Some Insights on Zeros of Fourier Transforms of Sets in $\mathbb{Z}_n^2$

Weiqi Zhou

2025.09

Quick facts and notations

Fourier transform:

$$\widehat{1}_A(x) = \sum_{a \in A} e^{2\pi i \langle a,x \rangle / n}, \quad A \subseteq \mathbb{Z}_n^2$$

Zero set:

$$Z(\widehat{1}_A) = \{x \in \mathbb{Z}_n^2 : \widehat{1}_A(x) = 0\}$$

Difference set:

$$\Delta A = \{a - a' : a, a' \in A, a \neq a'\}$$

Quick facts and notations

$$(A,S) \text{ is a spectral pair on } \mathbb{Z}_n^2 \quad \Leftrightarrow \quad \begin{cases} |A| = |S| \\ \Delta S \subseteq Z(\widehat{1}_A) \end{cases}$$

$$(A,B) \text{ is a tiling pair on } \mathbb{Z}_n^2 \quad \Leftrightarrow \quad \begin{cases} |A| \cdot |B| = n^2 \\ \Delta \mathbb{Z}_n^2 \subseteq Z(\widehat{1}_A) \cup Z(\widehat{1}_B) \end{cases}$$

Appetizer

Let H be a maximal cyclic subgroup in $\mathbb{Z}_n^2$ generated by h, then

$$\widehat{1}_H(x) = \sum_{k=0}^{n-1} e^{2\pi ik\langle h,x\rangle/n} = \begin{cases} 0 & \text{if } \langle h,x\rangle \neq 0, \\ n & \text{if } \langle h,x\rangle = 0, \end{cases}$$

which means

$$Z(\widehat{1}_H) = \{x \in \mathbb{Z}_n^2 : \langle h,x\rangle \neq 0\}.$$

Appetizer

Let H be a maximal cyclic subgroup in $\mathbb{Z}_n^2$ generated by h, then

$$\widehat{1}_H(x) = \sum_{k=0}^{n-1} e^{2\pi i k \langle h,x\rangle / n} = \begin{cases} 0 & \text{if } \langle h,x\rangle \neq 0, \\ n & \text{if } \langle h,x\rangle = 0, \end{cases}$$

which means

$$Z(\widehat{1}_H) = \{x \in \mathbb{Z}_n^2 : \langle h,x\rangle \neq 0\}.$$

Orthogonal set:

$$A^\perp = \{x \in \mathbb{Z}_n^2 : \langle a,x\rangle = 0,\ \forall a \in A\}.$$

Poisson summation formula (maximal cyclic subgroups)

If H is a maximal cyclic subgroup, then

$$Z(\widehat{1}_H) = \mathbb{Z}_n^2 \setminus H^\perp$$

More precisely

$$\widehat{1}_H = |H| \cdot 1_{H^\perp}$$

Poisson summation formula (maximal cyclic subgroups)

If H is a maximal cyclic subgroup, then

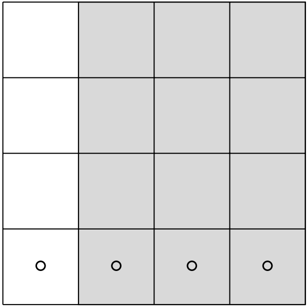
$$Z(\widehat{1}_H) = \mathbb{Z}_n^2 \setminus H^\perp$$

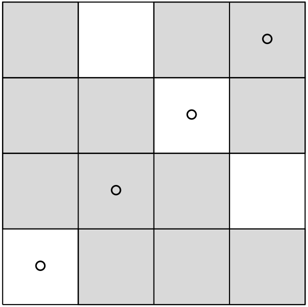
More precisely

$$\widehat{1}_H = |H| \cdot 1_{H^\perp}$$

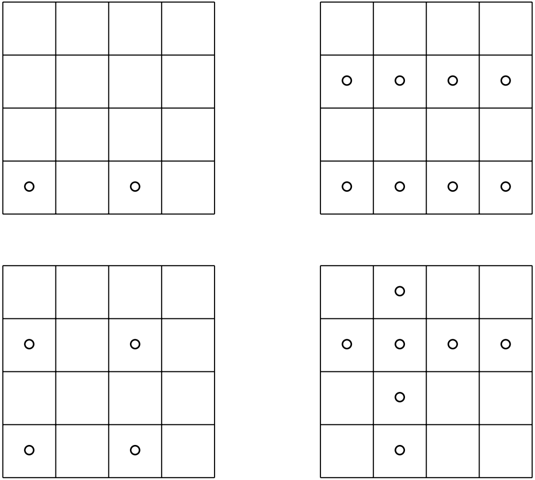
Spoiler: This actually holds for all subgroups.

Examples





How about such sets?



Basic observation

Given some A, let's consider whether $x = (k, 0)$ is in $Z(\widehat{1}_A)$:

$$\widehat{1}_A(x) = \sum_{(a_1,a_2)\in A} e^{2\pi i(a_1 \cdot k + a_2 \cdot 0)/n} = \sum_{(a_1,a_2)\in A} e^{2\pi i a_1 \cdot k/n}$$

Basic observation

Given some A, let's consider whether $x = (k, 0)$ is in $Z(\widehat{1}_A)$:

$$\widehat{1}_A(x) = \sum_{(a_1,a_2)\in A} e^{2\pi i(a_1\cdot k + a_2\cdot 0)/n} = \sum_{(a_1,a_2)\in A} e^{2\pi i a_1\cdot k/n}$$

(1) If A_1 is the multiset obtained by applying $(a_1, a_2) \mapsto (a_1, 0)$ on A, then $\widehat{1}_A(x) = \widehat{1}_{A_1}(x)$ for $x = (k, 0)$.

Basic observation

Given some A, let's consider whether $x = (k, 0)$ is in $Z(\widehat{1}_A)$:

$$\widehat{1}_A(x) = \sum_{(a_1,a_2)\in A} e^{2\pi i(a_1\cdot k + a_2\cdot 0)/n} = \sum_{(a_1,a_2)\in A} e^{2\pi i a_1\cdot k/n}$$

(1) If A_1 is the multiset obtained by applying $(a_1, a_2) \mapsto (a_1, 0)$ on A, then $\widehat{1}_A(x) = \widehat{1}_{A_1}(x)$ for $x = (k, 0)$.

(2) We may view $\sum_{(a_1,a_2)\in A} e^{2\pi i a_1\cdot k/n}$ as the univariate polynomial

$$p(z) = \sum_{(a_1,a_2)\in A} z^{a_1}$$

evaluated at $z = e^{2\pi i k/n}$.

The idea

Given some A and x, to determine whether $x \in Z(\widehat{1}_A)$, we find some x', y' so that $x \in \langle x' \rangle$, $x' \perp y'$, and x', y' generates $\mathbb{Z}_n^2$.

The idea

Given some A and x, to determine whether $x \in Z(\widehat{1}_A)$, we find some x', y' so that $x \in \langle x' \rangle$, $x' \perp y'$, and x', y' generates $\mathbb{Z}_n^2$.

x', y' is a pair of "orthogonal Euclidean basis", and if $x' = (x_1, x_2)$, then $y' = (-x_2, x_1)$.

The idea

Given some A and x, to determine whether $x \in Z(\widehat{1}_A)$, we find some x', y' so that $x \in \langle x' \rangle$, $x' \perp y'$, and x', y' generates $\mathbb{Z}_n^2$.

x', y' is a pair of "orthogonal Euclidean basis", and if $x' = (x_1, x_2)$, then $y' = (-x_2, x_1)$.

Write every element $a \in A$ into linear combinations of x', y', then repeating the same procedure we obtain

(1) $\widehat{1}_A(x)$ depends only on the projection of A into $\langle x' \rangle$;

(2) $\widehat{1}_A(x)$ can be viewed as a univariate polynomial evaluated at $z = e^{2\pi i k/n}$ where k is the value so that $x = kx'$.

Facts: disjointness of difference sets

Fact 1:

$$A + B = A \oplus B \quad \Leftrightarrow \quad \Delta A \cap \Delta B = \emptyset$$

Facts: disjointness of difference sets

Fact 1:

$$A + B = A \oplus B \quad \Leftrightarrow \quad \Delta A \cap \Delta B = \emptyset$$

Define an equivalence relation in finite Abelian groups: $h \sim h'$ if h, h' generate the same cyclic subgroup.

