Uncertainty Principles for Abelian Groups

Liming Ge
(jointly with Jingsong Wu, Wenming Wu & Wei Yuan)

Chinese Academy of Sciences

June 18, 2013
(ECNU, Shanghai, China)

Heisenberg uncertainty principle

Heisenberg's canonical commutation relation:

$[P, Q] = PQ - QP = i\hbar$

A mathematical representation: $[D, M] = DM - MD = iI$

where $D = i\frac{d}{dx}$ and $M = M_x$. $D = i\mathcal{F}^* M \mathcal{F}$.

$||f||^2 = \langle f, f \rangle = |\langle [D - d, M - c] f, f \rangle|$

$= |\langle (M - c)f, (D - d)^* f \rangle - \langle (D - d)f, (M - c)^* f \rangle|$

$\leqslant 2\|(D - d)f\| \cdot \|(M - c)f\|.$

Heisenberg uncertainty principle in term of Fourier analysis:

If

$$\int_{\mathbb{R}} |f(x)|^2 dx = \int_{\mathbb{R}} |\hat{f}(\xi)|^2 d\xi = 1,$$

then we must have

$$\int_{\mathbb{R}} |xf(x)|^2 dx + \int_{\mathbb{R}} |\xi \widehat{f}(\xi)|^2 d\xi \geqslant \frac{1}{(4\pi)^2}.$$

Hardy uncertainty principle:

If $|f(x)| \leqslant C_1 e^{-\pi a x^2}$ and $|\widehat{f}(\xi)| \leqslant C_2 e^{-\pi \xi^2/a}$, then $f = Ce^{-\pi a x^2}$.

This implies immediately that f and $\widehat{f}$ cannot be both compactly supported.

Questions:

1. What could be the relation between the support of f and that of $\widehat{f}$? E.g. If f has a compact support, can the support of $\widehat{f}$ lie in $[0, \infty)$?

(It is known that f and $\widehat{f}$ can be supported in $[0, \infty)$.)

2. What if $\mathbb{R}$ is replaced by another abelian group G?

We shall study Question 2 for finite abelian groups and the group of integers.

G: a finite abelian group
$f : G \longrightarrow \mathbb{C}$, a complex valued function
$supp(f) := \{x \in G : x \in G, f(x) \neq 0\}$
$\widehat{f}$: the Fourier transform of f

Theorem 1 (An uncertainty principle)

(for a nonzero function f):

$$1). \quad |supp(f)| \cdot |supp(\widehat{f})| \geqslant |G|.$$

For a cyclic group of prime order p (T. Tao, 2005):

$$2). \quad |supp(f)| + |supp(\widehat{f})| \geqslant p + 1.$$

Uncertainty principle in term of spatial properties:

Suppose $X \subset G$ and $S \subset \widehat{G}$. Define

$$P_X = \{f : supp(f) \subset X\}; \quad Q_S = \{f : supp(\widehat{f}) \subset S\}.$$

Let f be a nonzero function on G, $X = supp(f)$ and $S = supp(\widehat{f})$. Then $f \in P_X \cap Q_S$.

Tao's result can be restated as follows:
For $G = \mathbb{Z}_p$ and any X, S given as above, if $P_X \cap Q_S \neq 0$, then $|X| + |S| \geq p + 1$.

We shall see $\dim(P_X \cap Q_S) = 1$ when $|X| + |S| = p + 1$.

Notation:

G: a finite additive abelian group, then G is self-dual.

$l^2(G)$: the Hilbert space of all complex-valued functions on G.

Inner product: $\langle f, g\rangle := \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g(x)}$.

Let f_x be the characteristic function on $\{x\}$. Then $\{f_x : x \in G\}$ is an orthogonal basis for $l^2(G)$.

Let $e : G \times G \longrightarrow \mathbb{T}$ be any non-degenerate bi-character of G.

Let e_x denote the function $e(x, \cdot)$.

Then $\{e_x\}_{x\in G}$ is an orthonormal basis of $l^2(G)$.

