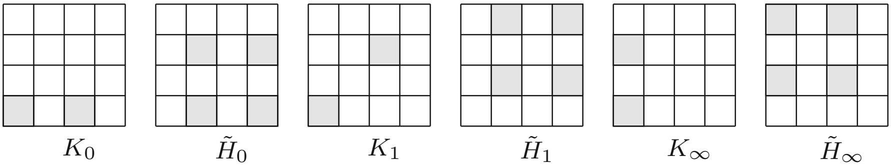

Fig. 2 K_k and $\tilde{H}_k$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$

Lemma 3.1 *Let p be a prime number and A a subset of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ that contains the identity element. If for some $j \in \mathbb{Z}_p$ and some $k \in \{0, 1, \dots, p-1, \infty\}$ we have that $\hat{h} \in \widehat{\tilde{H}_{j,k}}$ is in $Z(F_A)$, then*

$$|A \cap H_k| = p|A \cap H_{j,k}|.$$

Proof Let $z = e^{2\pi i/\operatorname{ord}(\hat{h})}$, then we have

$$0 = F_A(\hat{h}) = \sum_{a \in A} z^{\langle a,h \rangle_s} = f(z)\Phi_{\operatorname{ord}(\hat{h})}(z)$$

for some polynomial f. It is subtle but important to realize that since $\operatorname{ord}(h)$ is a prime power it is actually possible to have all coefficients of f positive (see [29, Theorem 3.3(1)]), and to have its order bounded by p since $z^p\Phi_{p^2}(z) = \Phi_{p^2}(z)$ if $z^{p^2} = 1$ and similarly $z^p\Phi_p(z) = \Phi_p(z)$ if $z^p = 1$. Now A containing the identity element implies that the lowest order term in g is the constant term, which we denote by d.

If $\langle a, h \rangle_s \in p\mathbb{Z}_p \setminus \{0\}$, then we have

$$0 \equiv p\langle a, h \rangle_s \equiv \langle a, ph \rangle_s \pmod{p^2},$$

which means all terms in $\Phi_{p^2}(z)$ is obtained from $a \in A \cap K_k^\perp$ since $ph \in K_k$. Recall that $K_k^\perp = H_k$, and $\langle a, h \rangle_s = 0$ for all $a \in H_{j,k}$, we must then have

$$d = |A \cap H_{j,k}|,$$

and thus

$$|A \cap H_k| = d|\Phi_{p^2}(1)| = p|A \cap H_{j,k}|.$$

□

3.2 Support of window vectors

Let $\zeta = e^{2\pi i/p}$, and $\{\vec{u}^{(j)}\}_{j\in\mathbb{Z}_p}$, $\{\vec{e}^{(j)}\}_{j\in\mathbb{Z}_p}$ be respectively the Fourier basis and the Euclidean basis on $\mathbb{C}^p$. Let $\otimes$ be the matrix Kronecker product. It is verifiable by straightforward computation that the set of vectors $\{\vec{u}^{(a)} \otimes \vec{e}^{(b)}\}_{a,b\in\mathbb{Z}_p}$ simultaneously diagonalize $\pi(K)$ with corresponding eigenvalues being

$$\pi(pj, pk)(\vec{u}^{(a)} \otimes \vec{e}^{(b)}) = \zeta^{bj-ak}(\vec{u}^{(a)} \otimes \vec{e}^{(b)}), \tag{3.1}$$

for each $(j, k) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Lemma 3.2 *Let p be a prime number, and a, b distinct elements from the index set $\{0, 1, \ldots, p-1, \infty\}$. If $\vec{c} \in \mathbb{C}^{p^2}$ satisfies*

$$P_{\vec{c}} \perp \pi(\tilde{H}_a \cup \tilde{K}_b), \tag{3.2}$$

then we will have

$$P_{\vec{c}} \perp \pi(\tilde{K}_a).$$

Proof By Lemma 2.3 it suffices to show for the case of $a = 0$ and $b = \infty$, all other cases can be reduced to this one upon a proper symplectomorphism.