Fact 2: Let E be an arbitrary equivalence class under $\sim$, then $\Delta A \cap E$ and $\Delta B \cap E$ can not be both non-empty.

Facts: disjointness of difference sets

Fact 1:

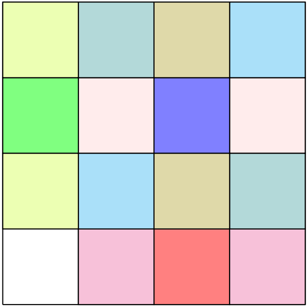
$$A + B = A \oplus B \quad \Leftrightarrow \quad \Delta A \cap \Delta B = \emptyset$$

Define an equivalence relation in finite Abelian groups: $h \sim h'$ if h, h' generate the same cyclic subgroup.

Fact 2: Let E be an arbitrary equivalence class under $\sim$, then $\Delta A \cap E$ and $\Delta B \cap E$ can not be both non-empty.

Reason(dilation trick): If $\gcd(m, |A|) = 1$ and (A, B) is a tiling pair, then (mA, B) is still a tiling pair.

Equivalence classes



Facts: a representation of $\mathbb{Z}_{p^k}$

Expand every element of $\mathbb{Z}_{p^k}$ in base p, then each element can be represented by a k-digit base p number.

Fact: Subgroups have common trailing 0s:

A subgroup of size p^t consists of all numbers whose last $k-t$ digits are 0, and its generators are of the form:

$$d_1 \ldots d_{t-1} x \underbrace{0 \ldots \ldots 0}_{k-t \text{ digits}},$$

with $x \neq 0$ and $d_1, \ldots, d_{t-1}$ arbitrary.

Quick facts and notations

Let

$$C' = \{\underbrace{0\ldots\ldots0}_{t-1 \text{ digits}} x \underbrace{0\ldots\ldots0}_{k-t \text{ digits}} : x \in \mathbb{Z}_p\},$$

then $|C'| = p$, and both $C', \Delta C'$ belong to the same equivalence class.

Quick facts and notations

Let

$$C' = \{\underbrace{0\ldots\ldots0}_{t-1\text{ digits}}x\underbrace{0\ldots\ldots0}_{k-t\text{ digits}} : x \in \mathbb{Z}_p\},$$

then $|C'| = p$, and both $C', \Delta C'$ belong to the same equivalence class.

Let E be an equivalence class in $\mathbb{Z}^2_{p^k}$, and $h \in E$.

E generates a cyclic group of some prime power order, hence if

$$E' = \{0, h, \ldots, (p-1)h\},$$

then $|E'| = p$, and both $E', \Delta E' \subseteq E$.

Quick facts

All elements in a given equivalence class are simultaneously annihilated.

Quick facts

All elements in a given equivalence class are simultaneously annihilated.

Each equivalence class E contains an size p subset E' whose difference set is still in the class.

We will construct sets of form $E_1' \oplus E_2' \oplus \ldots \oplus E_m'$ as spectra for tilings sets or tiling complements for spectral sets in $\mathbb{Z}_{p^k}^2$.

Some immediate consequences

Lemma

If $h \in Z(\widehat{1}_A)$, then $\widehat{1}_A$ annihilates the whole equivalence class of h.

Some immediate consequences

Lemma
If $h \in Z(\widehat{1}_A)$, then $\widehat{1}_A$ annihilates the whole equivalence class of h.

Lemma
If $h \in Z(\widehat{1}_A)$ and $\mathrm{ord}(h) = p^k$, then p divides $|A|$.

Some immediate consequences

Lemma

If $h \in Z(\widehat{1}_A)$, then $\widehat{1}_A$ annihilates the whole equivalence class of h.

Lemma

If $h \in Z(\widehat{1}_A)$ and $\mathrm{ord}(h) = p^k$, then p divides $|A|$.

Proposition

If $A \subset \mathbb{Z}_{p^k}^2$ is a tiling set with $|A| = p$ or p^{2k-1}, then A is spectral.

Some immediate consequences

Lemma

If $h \in Z(\widehat{1}_A)$, then $\widehat{1}_A$ annihilates the whole equivalence class of h.

Lemma

If $h \in Z(\widehat{1}_A)$ and $\mathrm{ord}(h) = p^k$, then p divides $|A|$.

Proposition

If $A \subset \mathbb{Z}_{p^k}^2$ is a tiling set with $|A| = p$ or p^{2k-1}, then A is spectral.

Proposition

If $A \subset \mathbb{Z}_{p^k}^2$ is a spectral set with $|A| \geq p^{2k-1}$, then A is tiling.

Some immediate consequences

Lemma
If $h \in Z(\widehat{1}_A)$, then $\widehat{1}_A$ annihilates the whole equivalence class of h.

Lemma
If $h \in Z(\widehat{1}_A)$ and $\mathrm{ord}(h) = p^k$, then p divides $|A|$.

Proposition
If $A \subset \mathbb{Z}_{p^k}^2$ is a tiling set with $|A| = p$ or p^{2k-1}, then A is spectral.

Proposition
If $A \subset \mathbb{Z}_{p^k}^2$ is a spectral set with $|A| \geq p^{2k-1}$, then A is tiling.

Theorem
Tiling sets and spectral sets coincide in $\mathbb{Z}_p^2$.

T⇒S: $|A| = p$ in $\mathbb{Z}_{p^k}^2$

Let (A,B) be a tiling pair in $\mathbb{Z}_{p^k}^2$ with $|A| = p$.

$Z(\widehat{1}_A) \neq \emptyset$ must hold, otherwise $Z(\widehat{1}_B)$ would contain the whole $\Delta\mathbb{Z}_{p^k}^2$.

There is some equivalence class E with $E \subseteq Z(\widehat{1}_A)$, and E' is a spectrum of A.

S⇒T: $|A| \geq p^{2k-1}$ in $\mathbb{Z}_{p^k}^2$

Let (A,S) be a spectral pair in $\mathbb{Z}_{p^k}^2$ with $|A| \geq p^{2k-1}$.

There must be some equivalence class E that is disjoint with ΔA, otherwise $Z(\widehat{1}_S)$ would contain the whole $\Delta \mathbb{Z}_{p^k}^2$.

$\Delta E' \cap \Delta A \subseteq E \cap \Delta A = \emptyset$, thus E' is a tiling complement of A.

Tiling: $|A| = p^{2k-1}$ in $\mathbb{Z}_{p^k}^2$

Let (A,B) be a tiling pair in $\mathbb{Z}_{p^k}^2$ with $|A| = p^{2k-1}$.

There must be some equivalence class E that is disjoint with ΔA, otherwise there is no place for ΔB.

There is an S with $|S| = p^{2k-1}$ and $Z(\widehat{1}_S) = \Delta\mathbb{Z}_{p^k}^2 \setminus E$.

S is essentially of form $H^\perp \oplus X'$, where H is a maximal cyclic subgroup that contains E, while X is the equivalence class of the subgroup of order $|H|/|E|$ in H. (that S takes such a form will be more evident in the symplectic setting)

The symplectic settings

Symplectic form (anti-symmetric, bilinear):

$$\langle x, y\rangle_s = x_1 y_2 - x_2 y_1 = \langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle,$$

where $x = (x_1, x_2), y = (y_1, y_2)$.

The symplectic settings

Symplectic form (anti-symmetric, bilinear):

$$\langle x,y\rangle_s = x_1y_2 - x_2y_1 = \langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle,$$

where $x = (x_1, x_2), y = (y_1, y_2)$.

Symplectic Fourier transform:

$$\widehat{1}_A^s(x) = \sum_{a\in A} e^{2\pi i \langle a,x\rangle_s/n}, \quad A \subseteq \mathbb{Z}_n^2$$

The symplectic settings

Symplectic form (anti-symmetric, bilinear):

$$\langle x,y\rangle_s = x_1y_2 - x_2y_1 = \langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle,$$

where $x = (x_1, x_2), y = (y_1, y_2)$.

Symplectic Fourier transform:

$$\widehat{1}_A^s(x) = \sum_{a\in A} e^{2\pi i \langle a,x\rangle_s/n}, \quad A \subseteq \mathbb{Z}_n^2$$

$Z(\widehat{1}_A^s)$ is the 90 degree rotation (a bijection) of $Z(\widehat{1}_A)$.

The symplectic settings

Symplectic form (anti-symmetric, bilinear):

$$\langle x, y\rangle_s = x_1 y_2 - x_2 y_1 = \langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle,$$

where $x = (x_1, x_2), y = (y_1, y_2)$.