If f is a complex function on G, the Fourier transform $\widehat{f}$ of f is

$$\widehat{f} := \frac{1}{|G|}\sum_{x\in G} f(x)\overline{e_x}.$$

More notation:

Let $X, S \subset G(= \widehat{G})$. Denote also by P_X the orthogonal projection from $l^2(G)$ onto the subspace $l^2(X)$ and Q_S the projection from $l^2(G)$ onto the subspace $span\{e_x : x \in S\}$.

Then the uncertainty principle on G given by Theorem 1, part 1) can be reformulated by:

$|supp(f)||supp(\widehat{f})| \geqslant |G|(f \neq 0)$ is equivalent to

$$|X| \cdot |S| < |G| \Rightarrow P_X \wedge Q_S = 0.$$

The proof follows from a straight forward computation:
for any $f \in l^2(G)$, if $f(x) = \sum_{y \in S} \lambda_y e_y(x)$, then

$$\widehat{f}(\xi) = \frac{1}{|G|} \sum_{y \in S} \lambda_y e_y(\xi) = \frac{1}{|G|} \lambda_\xi.$$

In fact,

$$\begin{aligned}
\widehat{f}(\xi) &= \frac{1}{|G|} \sum_{x \in G} f(x) \overline{e(x,\xi)} \\
&= \frac{1}{|G|} \sum_{x \in G} (\sum_{y \in S} \lambda_y e(y,x)) \overline{e(x,\xi)} \\
&= \frac{1}{|G|} \sum_{y \in S} \lambda_y (\sum_{x \in G} e(y,x) \overline{e(x,\xi)}) = \frac{1}{|G|} \lambda_\xi.
\end{aligned}$$

Thus $f \in (P_X \wedge Q_S)(l^2(G))) \Rightarrow supp(f) \subset X, supp(\widehat{f}) \subset S.$ □

Theorem 2: Let $G = \mathbb{Z}_p$ with p prime. Then the FAQ

1) **Chebotarev's theorem**(Resetnyak, Dieudonne, T.Tao, etc): Let $\{x_1, \cdots, x_n\}$, $\{y_1, \cdots, y_n\} \subset \mathbb{Z}_p, (n \leqslant p)$. Then

$$det(e^{\frac{2\pi i x_j y_k}{p}})_{1 \leqslant j,k \leqslant n} \neq 0.$$

2) (Tao's uncertainty principle)$|supp(f)| + |supp(\widehat{f})| \geqslant p + 1 (f \neq 0)$.

3) If $|X| + |S| \leqslant p$, then $P_X \wedge Q_S = 0$.

Proof. 1)$\Rightarrow$ 2) Theorem 1.1. in [9, T.Tao].
2) $\Rightarrow$ 3) If there is a nonzero function $f \in P_X \wedge Q_S$, then $supp(f) \subset X$ and $supp(\widehat{f}) \subset S$. Thus $|X| + |S| \geqslant |supp(f)| + |supp(\widehat{f})| \geqslant p + 1$.
3) $\Rightarrow$ 2) If $|supp(f)| + |supp(\widehat{f})| \leqslant p$, then let $X = supp(f)$ and $S = supp(\widehat{f})$. We get a contradiction.
3) $\Rightarrow$ 1) If there is $\{x_1, \cdots, x_n\}$, $\{y_1, \cdots, y_n\} \subset \mathbb{Z}/p\mathbb{Z}(n \leqslant p)$ such that

$$det(e^{\frac{2\pi i x_j y_k}{p}})_{1\leqslant j,k\leqslant n} = 0.$$

Then vectors $\{e_{x_1}, \cdots, e_{x_n}, f_y : y \in \{x_1, \cdots, x_n\}^c\}$ is linearly dependent. Thus there is a non-zero vector $(\lambda_0, \cdots, \lambda_{p-1})$ such that

$$\sum_{i=1}^{n} \lambda_{x_i} e_{x_i} + \sum_{y\in\{x_1,\cdots,x_n\}^c} \lambda_y f_y = 0.$$

Let $X = \{x_1, \cdots, x_n\}^c$, $S = \{x_1, \cdots, x_n\}$ and $f(x) = \lambda_x, x \in G$. Then $|X| + |S| = p$ but $f \in P_X \wedge Q_S$. $\square$

Proposition 1.