Consider first the Gabor system $\mathcal{G}(K_0, \vec{c})$ and its frame operator $pP_{K_0}P_{\vec{c}}$, clearly its rank is at most p since there are only p vectors in $\mathcal{G}(K_0, \vec{c})$. On the other hand, by Corollary 2.1, P_K is the orthogonal projection onto the span of $\pi(K)$, and P_{K_0} is the orthogonal projection onto the span of $\pi(K_0^{\perp})$, but

$$K_0^{\perp} = K_\infty \oplus H_{0,0} = K \cup \tilde{H}_0,$$

thus Eq. (3.2) actually implies

$$P_{K_0}P_{\vec{c}} = P_K P_{\vec{c}},$$

i.e., the rank of $\mathcal{G}(K, \vec{c})$ equals the rank of $\mathcal{G}(K_0, \vec{c})$, which is at most p since there are only p elements in $\mathcal{G}(K_0, \vec{c})$. On the other hand, Eq. (3.2) shows that the rank of $\mathcal{G}(K, \vec{c})$ is at least p since it contains $\mathcal{G}(K_\infty, \vec{c})$, which by Eq. (2.7) consists of p number of mutually orthogonal vectors. Therefore the ranks of both $\mathcal{G}(K_0, \vec{c})$ and $\mathcal{G}(K, \vec{c})$ are precisely p.

Now we expand $\vec{c}$ with respect to eigenvectors of K as prescribed in Eq. (3.1):

$$\vec{c} = \sum_{a,b\in\mathbb{Z}_p} c_{a,b}\vec{u}^{(a)} \otimes \vec{e}^{(b)}. \tag{3.3}$$

By Lemma 2.9, the rank of $\mathcal{G}(K, \vec{c})$ being p means that there are precisely p non-zero coefficients $c_{a,b}$ in the expansion equation (3.3).

Let $\vec{x}$ be the p-dimensional vector whose b-th (b starts from 0) element x_b is given by

$$x_b = \sum_{a \in \mathbb{Z}_p} |c_{a,b}|^2,$$

The condition that $P_{\vec{c}} \perp \pi(\tilde{K}_\infty)$ in Eq. (3.2) implies that for each $t \in \{1, 2, \ldots, p-1\}$ we have

$$0 = \langle \pi(0, tp)\vec{c}, \vec{c} \rangle,$$

which means $\vec{x}$ is orthogonal to all p-dimensional Fourier basis except $(1, 1, \ldots, 1)^T$. Consequently we get

$$x_0 = x_1 = \cdots = x_{p-1}.$$

which means that for each $b \in \mathbb{Z}_p$ there is precisely one non-zero entry in the set $\{c_{0,b}, c_{1,b}, \ldots, c_{p-1,b}\}$ and their moduli are same.

Now let us write $G_K(\vec{c})$ the same way as in equation (2.8), and look at its sub-matrix

$$G_{K_0}(\vec{c}) = V D_{\vec{c}} \left(\vec{d}^{(0)}, \vec{d}^{(1)}, \ldots, \vec{d}^{(p-1)} \right),$$

where as in Eq. (2.8), V is a matrix that simultaneously diagonalizes all members in $\pi(K)$, $D_{\vec{c}}$ is the diagonal matrix with $c_{a,b}$ inscribed on its main diagonals and $\vec{d}^{(a)}$ is vectorization of the spectrum of $\pi(a, 0)$.

Recall that the rank of $G_{K_0}(\vec{c})$ is p and the rank of V is p^2, hence the rank of $D_{\vec{c}} \left(\vec{d}^{(0)}, \vec{d}^{(1)}, \ldots, \vec{d}^{(p-1)} \right)$ is p. As argued there are only p number of non-zero coefficients $c_{a,b}$, i.e., there are only p non-vanishing rows in $D_{\vec{c}}$, but since $\vec{d}^{(0)}, \vec{d}^{(1)}, \ldots, \vec{d}^{(p-1)}$ are generated from the spectrum of $\pi(kp, 0)$ ($k \in \mathbb{Z}_p$), by Eq. (3.1) if we index its rows by $\mathbb{Z}_p \times \mathbb{Z}_p$, then two rows will be identical if they are in the same coset of K_0 in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$.