Symplectic Fourier transform:

$$\widehat{1}_A^s(x) = \sum_{a \in A} e^{2\pi i \langle a, x\rangle_s / n}, \quad A \subseteq \mathbb{Z}_n^2$$

$Z(\widehat{1}_A^s)$ is the 90 degree rotation (a bijection) of $Z(\widehat{1}_A)$.

Remark: The Fourier transform incurs a 90 degree rotation on the time-frequency plane, the rotation matrix is the symplectic matrix.

Appetizer revisited

Let H be a cyclic subgroup in $\mathbb{Z}_n^2$ generated by h, then

$$\widehat{1}_H^s(x) = \sum_{k=0}^{n-1} e^{2\pi ik\langle h,x\rangle_s/n} = \begin{cases} 0 & \text{if } \langle h,x\rangle_s \neq 0, \\ n & \text{if } \langle h,x\rangle_s = 0, \end{cases}$$

thus

$$Z(\widehat{1}_H^s) = \{x \in \mathbb{Z}_n^2 : \langle h,x\rangle_s \neq 0\}.$$

Appetizer revisited

Let H be a cyclic subgroup in $\mathbb{Z}_n^2$ generated by h, then

$$\widehat{1}_H^s(x) = \sum_{k=0}^{n-1} e^{2\pi i k \langle h,x\rangle_s/n} = \begin{cases} 0 & \text{if } \langle h,x\rangle_s \neq 0, \\ n & \text{if } \langle h,x\rangle_s = 0, \end{cases}$$

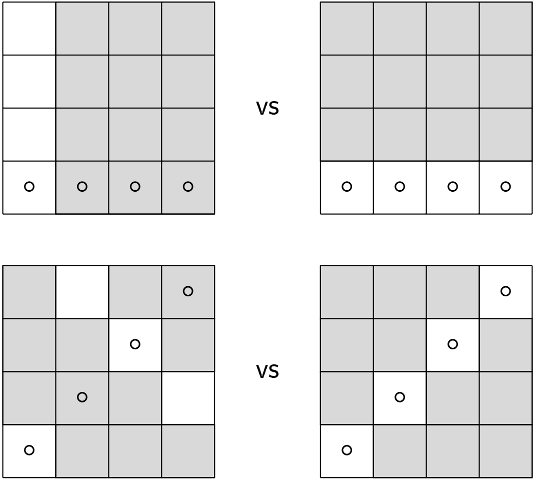
thus

$$Z(\widehat{1}_H^s) = \{x \in \mathbb{Z}_n^2 : \langle h,x\rangle_s \neq 0\}.$$

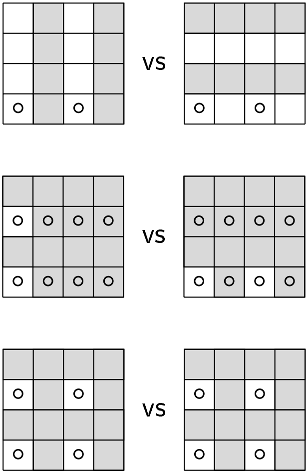
Symplectic orthogonal sets:

$$H^{\perp_s} = \{x \in \mathbb{Z}_n^2 : \langle h,x\rangle_s = 0\}.$$

Examples



More examples



Characterizing orthogonal sets

$A^{\perp}$ and $A^{\perp_s}$ are always subgroups. If $ab = n$, then

$$(a\mathbb{Z}_b \times \mathbb{Z}_n)^{\perp} = b\mathbb{Z}_a \times \{0\}, \quad (a\mathbb{Z}_b \times \mathbb{Z}_n)^{\perp_s} = \{0\} \times b\mathbb{Z}_a.$$

Characterizing orthogonal sets

$A^\perp$ and $A^{\perp_s}$ are always subgroups. If $ab = n$, then

$$(a\mathbb{Z}_b \times \mathbb{Z}_n)^\perp = b\mathbb{Z}_a \times \{0\}, \quad (a\mathbb{Z}_b \times \mathbb{Z}_n)^{\perp_s} = \{0\} \times b\mathbb{Z}_a.$$

Fact 1: A set complements a subgroup H in $\mathbb{Z}_n^2$ if and only if its size is $n^2/|H|$ and it annihilates $H^\perp$ (in the Euclidean setting) or $H^{\perp_s}$ (in the symplectic setting).

Fact 2: H is an order n subgroup in $\mathbb{Z}_n^2$ if and only if $H = H^{\perp_s}$.

Fact 3: Poisson summation formula: If H is a subgroup, then

$$\widehat{1}_H^s = |H| \cdot 1_{H^{\perp_s}}$$

Strategy and motivation revisited

To determine whether $h \in Z(\widehat{1}_A)$ or $Z(\widehat{1}^s_A)$, first we view the group as generated by linear combinations of x', y', where $h \perp y'$ or $h \perp_s y'$.

Strategy and motivation revisited

To determine whether $h \in Z(\widehat{1}_A)$ or $Z(\widehat{1}^s_A)$, first we view the group as generated by linear combinations of x', y', where $h \perp y'$ or $h \perp_s y'$.

Next we project A to $\langle x' \rangle$, and view the result as a univariate polynomial evaluated at some point, the polynomial can then be factorized.

Strategy and motivation revisited

To determine whether $h \in Z(\widehat{1}_A)$ or $Z(\widehat{1}^s_A)$, first we view the group as generated by linear combinations of x', y', where $h \perp y'$ or $h \perp_s y'$.

Next we project A to $\langle x' \rangle$, and view the result as a univariate polynomial evaluated at some point, the polynomial can then be factorized.

Direct computation is often complicated, ideally we shall find a map that preserves $\langle \cdot, \cdot \rangle$ or $\langle \cdot, \cdot \rangle_s$ (preserves tilingness and spectrality), and can send orthogonal basis to standard basis.

The Euclidean case

Let us inspect whether this is possible for $\langle \cdot, \cdot \rangle$:

The Euclidean case

Let us inspect whether this is possible for $\langle \cdot, \cdot \rangle$:

Suppose x, y generate $\mathbb{Z}_n^2$ and $x \perp y$:

(1) If $\langle Ua, Ub \rangle = \langle a, b \rangle$ holds for all a, b, then $UU^* = I$.

(2) If $Ux = (1,0)^T, Uy = (0,1)^T$, then $U\begin{pmatrix} x & y \end{pmatrix} = I$, hence $U = \begin{pmatrix} x^T \\ y^T \end{pmatrix}$ and $x_1 \cdot x_1 + x_2 \cdot x_2 = y_1 \cdot y_1 + y_2 \cdot y_2 = 1$.

The Euclidean case

Let us inspect whether this is possible for $\langle \cdot, \cdot \rangle$:

Suppose x, y generate $\mathbb{Z}_n^2$ and $x \perp y$:

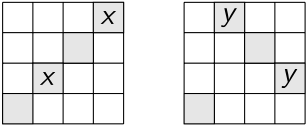
(1) If $\langle Ua, Ub \rangle = \langle a, b \rangle$ holds for all a, b, then $UU^* = I$.

(2) If $Ux = (1,0)^T, Uy = (0,1)^T$, then $U\begin{pmatrix} x & y \end{pmatrix} = I$, hence $U = \begin{pmatrix} x^T \\ y^T \end{pmatrix}$
and $x_1 \cdot x_1 + x_2 \cdot x_2 = y_1 \cdot y_1 + y_2 \cdot y_2 = 1$.

Conclusion: NOT always possible in $\mathbb{Z}_n^2$.

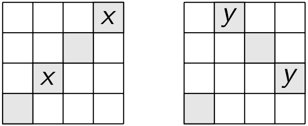
Example

No such U exists for orthogonal pairs from $\{(0,0),(1,1),(2,2),(3,3)\}$ and $\{(0,0),(1,3),(2,2),(3,1)\}$:



Example

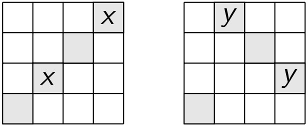
No such U exists for orthogonal pairs from $\{(0,0),(1,1),(2,2),(3,3)\}$ and $\{(0,0),(1,3),(2,2),(3,1)\}$:



$$1\cdot 1+1\cdot 1=3\cdot 3+3\cdot 3=1\cdot 1+3\cdot 3=2 \pmod 4.$$

Example

No such U exists for orthogonal pairs from $\{(0,0),(1,1),(2,2),(3,3)\}$ and $\{(0,0),(1,3),(2,2),(3,1)\}$:



$$1 \cdot 1 + 1 \cdot 1 = 3 \cdot 3 + 3 \cdot 3 = 1 \cdot 1 + 3 \cdot 3 = 2 \pmod 4.$$

For $x = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $y = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$, the candidate U should be $2^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}$, but 2 is not multiplicatively invertible in $\mathbb{Z}_4$.