Let $w = e^{\frac{2\pi i}{n}}$ and G be a cyclic group of order n and $|X| + |S| = n$. Then

$$det(w^{jk})_{j\in X, k\in S^c} = 0 \Leftrightarrow det(w^{jk})_{j\in X^c, k\in S} = 0.$$

In particular $P_X \wedge Q_S = 0 \Leftrightarrow det(w^{jk})_{j\in X, k\in S^c} \neq 0$.

Proof. Suppose $|X| = l, X^c = \{j_1', \cdots, j_{n-l}'\}, S = \{k_1, \cdots, k_{n-l}\}$. Define $Tf_x = f_x, x \in X$ and $Tf_{j_t} = e_{k_t}, t = 1, \cdots, n-l$.
Then $P_X \vee Q_S = I \Leftrightarrow T$ is invertible $\Leftrightarrow T|_{l^2(X^c)}$ is invertible.
The matrix of $T|_{l^2(X^c)} = (w^{jk})_{\{j\in X^c, k\in S\}}$.
□

Proposition 2

Let G be a finite abelian group and $X, S \subset G$. Then we have the following:

1) If $|X| + |S| > |G|$, then $P_X \wedge Q_S \neq 0$.

2) If $|X| + |S| = |G|$, then $P_X \wedge Q_S = 0$ if and only if $P_{X^c} \wedge Q_{S^c} = 0$.

3) If $|X| \cdot |S| < 2\sqrt{|G|}$, then $P_X \wedge Q_S = 0$.

Proof: $\tau(T) = \frac{1}{|G|} \sum_{x \in G} \langle Te_x, e_x \rangle$ (the trace on $\mathcal{B}(l^2(G))$).

By Kaplansky-formula, $\tau(P_X \vee Q_S - P_X) = \tau(Q_S - P_X \wedge Q_S)$

$$\tau(P_X \wedge Q_S) = \tau(P_X) + \tau(Q_S) - \tau(P_X \vee Q_S) > 0. \square$$

Proposition 3

Suppose G is a finite abelian group. Assume that there are $\alpha, \beta, \gamma \in \mathbb{N}$ such that, for any function f $(\neq 0)$ on G, we have $\alpha|supp(f)| + \beta|supp(\widehat{f})| \geqslant \gamma$. Then for any nonzero function g on $G \times \mathbb{Z}_p$ with p prime, we have

$$p\alpha|supp(g)| + \beta|supp(\widehat{g})| \geqslant p\gamma, \quad \alpha|supp(g)| + p\beta|supp(\widehat{g})| \geqslant p\gamma.$$

Corollary 1

Let $G = \mathbb{Z}_p \times \mathbb{Z}_q$ and f be a non zero function on G, where p and q are prime numbers. Then we have

$$q|supp(f)| + |supp(\widehat{f})| \geqslant q(p+1), |supp(f)| + q|supp(\widehat{f})| \geqslant q(p+1),$$

$$p|supp(f)| + |supp(\widehat{f})| \geqslant p(q+1), |supp(f)| + p|supp(\widehat{f})| \geqslant p(q+1).$$

Corollary 2

Let $G = (\mathbb{Z}_p)^n$ for a prime number p and a natural number n, and f be a non zero function on G. Then we have

$$p^j|supp(f)| + p^{n-j-1}|supp(\widehat{f})| \geqslant p^n + p^{n-1}(j = 0, \cdots, n-1).$$

Corollary 3

Let $G = (\mathbb{Z}_p)^n$ for a prime number p and a natural number n. For any subsets $X, S \subset G$, if there exist $0 \geqslant j \geqslant n-1$ such that $p^j|X| + p^{n-j-1}|S| < p^n + p^{n-1}$ holds, then $P_X \wedge Q_S = 0$.

Uncertainty Principles for $\mathbb{Z}$

Recall that an uncertainty principle for $\mathbb{R}$ states that, when $X \subset \mathbb{R}$ and $S \subset \widehat{\mathbb{R}}$ are both compact, then $P_X \cap Q_S = 0$. We hope to describe the largest possible such pairs (X, S). Or symmetrically the smallest pairs (X, S) so that $P_X \vee Q_S = I$.