Consequently for $D_{\vec{c}} \left(\vec{d}^{(0)}, \vec{d}^{(1)}, \ldots, \vec{d}^{(p-1)} \right)$ to have rank p, non-zero coefficients in the expansion equation (3.3) must also be evenly distributed in cosets of K_0, i.e., for each $a \in \mathbb{Z}_p$ there is also precisely one non-zero entry in each set $\{c_{a,0}, c_{a,1}, \ldots, c_{a,p-1}\}$ and their moduli are same. This implies again for each $t \in \{1, 2, \ldots, p-1\}$ we have

$$0 = \langle \pi(tp, 0)\vec{c}, \vec{c} \rangle,$$

i.e., $P_{\vec{c}} \perp \pi(\tilde{K}_0)$. □

Lemma 3.3 *Let p be a prime number and $S \subset \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ an order p^2 subset that contains the identity element. If S has discrete Gabor spectrum $\vec{c}$, and $P_{\vec{c}} \perp \pi(\Delta K)$, then $S = K$.*

Proof Let us first show that for each k in the index set $\{0, 1, \ldots, p-1, \infty\}$, there is at least one Q_k such (K, Q_k) is a tiling pair in $K_k^{\perp}$ and

$$Q_k \subseteq \operatorname{supp}(P_{\vec{c}}). \tag{3.4}$$

Suppose not, then there must be a coset $q_k + K$ of K in $K_k^{\perp}$ such that

$$P_{\vec{c}} \perp \pi(q_k + K), \tag{3.5}$$

for otherwise if no such coset exists, then each coset intersect $\operatorname{supp}(P_{\vec{c}})$ non-trivially, and we may simply pick a member from each intersection to form Q_k.

It then follows from Eq. (3.5) that

$$\pi^*(q_k)\vec{c} \in \ker\left(G_K^*(\vec{c})\right),$$

which means that $(K, \vec{c})$ is not full rank, and contradicts the assumption that $P_{\vec{c}} \perp \pi(\Delta K)$ (which by Eq. (2.7) implies that $G_K(\vec{c})$ is orthogonal).

Now for each k in the index set $\{0, 1, \ldots, p-1, \infty\}$, pick one Q_k that satisfies Eq. (3.4), and let Q be union of all such Q_k, then Q is a tiling complement of K in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. By Lemma 2.8 we shall have

$$\Delta\widehat{Q} \subseteq Z(F_S).$$

Set

$$a_k = |S \cap \tilde{K}_k|, \quad b_{j,k} = |S \cap \tilde{H}_{j,k}|,$$

and

$$a = a_0 + a_1 + \cdots + a_{p-1} + a_\infty, \quad b_k = \sum_{j \in \mathbb{Z}_p} b_{j,k},$$

with Lemma 3.1 we then have

$$1 + a + b_k = p(1 + a_k + b_{j,k}),$$

holds for all $j \in \mathbb{Z}_p$ and all k from the index set $\{0, 1, \ldots, p-1, \infty\}$. Fix k and sum up over j we get

$$p(1 + a + b_k) = p^2 + p^2 a_k + p b_k,$$

i.e.,

$$1 + a = p(1 + a_k).$$

Sum up over k we obtain

$$p + 1 + (p + 1)a = p(p + 1) + pa,$$

i.e.,

$$a = p^2 - 1,$$

which shows $|K \cap S| = p^2 = |S|$, and thus $S = K$. □

It is possible for $\mathrm{supp}(P_{\vec{c}})$ to be not solely contained in a Lagrangian, e.g., if $n = 4$ and $\vec{c} = (1, 1, 0, 0)$, then $Z(P_{\vec{c}}) = \Delta K \cup \tilde{H}_{(1,0)} \cup \tilde{H}_{(1,\infty)}$.

4 Main results

Theorem 4.1 *Let p be a prime number and $S \subset \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ a subset of order p^2, then S has a discrete Gabor spectrum if and only if it is a discrete Gabor tile.*

Proof Without loss of generality we may assume that S contains the identity element.

The if part is already elaborated in [50, Theorem 2] but for completeness we will still include a proof (it is a simpler and clearer proof nevertheless) here. There are two cases:

If S is a Lagrangian, then by Lemma 2.9, it is possible to take a $\vec{c} \in \mathbb{C}^n$ such that $\mathcal{G}(S, \vec{c})$ forms a basis of $\mathbb{C}^n$. Consider its frame operator

$$A = G_S(\vec{c})G_S^*(\vec{c}) = nP_S P_{\vec{c}}.$$

It follows from Corollary 2.1 that P_S is the orthogonal projection onto the span of $\pi(S)$, thus A commutes with every element in $\pi(S)$, consequently we get

$$G_S(A^{-\frac{1}{2}}\vec{c}) = A^{-\frac{1}{2}}G_S(\vec{c}),$$

where it is easy to verify that the right-hand side is unitary (this is actually the unitary component in the polar decomposition of $G_S(\vec{c})$). Therefore $\mathcal{G}(S, A^{-\frac{1}{2}}\vec{c})$ is an orthonormal basis of $\mathbb{C}^n$.