Symplectic bases

Fact: If $\langle h, h' \rangle_s = d$ and $\gcd(d, n) = 1$, then h, h' generate $\mathbb{Z}_n^2$.

Symplectic bases

Fact: If $\langle h, h' \rangle_s = d$ and $\gcd(d, n) = 1$, then h, h' generate $\mathbb{Z}_n^2$.

If $d = 1$, then h, h' is a pair of symplectic basis.

Fact: Symplectic basis exists in any pair of generating maximal cyclic subgroups.

Symplectic bases

Fact: If $\langle h, h' \rangle_s = d$ and $\gcd(d, n) = 1$, then h, h' generate $\mathbb{Z}_n^2$.

If $d = 1$, then h, h' is a pair of symplectic basis.

Fact: Symplectic basis exists in any pair of generating maximal cyclic subgroups.

Fact: Symplectic form is preserved on change of bases.

If $x = x_1 h + x_2 h', y = y_1 h + y_2 h'$, then

$$\begin{aligned} \langle x, y \rangle_s &= x_1 y_1 \langle h, h \rangle_s + x_1 y_2 \langle h, h' \rangle_s + x_2 y_1 \langle h', h \rangle_s + x_2 y_2 \langle h', h' \rangle_s \\ &= x_1 y_2 - x_2 y_1 \end{aligned}$$

Symplectomorphisms

Symplectomorphism: change of symplectic bases

Fact: On $\mathbb{Z}_n^2$ they are 2×2 matrices with $\det = 1$.

Symplectomorphisms

Symplectomorphism: change of symplectic bases

Fact: On $\mathbb{Z}_n^2$ they are 2×2 matrices with $\det = 1$.

(1) Unit determinant matrices preserve the symplectic form:

If $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, then $\langle x, y \rangle_s = \langle x, Sy \rangle$, and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $A^* SA = S$ if and only if $ad - bc = 1$.

Symplectomorphisms

Symplectomorphism: change of symplectic bases

Fact: On $\mathbb{Z}_n^2$ they are 2×2 matrices with $\det = 1$.

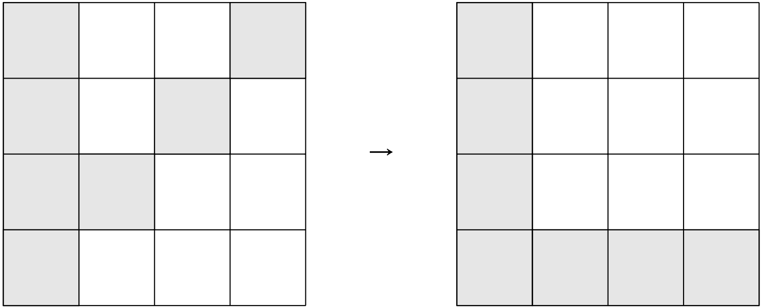
(1) Unit determinant matrices preserve the symplectic form:

If $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, then $\langle x, y \rangle_s = \langle x, Sy \rangle$, and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $A^* SA = S$ if and only if $ad - bc = 1$.

(2) Matrices formed by symplectic basis have unit determinant:

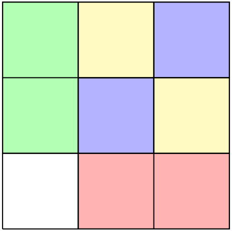
$$\langle x, y \rangle_s = x_1 y_2 - x_2 y_1 = \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

Example



Any pair of generating maximal cyclic groups would work, they don't have to be orthogonal to each other in the Euclidean sense.

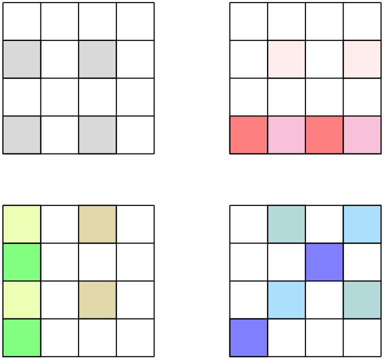
Structures of $\mathbb{Z}_p^2$



The group dissects into maximal cyclic subgroups that mutually intersect trivially.

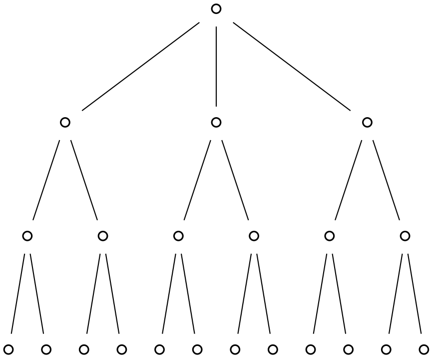
There are $p+1$ such subgroups, each subgroup forms a line.

Structures of $\mathbb{Z}_{p^2}^2$



For every order p cyclic subgroup H, there are precisely p maximal cyclic subgroups that intersect at H.

Structures of $\mathbb{Z}_{p^k}^2$



...

Each path from the root is a chain of cyclic subgroups by inclusion.

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Theorem

Tiling sets are also spectral in $\mathbb{Z}_{p^2}^2$.

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Theorem

Tiling sets are also spectral in $\mathbb{Z}_{p^2}^2$*.*

Suffices to consider tiling sets of size p^2. Let (A, B) be such a pair.

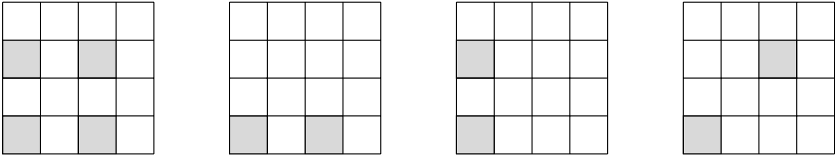
$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Theorem

Tiling sets are also spectral in $\mathbb{Z}_{p^2}^2$.

Suffices to consider tiling sets of size p^2. Let (A, B) be such a pair.

Denote and distinguish order p subgroups by their "slopes":



K $\quad$ K_0 $\quad$ K_∞ $\quad$ K_1

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Let $M = \{i : \Delta K_i \subseteq Z(\widehat{1}_A^s)\}$ and $M' = \{i : \Delta K_i \cap Z(\widehat{1}_A^s) = \emptyset\}$

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Let $M = \{i : \Delta K_i \subseteq Z(\widehat{1}_A^s)\}$ and $M' = \{i : \Delta K_i \cap Z(\widehat{1}_A^s) = \emptyset\}$

(1) If $|M| = p+1$, then $\Delta K \subseteq Z(\widehat{1}_A^s)$, and (A, K) is spectral.

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Let $M = \{i : \Delta K_i \subseteq Z(\widehat{1}_A^s)\}$ and $M' = \{i : \Delta K_i \cap Z(\widehat{1}_A^s) = \emptyset\}$

(1) If $|M| = p+1$, then $\Delta K \subseteq Z(\widehat{1}_A^s)$, and (A, K) is spectral.

(2) If $|M| = 0$, then $\Delta K \subseteq Z(\widehat{1}_B^s)$, hence B complements K, which implies $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$. Therefore $\Delta B \subseteq Z(\widehat{1}_A^s)$, then (A, B) is spectral. (Mutual Annihilation)

$T \Rightarrow S$ in $\mathbb{Z}_{p^2}^2$

Let $M = \{i : \Delta K_i \subseteq Z(\widehat{1}_A^s)\}$ and $M' = \{i : \Delta K_i \cap Z(\widehat{1}_A^s) = \emptyset\}$

(1) If $|M| = p+1$, then $\Delta K \subseteq Z(\widehat{1}_A^s)$, and (A,K) is spectral.