Since $\mathbb{Z}$ has no invariant finite measure, we may consider its dual group $G = \mathbb{T}$, the unit circle on the complex plane.

Now $G = \widehat{\mathbb{Z}} = \mathbb{T}$, $\widehat{G} = \widehat{\mathbb{T}} = \mathbb{Z}$. G is not self-dual.

Goal: To investigate the respective subsets X of $\mathbb{T}$ and S of $\mathbb{Z}$ such that $P_X \wedge Q_S = 0$ and $P_X \vee Q_S = I$.

Notation:

$dm(z) = \frac{1}{2\pi i}\frac{dz}{z} = \frac{1}{2\pi}d\theta$: the normalized Lebesgue measure on $\mathbb{T}$, where $z = e^{i\theta}, \theta \in [0, 2\pi)$. Also denote $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, or simply $[0, 2\pi]$.

$\{e^{im\theta} : \theta \in [0, 2\pi), m \in \mathbb{Z}\}$: an orthonormal basis of $L^2(\mathbb{T})$.

$\{e_n : n \in \mathbb{Z}\}$: the standard orthonormal basis in $l^2(\mathbb{Z})$, where $e_n(m) = \delta_{n,m}$.

The Fourier transformation: $e^{im\theta} \mapsto e_m$ is a unitary operator from $L^2(\mathbb{T})$ to $l^2(\mathbb{Z})$.

Recall:

$X \subset [0, 2\pi]$: a measurable subset, $m(X)$: the measure of X
P_X: the orthogonal projection from $L^2(\mathbb{T})$ onto $L^2(X)$

$S \subset \mathbb{Z}$
Q_S: the projection from $L^2(\mathbb{T})$ onto $\overline{span}\{e^{im\theta} : m \in S\}$

P_t: the projection from $L^2(\mathbb{T})$ onto $L^2([2(1-t)\pi, 2\pi])$ for any $0 < t < 1$
$Q_{\geqslant j}$: the projection from $L^2(\mathbb{T})$ onto $\overline{span}\{e^{im\theta} : m \geqslant j, m \in \mathbb{Z}\}$

When $j = 0$, the range of projection $Q_{\geqslant 0}$ is the Hardy space $H^2(\mathbb{T})$

For a mean μ_ω on $\mathbb{Z}$ given by a free ultrafilter ω,
we define $\mu_\omega(S) = \mu_\omega(\chi_S)$

If the above is independent of ω, then we denote it by $\mu_\infty(S)$ and it is given by

$$\mu_\infty(S) = \lim_{n \to \infty} \frac{|S \cap \{-n, -(n-1), \cdots, n-1, n\}|}{2n+1}.$$

Definition

A pair (X, S) is called balanced if $P_X \wedge Q_S = 0$ and $P_X \vee Q_S = I$.

When G is a finite abelian group, if (X, S) is balance, then $\tau(P_X) + \tau(Q_S) = 1$.

Examples and Questions:

Examples $X = [0, \pi]$, $S_0 = 2\mathbb{Z}$, all even integers, $S_1 \subset \mathbb{Z}$ all odd integers. (X, S_0) and (X, S_1) are balanced pairs.
$m(X) + \mu_\infty(S_0) = m(X) + \mu_\infty(S_1) = 1$.

Questions Is $m(X) + \mu_\infty(S) = 1$ a necessary condition for balanced pairs? If "no", for any $\epsilon > 0$, can one find a balanced pair (X, S) so that $m(X) + \mu_\infty(S) < \epsilon$ or $m(X) + \mu_\omega(S) < \epsilon$?

Some basic facts:

1) $P_X \vee Q_S = I \Leftrightarrow P_X \vee Q_{-S} = I$, where $-S = \{-s : s \in S\}$;

2) $P_X \wedge Q_S = 0 \Leftrightarrow P_X \wedge Q_{-S} = 0$;

3) $P_X \vee Q_S = I \Leftrightarrow P_X \vee Q_{S+j} = I$, where $S + j = \{s + j : s \in S\}$;

4) $P_X \wedge Q_S = 0 \Leftrightarrow P_X \wedge Q_{S+j} = 0$;

5) If $X \subset \mathbb{T}$ with $0 < m(X) < 1$, then $P_X \wedge Q_{\geqslant j} = 0$ and $P_X \vee Q_{\geqslant j} = I (\forall j \in \mathbb{Z})$.