Alternatively if S is the tiling complement of a Lagrangian, then suppose $H \lhd \mathbb{Z}_n \times \mathbb{Z}_n$ is a Lagrangian that S complements. Let $\vec{c}$ be a vector as in Lemma 2.7, then $P_{\vec{c}}$ is in the span of $\pi(H) = \pi(\Delta H) \cup \{\pi(0, 0)\}$, which by Eq. (2.1) is disjoint from $\pi(\Delta S)$, and further implies $P_{\vec{c}} \perp \pi(\Delta S)$. Therefore by Eq. (2.7) this means that $\mathcal{G}(S, \vec{c})$ is an orthonormal basis of $\mathbb{C}^n$.

The only if part: Suppose that $\mathcal{G}(S, \vec{c})$ is an orthonormal basis for $\mathbb{C}^n$, but S complements no cyclic Lagrangians. For each cyclic Lagrangian $H_{j,k}$, by Lemma 2.4 there are only four possibilities for $Z(F_S) \cap \widehat{H_{j,k}}$: it is either empty, or equals $\Delta\widehat{H_{j,k}}$ or equals $\widehat{\tilde{H}_{j,k}}$, or equals $\widehat{\tilde{K}_k}$. But since S complements no cyclic Lagrangians, by

Lemma 2.6 the case of $Z(F_S) \cap \widehat{H_{j,k}} = \Delta\widehat{H_{j,k}}$ shall be ruled out. By Lemma 2.8 this further implies that at least one of $\tilde{H}_{i,j}$ and $\tilde{K}_k$ is included in $Z(P_{\vec{c}})$. In particular, if

$$\tilde{K}_k \cap \operatorname{supp}(P_{\vec{c}}) \neq \emptyset,$$

then we must have

$$\tilde{H}_k \subseteq Z(P_{\vec{c}}), \tag{4.1}$$

otherwise if on the contrary there is some $\tilde{H}_{j,k}$ that is not completely included in $Z(P_{\vec{c}})$, then

$$\Delta\widehat{H_{j,k}} \subseteq Z(F_S),$$

by Lemma 2.8, which means S complements $H_{j,k}$ by Lemma 2.6 and thus contradicts the assumption that S complements no cyclic Lagrangians.

Now there are three cases:

Case 1: $\Delta K \subseteq Z(P_{\vec{c}})$. By Lemma 3.3 this means $S = K$.

Case 2: $\Delta K \subseteq \operatorname{supp}(P_{\vec{c}})$. By Lemma 2.8 this means $\Delta K \subseteq Z(F_S)$, which by Lemma 2.6 further implies that S is a tiling complement of K.

Case 3: The set $\{\tilde{K}_0, \ldots, \tilde{K}_{p-1}, \tilde{K}_\infty\}$ can be partitioned into two proper and non-empty subsets X, Y, so that $X \subseteq Z(P_{\vec{c}})$ and $Y \subseteq \operatorname{supp}(P_{\vec{c}})$. By Lemma 3.2 and Eq. (4.1) this would imply that $P_{\vec{c}} \perp \pi(\tilde{K}_k)$ for each k in the index set $\{0, 1, \ldots, p-1, \infty\}$, i.e., $Y = \emptyset$, which is a contradiction.

Thus in summary, if S is not a tiling complement of any cyclic Lagrangians, then either $S = K$ or it is a tiling complements of K. This completes the proof. □

Several colleagues have brought to the author the question that in Theorem 4.1 whether it is possible to replace the condition of S being a discrete Gabor tile to S being merely a tile of order n (i.e., as defined in Definition 1.2), as for prime n clearly these two notions coincide.

The question is twofold: for a composite number n, is a tile of order n necessarily a subgroup or complements a subgroup? If not, and if S is an order n tile that is neither a subgroup nor the tiling complement of some group, then is it still possible to have some window vector $\vec{c}$ so that $\mathcal{G}(S, \vec{c})$ is an orthonormal basis?