(2) If $|M| = 0$, then $\Delta K \subseteq Z(\widehat{1}_B^s)$, hence B complements K, which implies $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$. Therefore $\Delta B \subseteq Z(\widehat{1}_A^s)$, then (A,B) is spectral. (Mutual Annihilation)

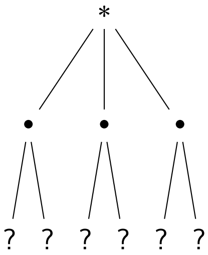
(3) If $0 < |M| < p+1$, then depending on the status of leaf nodes:

(3.1) A annihilates a maximal path;

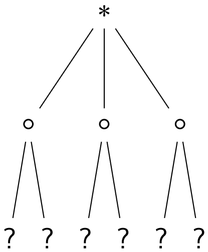
(3.2) A annihilates a full sub-branch of some $m' \in M'$;

(3.3) No other cases possible.

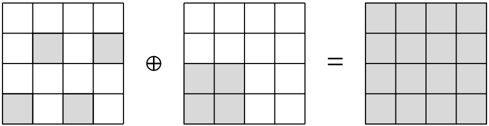
T2S case (1)



T2S case (2)



That B complementing K does not mean A is K, an example:



(Not K) (Complements K)

A counting lemma

Lemma

If $x \in Z(\widehat{1}^s_A)$, *and* $\operatorname{ord}(x) = p$ *is a prime power, then*

$$|A \cap \langle px \rangle^{\perp_s}| = p \cdot |A \cap \langle x \rangle^{\perp_s}|$$

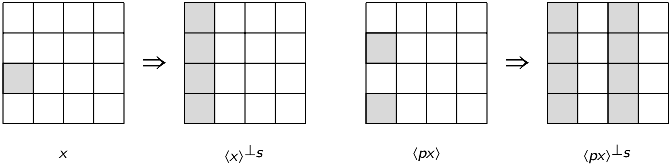
A counting lemma

Lemma

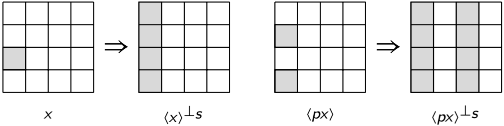
If $x \in Z(\widehat{1}^s_A)$, *and* $\mathrm{ord}(x) = p$ *is a prime power, then*

$$|A \cap \langle px \rangle^{\perp_s}| = p \cdot |A \cap \langle x \rangle^{\perp_s}|$$

For illustration purpose, let's say $x = (0,1)$:



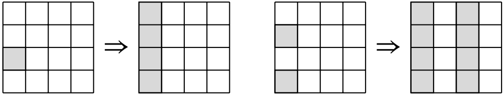
A counting lemma



Let $\omega = e^{2\pi i/p^2}, P(z) = \sum_{(a_1,a_2)\in A} z^{a_1}$, then

$$\widehat{1}_A^s(x) = \sum_{(a_1,a_2)\in A} e^{2\pi i(a_1 \cdot 1 - a_2 \cdot 0)/p^2} = \sum_{(a_1,a_2)\in A} \omega^{a_1} = P(\omega).$$

A counting lemma



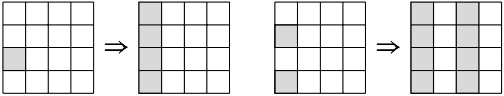
Let $\omega = e^{2\pi i/p^2}, P(z) = \sum_{(a_1,a_2)\in A} z^{a_1}$, then

$$\widehat{1}^s_A(x) = \sum_{(a_1,a_2)\in A} e^{2\pi i(a_1\cdot 1 - a_2\cdot 0)/p^2} = \sum_{(a_1,a_2)\in A} \omega^{a_1} = P(\omega).$$

If $x \in Z(\widehat{1}^s_A)$, then $P(\omega) = 0$, which means $P(z)$ is divisible by the p^2-th cyclotomic polynomial, hence

$$P(\omega) = (1 + \omega^p + \ldots + \omega^{p(p-1)})(c_0 + c_1\omega + \ldots + c_{p-1}\omega^{p-1}).$$

A counting lemma

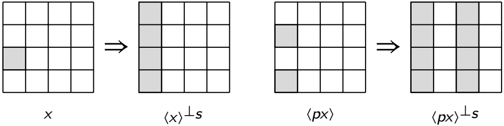


x $\quad \langle x \rangle^{\perp_s}$ $\quad \langle px \rangle$ $\quad \langle px \rangle^{\perp_s}$

$$\widehat{1}_A^s(x) = \sum_{a \in A} \omega^{\langle a,x \rangle_s} = \sum_{(a_1,a_2) \in A} \omega^{a_1}$$

$$= (1 + \omega^p + \ldots + \omega^{p(p-1)})(c_0 + c_1\omega + \ldots + c_{p-1}\omega^{p-1}).$$

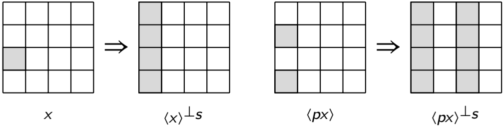
A counting lemma



$$\widehat{1}_A^s(x) = \sum_{a\in A} \omega^{\langle a,x\rangle_s} = \sum_{(a_1,a_2)\in A} \omega^{a_1}$$
$$= (1+\omega^p+\ldots+\omega^{p(p-1)})(c_0+c_1\omega+\ldots+c_{p-1}\omega^{p-1}).$$

$c_0 = |A \cap \langle x\rangle^{\perp_s}|$

A counting lemma



$$\widehat{1}_A^s(x) = \sum_{a \in A} \omega^{\langle a,x\rangle_s} = \sum_{(a_1,a_2)\in A} \omega^{a_1}$$

$$= (1 + \omega^p + \ldots + \omega^{p(p-1)})(c_0 + c_1\omega + \ldots + c_{p-1}\omega^{p-1}).$$

$c_0 = |A \cap \langle x\rangle^{\perp_s}|$

pc_0 =sum of coefficients in front of $1, \omega^p, \ldots, \omega^{p(p-1)} = |A \cap \langle px\rangle^{\perp_s}|$

Mutual annihilation

Lemma
If B complements K, then $\Delta B \cap Z(\widehat{1}^s_B) = \emptyset$.

Mutual annihilation

Lemma

If B complements K, then $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$.

Suffices to show $B \cap Z(\widehat{1}_B^s) = \emptyset$, otherwise if $b - b' \in \Delta B \cap Z(\widehat{1}_B^s)$, then consider equivalently $B - b'$. Similarly $0 \in B$ can be assumed.

Mutual annihilation

Lemma

If B complements K, then $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$.

Suffices to show $B \cap Z(\widehat{1}_B^s) = \emptyset$, otherwise if $b - b' \in \Delta B \cap Z(\widehat{1}_B^s)$, then consider equivalently $B - b'$. Similarly $0 \in B$ can be assumed.

Suppose $b \in B \cap Z(\widehat{1}_B^s)$, then $|B \cap \langle b \rangle| \geq 2$, hence $|B \cap \langle bp \rangle^{\perp_s}| \geq 2p$.

Mutual annihilation

Lemma
If B complements K, then $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$.

Suffices to show $B \cap Z(\widehat{1}_B^s) = \emptyset$, otherwise if $b - b' \in \Delta B \cap Z(\widehat{1}_B^s)$, then consider equivalently $B - b'$. Similarly $0 \in B$ can be assumed.

Suppose $b \in B \cap Z(\widehat{1}_B^s)$, then $|B \cap \langle b \rangle| \geq 2$, hence $|B \cap \langle bp \rangle^{\perp_s}| \geq 2p$.

Fact: B complements $K \quad \Rightarrow \quad \mathrm{ord}(b) = p^2 \quad \Rightarrow \quad |B \cap \langle bp \rangle^{\perp_s}| = p$.

Mutual annihilation

Lemma

If B complements K, then $\Delta B \cap Z(\widehat{1}_B^s) = \emptyset$.

Suffices to show $B \cap Z(\widehat{1}_B^s) = \emptyset$, otherwise if $b - b' \in \Delta B \cap Z(\widehat{1}_B^s)$, then consider equivalently $B - b'$. Similarly $0 \in B$ can be assumed.

Suppose $b \in B \cap Z(\widehat{1}_B^s)$, then $|B \cap \langle b \rangle| \geq 2$, hence $|B \cap \langle bp \rangle^{\perp_s}| \geq 2p$.

Fact: B complements $K \quad \Rightarrow \quad \mathrm{ord}(b) = p^2 \quad \Rightarrow \quad |B \cap \langle bp \rangle^{\perp_s}| = p$.