From 5), we see that $\frac{1}{2} < m(X) + \mu_\infty(Q_{\geqslant 0}) < \frac{3}{2}$.

Proof. Let $(Uf)(z) = \overline{f(z)}$. Then U is a conjugate linear operator such that $U^2 = I$ and $UP_X U = P_X, UQ_S U = Q_{-S}$. Thus 1) and 2) are true.

Let $(U_j f)(z) = z^j f(z)$. Then U_j is a unitary operator such that $UP_X U^* = P_X, UQ_S U^* = Q_{S+j}$. Hence 3) and 4) are true.

For 5), let $(Vf)(z) = zf(z)$. Then V is a unitary operator such that $(I - P_X \wedge Q_{\geqslant 0})VP_X \wedge Q_{\geqslant 0} = 0$. As $P_X \wedge Q_{\geqslant 0} \leqslant Q_{\geqslant 0}$ and by Beurling theorem, there exists an inner function φ such that $P_X \wedge Q_{\geqslant 0}(H^2(\mathbb{T})) = \varphi H^2(\mathbb{T})$. Thus $\varphi = 0$ and $P_X \wedge Q_{\geqslant 0} = 0$. From 2), $P_{X^c} \wedge Q_{\leqslant 0} = 0$. This implies that $P_X \vee Q_{\geqslant 0} = I$.

Theorem 3

For any $\varepsilon > 0$, there exists a measurable subset X of $[0, 2\pi]$ with $0 < m(X) < \varepsilon$ and a subset S of $\mathbb{Z}$ with $\mu_\omega(S) = 0$ for some free ultrafilter ω such that $P_X \wedge Q_S = 0$ and $P_X \vee Q_S = I$.

Proof. For any $\epsilon > 0$, there exist n in $\mathbb{N}$ such that $\frac{1}{n} < \epsilon$. Let $X = [2(1-\frac{1}{n})\pi, 2\pi]$. Then $m(X) = \frac{1}{n} < \epsilon$. From Basic Fact 5), we have $P_X \wedge Q_{\geq 0} = 0$ and $P_X \vee Q_{\geq 0} = P_X \vee Q_{\geq j} = I$ for any $j \in \mathbb{Z}$. Then $\overline{span}\{e^{i\frac{n-1}{n}m\theta}, m \geq j\} = L^2[0, 2\pi]$ for j in $\mathbb{Z}$. In fact if there is a non zero vector f in $L^2[0, 2\pi]$ orthogonal to $\overline{span}\{e^{i\frac{n-1}{n}m\theta}, m \geq j\}$, we define a function $g(\theta) = f(\frac{n}{n-1}\theta)$ when $0 \leq \theta \leq 2\pi\frac{n-1}{n}$, 0 elsewhere, then we have

$$\int_0^{2\pi} f(\theta)e^{-i\frac{n-1}{n}m\theta}d\theta = \int_0^{2\pi} g(\frac{n-1}{n}\theta)e^{-i\frac{n-1}{n}m\theta}d\theta = \int_0^{2\frac{n-1}{n}\pi} g(\theta)e^{-im\theta} = 0,$$

and hence g is a non zero vector in the range of $I - (P_{1/n} \vee Q_{\geq j})$ which leads a contradiction.

For any n in $\mathbb{N}$, since $\overline{span}\{e^{i\frac{n-1}{n}m\theta}, m \geq j\} = L^2[0, 2\pi]$ for j in $\mathbb{Z}$, there exists $m(n, j)$ in $\mathbb{N}$ such that the distance between $e^{ik\theta}$ and

$$\overline{span}\{e^{i\frac{n-1}{n}j\theta}, \ldots, e^{i\frac{n-1}{n}m(n,j)\theta}\}(= \mathcal{H}_{n,j})$$