In general a tile need not be, or complement, or contain, or be contained in a subgroup. There are extensive researches classifying these cases, see e.g., Tijdeman properties [46] (see also [28]), periodicity and quasi-periodicity [3, 15, 39, 40] etc., or the book [42] for details. At the moment the author is unfortunately not even able to determine any of these two questions.

Data Availability Not applicable.

Declarations

Conflict of interest The author has no relevant financial or non-financial interests to disclose.

References

1. Benedetto, J., Cordwell, K., Magsino, M.: CAZAC sequences and Haagerup's characterization of cyclic n-roots. In: Aldroubi, A., Cabrelli, C., Jaffard, S., Molter, U. (eds.) New Trends in Applied Harmonic Analysis, vol. 2, pp. 1–43. Birkhäuser, Cham (2019)
2. Bhattacharya, S.: Periodicity and decidability of tilings of $\mathbb{Z}^2$. Am. J. Math. **142**, 255–266 (2020)
3. Bruijn, N.: On the factorisation of cyclic groups. Indag. Math. **17**, 370–377 (1955)
4. Coven, E., Meyerowitz, A.: Tiling the integers with translates of one finite set. J. Algebra **212**, 161–174 (1999)
5. Debernardi, A., Lev, N.: Gabor orthonormal bases, tiling and periodicity. Math. Ann. **384**(3–4), 1461–1467 (2022)
6. Dutkay, D., Lai, C.: Some reduction of the spectral set conjecture on integers. Math. Proc. Camb. Philos. Soc. **156**(1), 123–135 (2014)
7. Fallon, T., Kiss, G., Somlai, G.: Spectral sets and tiles in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$. J. Funct. Anal. **282**(12), 109472 (2022)
8. Fan, A., Fan, S., Liao, L., Shi, R.: Fuglede's conjecture holds in $\mathbb{Q}_p$. Math. Ann. **375**, 315–341 (2019)
9. Farkas, B., Matolcsi, M., Móra, P.: On Fuglede's conjecture and the existence of universal spectra. J. Fourier Anal. Appl. **12**(5), 483–494 (2006)
10. Fuglede, B.: Commuting self-adjoint partial differential operators and a group theoretic problem. J. Funct. Anal. **16**, 101–121 (1974)
11. Gabor, D.: Theory of communication part 1: the analysis of information. J. Inst. Electr. Eng. Part III: Radio Commun. Eng. **93**(26), 429–441 (1946)
12. Gabardo, J.P., Lai, C.K., Wang, Y.: Gabor orthonormal bases generated by the unit cube. J. Funct. Anal. **269**, 1515–1538 (2015)
13. Greenfeld, R., Tao, T.: The structure of translational tilings in $\mathbb{Z}^d$. Discret. Anal. **16** (2021)
14. Greenfeld, R., Tao, T.: A counterexample to the periodic tiling conjecture. Ann. Math. (2024) (**accepted**)
15. Hajós, G.: Sur le problème de factorisation des groupes cycliques. Acta Math. Acad. Sci. Hung. **1**, 189–195 (1950)
16. Iosevich, A., Kolountzakis, M.: Periodicity of the spectrum in dimension one. Anal. PDE **6**(4), 819–827 (2013)
17. Iosevich, A., Kolountzakis, M., Lyubarskii, Y., Mayeli, A., Pakianathan, J.: On Gabor orthonormal bases over finite prime fields. Bull. Lond. Math. Soc. **53**(2), 380–391 (2021)
18. Iosevich, A., Mayeli, A., Pakianathan, J.: The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$. Anal. PDE **10**(4), 757–764 (2017)
19. Kenyon, R.: Rigidity of planar tilings. Invent. Math. **107**, 637–651 (1992)
20. Kiss, G., Malikiosis, R., Somlai, G., Vizer, M.: Fuglede's conjecture holds for cyclic groups of order $pqrs$. J. Fourier Anal. Appl. **28**, 79 (2022)
21. Kolountzakis, M., Lagarias, J.: Structure of tilings of the line by a function. Duke Math. J. **82**, 653–678 (1996)
22. Kolountzakis, M., Matolcsi, M.: Complex Hadamard matrices and the spectral set conjecture. Collect. Math. **57**, 281–291 (2006)
23. Kolountzakis, M., Matolcsi, M.: Tiles with no spectra. Forum Math. **18**(3), 519–528 (2006)
24. Łaba, I.: The spectral set conjecture and multiplicative properties of roots of polynomials. J. Lond. Math. Soc. **65**(3), 661–671 (2002)
25. Łaba, I., Londner, I.: The Coven–Meyerowitz tiling conditions for 3 odd prime factors. Invent. Math. **232**, 365–470 (2022)
26. Lai, C.K., Mayeli, A.: Non-separable lattices, Gabor orthonormal bases and tilings. J. Fourier Anal. Appl. **25**(6), 3075–3103 (2019)
27. Lagarias, J., Wang, Y.: Tiling the line with translates of one tile. Invent. Math. **124**, 341–365 (1996)
28. Lagarias, I., Wang, Y.: Spectral sets and factorizations of finite Abelian groups. J. Funct. Anal. **145**, 73–98 (1997)
29. Lam, T., Leung, K.: On vanishing sums of roots of unity. J. Algebra **224**, 91–109 (2000)
30. Lawrence, J., Pfander, G., Walnut, D.: Linear independence of Gabor systems in finite dimensional vector spaces. J. Fourier Anal. Appl. **11**(6), 715–726 (2005)
31. Lev, N., Matolcsi, M.: The Fuglede conjecture for convex domains is true in all dimensions. Acta Math. **228**, 385–420 (2022)