W.L.O.G., take $b = (0,1)$, then $\langle bp \rangle^{\perp_s} = \{(u,v) : u \bmod p = 0\}$, $B = \{\kappa_{x,y} + (x,y)\}$ with $\kappa_{x,y} \in K$ and x, y ranging from 0 to $p-1$.

Mutual annihilation

Lemma

If B complements K, then $\Delta B \cap Z(\widehat{1}^s_B) = \emptyset$.

Suffices to show $B \cap Z(\widehat{1}^s_B) = \emptyset$, otherwise if $b - b' \in \Delta B \cap Z(\widehat{1}^s_B)$, then consider equivalently $B - b'$. Similarly $0 \in B$ can be assumed.

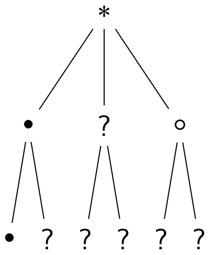
Suppose $b \in B \cap Z(\widehat{1}^s_B)$, then $|B \cap \langle b \rangle| \geq 2$, hence $|B \cap \langle bp \rangle^{\perp_s}| \geq 2p$.

Fact: B complements $K \quad \Rightarrow \quad \mathrm{ord}(b) = p^2 \quad \Rightarrow \quad |B \cap \langle bp \rangle^{\perp_s}| = p$.

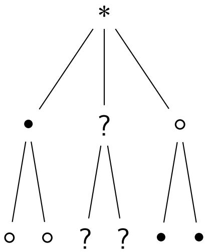
W.L.O.G., take $b = (0,1)$, then $\langle bp \rangle^{\perp_s} = \{(u,v) : u \bmod p = 0\}$,
$B = \{\kappa_{x,y} + (x,y)\}$ with $\kappa_{x,y} \in K$ and x, y ranging from 0 to $p-1$.

$|B \cap \langle bp \rangle^{\perp_s}| = |\{\kappa_{0,y} + (0,y)\}| = p$.

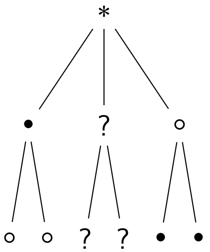
T2S case (3.1)

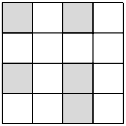


T2S case (3.2)

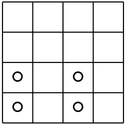


T2S case (3.2)

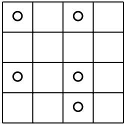




(in $Z(\widehat{1}^{s}_{A})$)

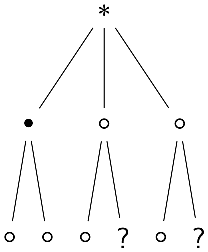


$S = \{(0,0),(0,1)\} \oplus \{(0,0),(2,0)\}$

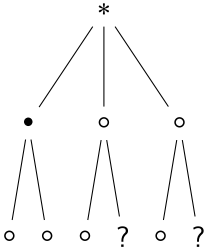


$\Delta S = \Delta E' \oplus \Delta K_0$

T2S case (3.3)

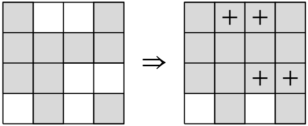


T2S case (3.3)



B has to annihilate the white nodes, which implies that

B annihilates $\mathbb{Z}_{p^2} \setminus K$ and all ΔK_i for i in M', it has too many zeros!



(in $Z(\hat{1}^s_B)$) (in $Z(\hat{1}^s_B)$)

A form of uncertainty principle

Fact: A set can not annihilate (the difference of) a larger subgroup.

A form of uncertainty principle

Fact: A set can not annihilate (the difference of) a larger subgroup.

Suppose $\Delta H \subseteq Z(\widehat{1}^s_A)$ where H is a subgroup and $|H| > |A|$.

A form of uncertainty principle

Fact: A set can not annihilate (the difference of) a larger subgroup.

Suppose $\Delta H \subseteq Z(\widehat{1}_A^s)$ where H is a subgroup and $|H| > |A|$.

Then $\Delta \mathbb{Z}_n^2 \subseteq Z(\widehat{1}_A^s \cdot \widehat{1}_{H^{\perp_s}}^s)$,

A form of uncertainty principle

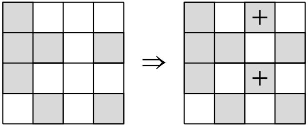
Fact: A set can not annihilate (the difference of) a larger subgroup.

Suppose $\Delta H \subseteq Z(\widehat{1}_A^s)$ where H is a subgroup and $|H| > |A|$.

Then $\Delta \mathbb{Z}_n^2 \subseteq Z(\widehat{1}_A^s \cdot \widehat{1}_{H^{\perp_s}}^s)$,

which means $|A| \geq n^2/|H^{\perp_s}| = |H| > |A|$.

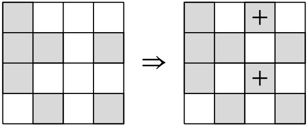
Excessive zeros



(in $Z(\widehat{1}^s_B)$) (in $Z(\widehat{1}^s_B)$)

$$\Delta\big(\{0\} \times \mathbb{Z}_{p^2}\big) \subseteq Z\big(\widehat{1}^s_B\big) \text{ implies } B = \{(0, b_0), \ldots, (p^2 - 1, b_{p^2-1})\}.$$

Excessive zeros

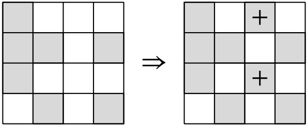


(in $Z(\widehat{1}_B^s)$) (in $Z(\widehat{1}_B^s)$)

$\Delta(\{0\} \times \mathbb{Z}_{p^2}) \subseteq Z(\widehat{1}_B^s)$ implies $B = \{(0, b_0), \ldots, (p^2 - 1, b_{p^2-1})\}$.

Set $B_m = \{(kp+m, b_{kp+m}) : k = 0, \ldots, p-1\}$, $u_m = \sum_{k=0}^{p-1} e^{2\pi i b_{kp+m}/p^2}$.

Excessive zeros



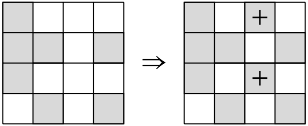
(in $Z(\widehat{1}_B^s)$) (in $Z(\widehat{1}_B^s)$)

$$\Delta(\{0\}\times\mathbb{Z}_{p^2})\subseteq Z(\widehat{1}_B^s) \text{ implies } B=\{(0,b_0),\dots,(p^2-1,b_{p^2-1})\}.$$

$$\text{Set } B_m=\{(kp+m,b_{kp+m}):k=0,\dots,p-1\},\ u_m=\sum_{k=0}^{p-1}e^{2\pi i b_{kp+m}/p^2}.$$

$$K_0^\perp\setminus K\subseteq Z(\widehat{1}_B^s) \text{ implies } Fu=0.$$ $F: p\times p$ Fourier matrix, $u=(u_0,\dots,u_{p-1})^T$.

Excessive zeros



(in $Z(\hat{1}_B^s)$) (in $Z(\hat{1}_B^s)$)

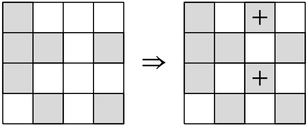
$\Delta(\{0\}\times\mathbb{Z}_{p^2})\subseteq Z(\widehat{1}_B^s)$ implies $B=\{(0,b_0),\ldots,(p^2-1,b_{p^2-1})\}$.

Set $B_m=\{(kp+m,b_{kp+m}):k=0,\ldots,p-1\}$, $u_m=\sum_{k=0}^{p-1}e^{2\pi i b_{kp+m}/p^2}$.

$K_0^{\perp}\setminus K\subseteq Z(\widehat{1}_B^s)$ implies $Fu=0$. $F: p\times p$ Fourier matrix, $u=(u_0,\ldots,u_{p-1})^T$.

Thus $u=0$, consequently for each fixed m, $\{b_{kp+m}\}_{k=0}^{p-1}=\{kp\}_{k=0}^{p-1}$.

Excessive zeros



$\Delta(\{0\}\times\mathbb{Z}_{p^2}) \subseteq Z(\widehat{1}^s_B)$ implies $B=\{(0,b_0),\ldots,(p^2-1,b_{p^2-1})\}$.

Set $B_m=\{(kp+m,b_{kp+m}):k=0,\ldots,p-1\}$, $u_m=\sum_{k=0}^{p-1} e^{2\pi i b_{kp+m}/p^2}$.