is less than $\frac{1}{n}$ for any $-n \leq k \leq n$. Obviously, $m(n, j) > j$ for any j in $\mathbb{Z}$. Let $S_{n,j}$ be the set $\{j, \ldots, m(n, j)\}$. We define m_k in $\mathbb{N}$ by induction. Let $m_1 = m(1, 0)$. Suppose that m_k is defined. Then $m_{k+1} = m(k + 1, m_k^2)$ for $k \geq 1$ and $m_{k+1} > m_k^2$. It is clear that the closure of the union of $\mathcal{H}_{k,m_k}$, $k \geq 1$ is $L^2[0, 2\pi]$ and its corresponding set S is $\bigcup_{k\geq 1} S_{k,m_k}$. For the sequence $\frac{\#S\cap\{-n,\ldots,0,\ldots,n\}}{2n+1}$, there is a subsequence $\{\frac{\sum_{j=1}^{k}(m_j - m_{j-1}^2)}{2m_k^2+1}\}_{k\geq 1}$ with limit zero, since $\sum_{j=1}^{k}(m_j - m_{j-1}^2) < m_k$. Hence there is a free ultrafilter ω such that $\lim_{n\to\omega} \frac{\#S\cap\{-n,\ldots,0,\ldots,n\}}{2n+1} = 0$. $\square$

Corollary

Let $X_n = [0, \frac{1}{n}] \subset \mathbb{T}$. For any free ultrafilter ω, there is a subset S of $\mathbb{Z}$ with $\mu_\omega(S) = 0$ such that $P_{X_n} \wedge Q_S = 0$ and $P_{X_n} \vee Q_S = I$, for any $n \geq 1$. Thus, for any $f, g \in L^2(\mathbb{T})$, if there is an n such that $f|_{X_n} = g|_{X_n}$ and $\widehat{f}|_S = \widehat{g}|_S$, then $f = g$.

Conjecture: $S = \{0, \pm 1, \pm p, \pm 2p : p \text{ a prime number}\}$ is such a set satisfies our Theorem 4, i.e., $([0, \epsilon], S)$ is balanced for any $\epsilon > 0$.

In other words, two functions on $\mathbb{T}$ agree on $[0, \epsilon]$ and their Fourier expansions agree on S. Then they must be the same function.

One possible application:

If (X, S) is a balanced pair for $\mathbb{T}$ and $f \in L^2(\mathbb{T})$, then how can we recover f from $f|_X$ and $\widehat{f}|_S$?

It is not an easy question. In the following we shall workout a concrete example.

Theorem 4

Let $\{a_n\}_{n=1}^{\infty}$ be an increasing sequence of odd natural numbers such that

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = +\infty.$$

Suppose $S = \{2k : k \in \mathbb{N}\} \cup \{a_n\}$. Then $P_{1/2} \vee Q_S = I$ and $P_{1/2} \wedge Q_S = 0$. In this case, $X = [\pi, 2\pi]$. We may choose $\{a_n\}$ so that $m(X) + \mu_\infty(S) = \frac{3}{4}$.

Lemma Suppose p is a prime number and $I_j = \{w^j e^{i\theta} \in \mathbb{T} : \theta \in [0, \frac{2\pi}{p})\}$ for $j = 0, 1, \cdots, p-1$. Let $X(i_1, \cdots, i_m) = I_{i_1} \cup \cdots \cup I_{i_m}$ where $0 \leqslant i_1 < \cdots < i_m \leqslant p-1$. Let $S_0 \subset \{0, 1, \cdots, p-1\}$ and $\emptyset \neq S_1 \subset S_0^c$. Let $S = \{kp + s_0 : k \in \mathbb{Z}, s_0 \in S_0\} \cup \{kp + s_1 : k \geqslant 0, s_1 \in S_1\}$. Then we have

$$P_{X(i_1, \cdots, i_m)} \wedge Q_S = 0 \Leftrightarrow |S_0^c| \geqslant m + 1.$$

Proof of Theorem 4. $Q_S < Q_{\geqslant 0}, P_{1/2} \wedge Q_{\geqslant 0} = 0 \Rightarrow P_{1/2} \wedge Q_S = 0$. Assume that $P_{1/2} \vee Q_S \neq I$. Then there exists a non-zero function f in $L^2([0, 2\pi])$ such that f is orthogonal to the ranges of $P_{1/2}$ and Q_S. Thus $supp(f) \subset [0, \pi]$ and for any $s \in S$, we have

$$\frac{1}{2\pi}\int_0^{\pi} f(\theta)e^{-is\theta}d\theta = \frac{1}{4\pi}\int_0^{2\pi} f(\frac{\theta}{2})e^{-is\theta/2}d\theta = 0.$$

Claim. $\mathscr{H}_S := \overline{span}\{e^{is\theta/2} : s \in S\} = L^2([0, 2\pi])$.