32. Malikiosis, R.: A note on Gabor frames in finite dimensions. Appl. Comput. Harmon. Anal. **38**(2), 318–330 (2015)
33. Malikiosis, R.: On the structure of spectral and tiling subsets of cyclic groups. Forum Math. Sigma **10**, 1–42 (2022)
34. Matolcsi, M.: Fuglede's conjecture fails in dimension 4. Proc. Am. Math. Soc. **133**(10), 3021–3026 (2005)
35. McMullen, P.: Convex bodies which tile space by translations. Mathematika **27**, 113–121 (1980)
36. Pfander, G.: Gabor frames in finite dimensions. In: Casazza, P., Kutyniok, G. (eds.) Finite Frames, pp. 193–239. Springer, New York (2013)
37. Qiu, S., Feichtinger, H.: Discrete Gabor structures and optimal representations. IEEE Trans. Signal Process. **43**(10), 2258–2268 (1995)
38. Qiu, S.: Discrete Gabor transforms: the Gabor-Gram matrix approach. J. Fourier Anal. Appl. **4**(1), 1–17 (1998)
39. Sands, A.: On the factorisation of finite Abelian groups. Acta Math. Acad. Sci. Hung. **8**, 65–86 (1957)
40. Sands, A.: On the factorization of finite Abelian groups II. Acta Math. Acad. Sci. Hung. **13**, 153–159 (1962)
41. Somlai, G.: Spectral sets in $\mathbb{Z}_{p^2qr}$ tile. Discret. Anal. **5**, 10 (2023)
42. Szabó, S., Sands, A.: Factoring Groups into Subsets. CRC Press, Boca Raton (2008)
43. Shi, R.: Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$. Discret. Anal. **14** (2019)
44. Shi, R.: Equi-distribution on planes and spectral set conjecture on $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. J. Lond. Math. Soc. **102**(2), 1030–1046 (2020)
45. Tao, T.: Fuglede's conjecture is false in 5 and higher dimensions. Math. Res. Lett. **11**(2–3), 251–258 (2004)
46. Tijdeman, R.: Decomposition of the integers as a direct sum of two subsets. In: David, S. (eds) Number Theory Seminar Paris, pp. 261–276. Cambridge University Press, Cambridge (1995)
47. Venkov, B.: On a class of Euclidean polyhedra. Vestnik Leningradskogo Universiteta Seria Matematiki Fiziki Himii **9**, 11–31 (1954)
48. Zhang, T.: Fuglede's conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$. SIAM J. Discret. Math. **37**(2), 1180–1197 (2023)
49. Zhang, T.: A group ring approach to Fuglede's conjecture in cyclic groups. Combinatorica **44**, 393–416 (2024)
50. Zhou, W.: On the construction of discrete orthonormal Gabor bases on finite dimensional spaces. Appl. Comput. Harmon. Anal. **55**, 270–281 (2021)