$K_0^{\perp}\setminus K \subseteq Z(\widehat{1}^s_B)$ implies $Fu=0$. $F: p\times p$ Fourier matrix, $u=(u_0,\ldots,u_{p-1})^T$.

Thus $u=0$, consequently for each fixed m, $\{b_{kp+m}\}_{k=0}^{p-1}=\{kp\}_{k=0}^{p-1}$.

If $x=(p,1)$, then $\widehat{1}^s_B(x)=\sum_{k=0}^{p^2-1} e^{2\pi i k/p^2}=0$ (since $pb_{kp+m}=0 \bmod p^2$).

$S \Rightarrow T$ in $\mathbb{Z}_{p^2}^2$

Theorem

Spectral sets are also tiling in $\mathbb{Z}_{p^2}^2$.

$S \Rightarrow T$ in $\mathbb{Z}_{p^2}^2$

Theorem

Spectral sets are also tiling in $\mathbb{Z}_{p^2}^2$.

Let (A, S) be a spectral pair, both containing the identity.

$S \Rightarrow T$ in $\mathbb{Z}_{p^2}^2$

Theorem

Spectral sets are also tiling in $\mathbb{Z}_{p^2}^2$.

Let (A, S) be a spectral pair, both containing the identity.

Suffices to consider $p^2 \leq |A| < p^3$ and $p \leq |A| < p^2$.

$S \Rightarrow T$ in $\mathbb{Z}_{p^2}^2$

Theorem
Spectral sets are also tiling in $\mathbb{Z}_{p^2}^2$.

Let (A,S) be a spectral pair, both containing the identity.

Suffices to consider $p^2 \leq |A| < p^3$ and $p \leq |A| < p^2$.

The aim is to produce a B so that $\Delta A \cap \Delta B = \emptyset$, and $|B| = p^2$ or p^3 respectively.

$S2T : p^2 \leq |A| < p^3$

(1) There is some B satisfying $\Delta A \cap \Delta B = \emptyset$, and B either is or complements an order p^2 subgroup.

$S2T : p^2 \leq |A| < p^3$

(1) There is some B satisfying $\Delta A \cap \Delta B = \emptyset$, and B either is or complements an order p^2 subgroup.

(2) ΔA intersects each order p^2 subgroup (i.e., K and each maximal cyclic subgroup) non-trivially.

Consider $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

$S2T: p^2 \leq |A| < p^3$

(1) There is some B satisfying $\Delta A \cap \Delta B = \emptyset$, and B either is or complements an order p^2 subgroup.

(2) ΔA intersects each order p^2 subgroup (i.e., K and each maximal cyclic subgroup) non-trivially.

Consider $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

If $m' \in M'$, and $H' = E \cup K_{m'}$ is a maximal cyclic subgroup,

then $E \cap \Delta A \neq \emptyset$ (since $\Delta A \cap \Delta H$ has to be non-empty).

$S2T : p^2 \leq |A| < p^3$

(1) There is some B satisfying $\Delta A \cap \Delta B = \emptyset$, and B either is or complements an order p^2 subgroup.

(2) ΔA intersects each order p^2 subgroup (i.e., K and each maximal cyclic subgroup) non-trivially.

Consider $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

If $m' \in M'$, and $H' = E \cup K_{m'}$ is a maximal cyclic subgroup,

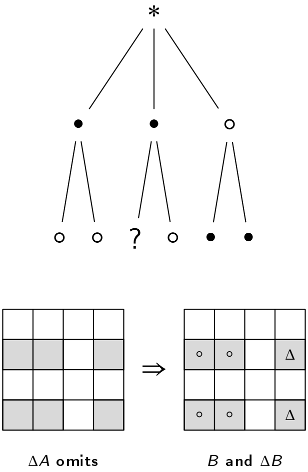
then $E \cap \Delta A \neq \emptyset$ (since $\Delta A \cap \Delta H$ has to be non-empty).

(2.1) $|M'| > 0$, $\exists m \in M$ with empty leaf: complements some $K_i \oplus E'$.

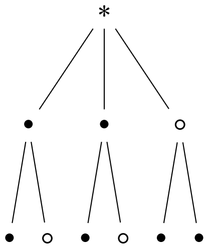
(2.2) $|M'| > 0$, no branch of M has empty leaf: impossible.

(2.3) $|M'| = 0$: S is a tiling complement of K, mutual annihilation.

$S2T : p^2 \leq |A| < p^3$ case (2.1)

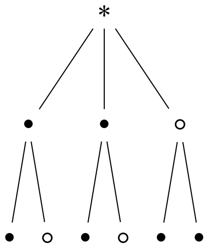


$S2T : p^2 \leq |A| < p^3$ case (2.2)



More complicated than the T2S (3.3) excessive zero case, since $|S| \geq p^2$ instead of $= p^2$.

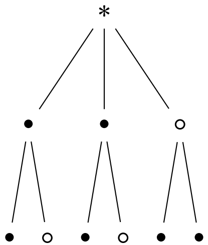
$S2T : p^2 \leq |A| < p^3$ case (2.2)



More complicated than the T2S (3.3) excessive zero case, since $|S| \geq p^2$ instead of $= p^2$.

On the other hand, $\widehat{1}_S^s$ has more zeros than in the setting of the excessive zero case.

$S2T : p^2 \leq |A| < p^3$ case (2.2)

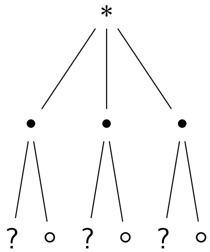


More complicated than the T2S (3.3) excessive zero case, since $|S| \geq p^2$ instead of $= p^2$.

On the other hand, $\widehat{1}_S^s$ has more zeros than in the setting of the excessive zero case.

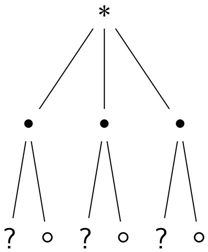
This puts more restrictions on it and leads to a contradiction by counting.

$S2T : p^2 \leq |A| < p^3$ case (2.3)



For each K_i, there shall be some maximal cyclic subgroup H_i so that $\Delta A \cap \Delta H_i \subseteq K_i$, otherwise $\Delta K_i^{\perp_s} \subseteq Z(\widehat{1}_S^s)$ (violates uncertainty).

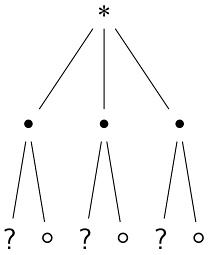
$S2T : p^2 \leq |A| < p^3$ case (2.3)



For each K_i, there shall be some maximal cyclic subgroup H_i so that $\Delta A \cap \Delta H_i \subseteq K_i$, otherwise $\Delta K_i^{\perp_s} \subseteq Z(\widehat{1}_S^s)$ (violates uncertainty).

If S falls into (2.1) or (2.2), then $|A| = |S| = p^2$, which leads to mutual annihilation.

$S2T : p^2 \leq |A| < p^3$ case (2.3)



For each K_i, there shall be some maximal cyclic subgroup H_i so that $\Delta A \cap \Delta H_i \subseteq K_i$, otherwise $\Delta K_i^{\perp_s} \subseteq Z(\widehat{1}_S^s)$ (violates uncertainty).

If S falls into (2.1) or (2.2), then $|A| = |S| = p^2$, which leads to mutual annihilation.

Otherwise both ΔA and ΔS comply with the above tree and will lead to a contradiction by counting as in (2.2).

$S2T : p \leq |A| < p^2$

Consider again $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

$S2T : p \leq |A| < p^2$

Consider again $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

M' is not empty, otherwise S annihilates K (subgroup of larger size).

$S2T: p \le |A| < p^2$

Consider again $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

M' is not empty, otherwise S annihilates K (subgroup of larger size).

Similarly if $H = E \cup K_i$ is a maximal cyclic subgroup, then ΔA can not intersect both E and K_i.

$S2T : p \leq |A| < p^2$

Consider again $M = \{i : \Delta K_i \cap \Delta A \neq \emptyset\}$ and $M' = \{i : \Delta K_i \cap \Delta A = \emptyset)\}$.

M' is not empty, otherwise S annihilates K (subgroup of larger size).

Similarly if $H = E \cup K_i$ is a maximal cyclic subgroup, then ΔA can not intersect both E and K_i.