Firstly when $s = 2k(k \in \mathbb{N})$, we have $e^{ik\theta} \in \mathcal{H}_S$. When $s = a_n$ for $n \geqslant 1$, for any $m \in \mathbb{Z}$, we have

$$\langle e^{ia_n\theta/2}, e^{im\theta} \rangle = \frac{2i}{\pi(a_n - 2m)}.$$

Then $e^{ia_n\theta/2} = \sum_{m\in\mathbb{Z}} \frac{2i}{\pi} \frac{e^{im\theta}}{a_n - 2m}$.
Let $\xi_n = \sum_{m=-\infty}^{-1} \frac{e^{im\theta}}{a_n - 2m} = \sum_{m=1}^{\infty} \frac{e^{-im\theta}}{a_n + 2m}$. To show that the claim holds, we just need to show that $\overline{span}\{\xi_n : n \geqslant 1\} = \overline{span}\{e^{-im\theta} : m \geqslant 1\}$ which is equivalent to $\{\xi_n : n \geqslant 1\}^{\perp} \cap \overline{span}\{e^{-im\theta} : m \geqslant 1\} = 0$.

Suppose that $\alpha^{(0)} = \sum_{m\geqslant 1} \alpha_m^{(0)} e^{-im\theta}$ such that $\alpha^{(0)} \perp \{\xi_n : n \geqslant 1\}$ and $\sum_{m\geqslant 1} |\alpha_m^{(0)}|^2 < \infty$. Thus for any $n \geqslant 1$, we have

$$\sum_{m\geqslant 1} \frac{\alpha_m^{(0)}}{a_n + 2m} = 0.$$

This implies that for any $n \geqslant 2$, we have

$$0 = \frac{1}{a_n - a_1} \sum_{m=1}^{\infty} \left(\frac{\alpha_m^{(0)}}{a_1 + 2m} - \frac{\alpha^{(0)}}{a_n + 2m} \right) = \sum_{m=1}^{\infty} \frac{\alpha_m^{(0)}}{a_1 + 2m} \frac{1}{a_n + 2m}.$$

Let $\alpha_m^{(1)} := \frac{\alpha_m^{(0)}}{a_1 + 2m}$ and $\alpha^{(1)} := \sum_{m\geqslant 1} \alpha_m^{(1)} e^{-im\theta}$. Then $\alpha^{(1)} \perp \{\xi_n : n \geqslant 2\}$ and

$$\sum_{m=1}^{\infty} |\alpha_m^{(1)}| \leqslant \|\alpha^{(0)}\| \cdot \left(\sum_{m=1}^{\infty} \frac{1}{(a_n + 2m)^2} \right)^{1/2} < \infty.$$

Iterating the process, for any $N > 0$, we can define $\alpha_m^{(N)} = \frac{\alpha_m^{(N-1)}}{a_N + 2m}$ and $\alpha^{(N)} = \sum_{m \geqslant 1} \alpha_m^{(N)} e^{-im\theta}$ with $\alpha^{(N)} \perp \{\xi_n : n \geqslant N+1\}$.
Without loss of generality, we can assume that $\alpha_1^{(0)} = 1$. Then $\alpha_1^{(N)} = \prod_{n=1}^{N} \frac{1}{a_n + 2}$. We define

$$\beta_m^{(N)} = \frac{\alpha_m^{(N)}}{\alpha_1^{(N)}} = (a_1 + 2) \prod_{n=2}^{N} \frac{a_n + 2}{a_n + 2m} \alpha_m^{(1)}, m \geqslant 1.$$