The branch of every $m \in M$ must have empty leaf node.

$S2T : p \leq |A| < p^2$

(1) ΔA intersects each order p^2 subgroup non-trivially:

$\Rightarrow$ M is not empty (since ΔA needs to intersect K).

$\Rightarrow$ The branch of every $m' \in M'$ has full leaf.

$\Rightarrow$ S can tile along with some $E' \oplus K_i$.

$S2T: p \leq |A| < p^2$

(1) ΔA intersects each order p^2 subgroup non-trivially:

$\Rightarrow$ M is not empty (since ΔA needs to intersect K).

$\Rightarrow$ The branch of every $m' \in M'$ has full leaf.

$\Rightarrow$ S can tile along with some $E' \oplus K_i$.

(2) $\Delta A \cap \Delta K = \emptyset$.

(2.1) There is some E' such that $\Delta E' \cap \Delta(A \oplus K) = \emptyset$: $(A, K \oplus E)$ is a tiling pair.

(2.2) No such E': impossible by the counting lemma.

$S2T: p \le |A| < p^2$

(1) ΔA intersects each order p^2 subgroup non-trivially:

$\Rightarrow$ M is not empty (since ΔA needs to intersect K).

$\Rightarrow$ The branch of every $m' \in M'$ has full leaf.

$\Rightarrow$ S can tile along with some $E' \oplus K_i$.

(2) $\Delta A \cap \Delta K = \emptyset$.

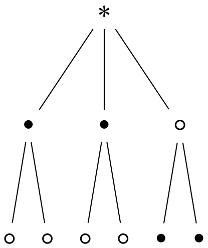
(2.1) There is some E' such that $\Delta E' \cap \Delta(A \oplus K) = \emptyset$: $(A, K \oplus E)$ is a tiling pair.

(2.2) No such E': impossible by the counting lemma.

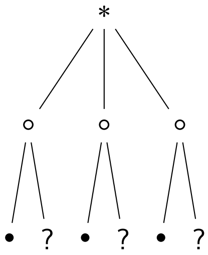
(3) $\Delta A \cap \Delta H = \emptyset$ for some maximal cyclic subgroup H.

Reduce to $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$.

$S2T : p \leq |A| < p^2$ case (1)

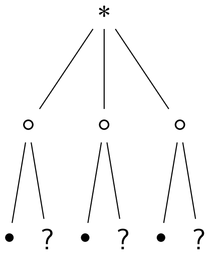


$S2T : p \le |A| < p^2$ case (2)



At least one leaf in each branch for $\Delta(A \oplus K)$ to intersect all $\Delta E'$.

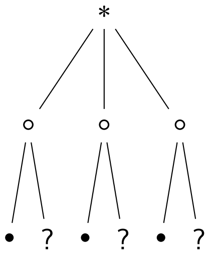
$S2T : p \leq |A| < p^2$ case (2)



At least one leaf in each branch for $\Delta(A \oplus K)$ to intersect all $\Delta E'$.

Apply counting lemma on S and each branch: $|S \cap K_i^{\perp_s}| = p|S \cap H_i|$.

$S2T : p \leq |A| < p^2$ case (2)

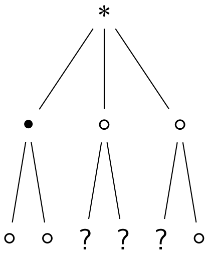


At least one leaf in each branch for $\Delta(A \oplus K)$ to intersect all $\Delta E'$.

Apply counting lemma on S and each branch: $|S \cap K_i^{\perp_s}| = p|S \cap H_i|$.

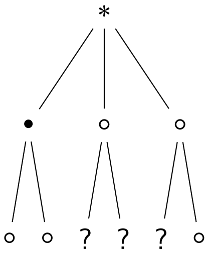
Sum over i: $|S| + p|S \cap K| = p^2 + p|S \cap K| + p|S \cap E_i| \quad \Rightarrow \quad |S| \geq p^2$.

$S2T : p \leq |A| < p^2$ case (3)



Let $a_i = |A \cap (K_i^{\perp_s} \setminus K)|, b = |A \cap K|, a'_i = |S \cap (K_i^{\perp_s} \setminus K)|, b' = |S \cap K|$.

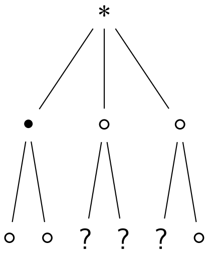
$S2T : p \leq |A| < p^2$ case (3)



Let $a_i = |A \cap (K_i^{\perp_s} \setminus K)|, b = |A \cap K|, a'_i = |S \cap (K_i^{\perp_s} \setminus K)|, b' = |S \cap K|$.

Counting $\Rightarrow$ $b, b' < p$ (otherwise $|A| \geq p^2$) $\Rightarrow$ $a_i \neq 0 \Leftrightarrow a'_i \neq 0$.

$S2T: p \leq |A| < p^2$ case (3)

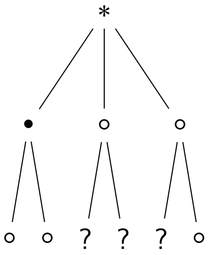


Let $a_i = |A \cap (K_i^{\perp_s} \setminus K)|, b = |A \cap K|, a_i' = |S \cap (K_i^{\perp_s} \setminus K)|, b' = |S \cap K|$.

Counting $\Rightarrow \quad b, b' < p$ (otherwise $|A| \geq p^2$) $\Rightarrow \quad a_i \neq 0 \Leftrightarrow a_i' \neq 0$.

Let $R = \{i : a_i \neq 0\}$, then $p | (a_i + b)$ (counting), and $|R| \leq |M'| \leq p$.

$S2T: p \le |A| < p^2$ case (3)



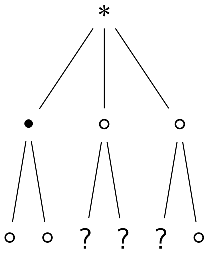
Let $a_i = |A \cap (K_i^{\perp_s} \setminus K)|, b = |A \cap K|, a'_i = |S \cap (K_i^{\perp_s} \setminus K)|, b' = |S \cap K|$.

Counting $\Rightarrow \quad b, b' < p$ (otherwise $|A| \ge p^2$) $\Rightarrow \quad a_i \ne 0 \Leftrightarrow a'_i \ne 0$.

Let $R = \{i : a_i \ne 0\}$, then $p | (a_i + b)$ (counting), and $|R| \le |M'| \le p$.

$(|R| - 1)b = (\sum_{i \in R} a_i + b) - |A|$ is divisible by p.

$S2T: p \le |A| < p^2$ case (3)



Let $a_i = |A \cap (K_i^{\perp_s} \setminus K)|, b = |A \cap K|, a'_i = |S \cap (K_i^{\perp_s} \setminus K)|, b' = |S \cap K|$.

Counting $\Rightarrow \quad b, b' < p$ (otherwise $|A| \ge p^2$) $\Rightarrow \quad a_i \ne 0 \Leftrightarrow a'_i \ne 0$.

Let $R = \{i : a_i \ne 0\}$, then $p|(a_i + b)$ (counting), and $|R| \le |M'| \le p$.

$(|R| - 1)b = (\sum_{i \in R} a_i + b) - |A|$ is divisible by p.

$|R| = 1 \quad \Rightarrow \quad$ reduce to $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$.

Summary

To analyze the zero set of a given set, we project it onto maximal cyclic subgroups to reduce to univariate polynomials.

Summary

To analyze the zero set of a given set, we project it onto maximal cyclic subgroups to reduce to univariate polynomials.

This leads to immediate results for highest (both) / lowest (T2S only) order tiling/spectral sets in prime power cases.

Summary

To analyze the zero set of a given set, we project it onto maximal cyclic subgroups to reduce to univariate polynomials.

This leads to immediate results for highest (both) / lowest (T2S only) order tiling/spectral sets in prime power cases.

To facilitate further computations we need a better way of changing bases, and this shall be done in the symplectic setting.

Summary

To analyze the zero set of a given set, we project it onto maximal cyclic subgroups to reduce to univariate polynomials.

This leads to immediate results for highest (both) / lowest (T2S only) order tiling/spectral sets in prime power cases.

To facilitate further computations we need a better way of changing bases, and this shall be done in the symplectic setting.

Structures and results on $\mathbb{Z}_{p^2}^2$ are briefed by a case discussion along its tree structure.


Thank You!