Then we have $\beta^{(N)} = \frac{\alpha^{(N)}}{\alpha_1^{(N)}}$ and $\beta^{(N)} \perp \{\xi_n : n \geqslant N+1\}$ and

$$\sum_{m\geqslant 2} |\beta_m^{(N)}| = \sum_{m\geqslant 2} (a_1+2)(\prod_{n=2}^{N} \frac{a_n+2}{a_n+2m})|\alpha_m^{(1)}|$$
$$\leqslant (a_1+2)(\prod_{n=2}^{N} \frac{a_n+2}{a_n+4}) \sum_{m\geqslant 2} |\alpha_m^{(1)}|.$$

Then as $\sum \frac{1}{a_n} = +\infty$, thus $\prod_{n=2}^{N} \frac{a_n+2}{a_n+4} = \prod(1-\frac{2}{a_n+4}) \to 0$ as $N \to \infty$.
Then $\exists$ sufficient large N_0 such that for any $N \geqslant N_0$ we have

$$(a_1+2)(\prod_{n=2}^{N} \frac{a_n+2}{a_n+4}) \sum_{m\geqslant 2} |\alpha_m^{(1)}| < 1. \tag{1}$$

Thus $\sum_{m\geqslant 2} |\beta_m^{(N)}| < 1$ for any $N \geqslant N_0$.

On the other hand for any vector $\beta = e^{-i\theta} + \sum_{m\geqslant 2} \beta_m e^{-im\theta}$ which is orthogonal some ξ_k, $k \geqslant 1$, then we have

$$1 = -\sum_{m\geqslant 2} \beta_m \frac{a_k + 2}{a_k + 2m} \leqslant \sum_{m\geqslant 2} |\beta_m|.$$

Thus by (1) and (2), we get a contradiction. Thus $\alpha^{(0)} = 0$. □

Corollary Let $S = \{nk : k \geqslant 0\} \cup \{a_m\}$ where $\{a_m\}$ is an increasing sequence of positive integers in $(n\mathbb{Z})^c$ and $\sum_m \frac{1}{a_m} = \infty$, then $P_{(n-1)/n} \vee Q_S = I$ and $P_{(n-1)/n} \wedge Q_S = 0$.

Finding f from the restrictions to (X, S) is related to finding the inverse of certain Hankel operators. A special one is the following:

Let $H(s)(0 < s < 1)$ be the Hankel operator with the following matrix form

$$\begin{pmatrix} \frac{1}{1+s} & \frac{1}{2+s} & \frac{1}{3+s} & \cdots \\ \frac{1}{2+s} & \frac{1}{3+s} & \frac{1}{4+s} & \cdots \\ \frac{1}{3+s} & \frac{1}{4+s} & \frac{1}{5+s} & \cdots \\ \cdots & \cdots & \cdots & \ddots \end{pmatrix}.$$

Some References

[1] Man-Duen Choi, *Tricks or Treats with the Hilbert Matrix*, The Amer. Math. Monthly. Vol.90, No.5, 301-312, 1983.

[2] J. Dieudonné, *Une propritété des racines de l'unité*, Collection of articles dedicated to Alberto González Dominguez on his sixty-fifth birthday, Rev. Un. Mat. Argentina Vol.25, 1-3, 1970/71.

[3] R.J. Evan and I.M. Stark, *Generalized Vandermonde determinants and roots of unity of prime order*, Proc. Amer. Math. Soc. Vol. 58,51-54, 1977.

[4] P. Frenkel, *Simple proof of Chebotarev's theorem on roots of unity preprint*, math. AC/0312398.

[5] D. Goldstein, R. Guralnick, and I. Issaacs, *Inequalities for finite group per- mutation modules preprint*, math. CO/0312407.

[6] M. Newman, *On a theorem of Cebotarev Linear and Multilinear Algebra*, Vol.3 (no. 4), 259-262, 1975/76.
[7] Yu. G. Rešetnyak, *New Proof of a theorem of N.G. Cebotarev*, (Russian) Uspehi Mat. Nauk (N.S.), Vol.10, 155-157, 1955.
[8] P. Stevenhagen and H.W. Lenstra Jr., *Chebotarëv and his density theorem*, Math Intelligencer, Vol.18, 26-37, 1996.
[9] Terence Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett., Vol.12, 121-127, 2005.

Thanks