An Uncertainty Principle for Discrete Fourier Transform

Irish Debbarma
Undergraduate (Mathematics Major)
Indian Institute of Science, University of Lille

Contents

1 Notation

- G unless specified otherwise is a finite abelian group with addition as the group operation
- $\widehat{G}$ is used to denote the group of characters of the finite abelian group G

- $L(G)$ - the set of all complex valued functions on the group G
- If $f : G \longrightarrow \mathbb{C}$ is a nonzero function, then the fourier transform of f, denoted by $\mathcal{F}f$ or $\hat{f}$ is given by

$$\hat{f}(\chi) = \sum_{x \in G} f(x)\chi(x)$$

- $\operatorname{supp} f = \{x \in G : f(x) \neq 0\}$
- $\theta(G, k) = \min\{|\operatorname{supp} \hat{f}| : 0 \neq f \in L(G), |\operatorname{supp} f| \leq k\}$
- $d_1(n, k) =$ the largest divisor d of n less than or equal to k, $d_2(n, k) =$ the smallest divisor d of n greater than or equal to k. If we let $d_i(n, k) = d_i$ for $i = 1, 2$, we define

$$u(n, k) = \frac{n}{d_1 d_2} \cdot (a_1 + a_2 - k)$$

2 Overview

Uncertainty principle has its origins deep rooted in physics. The classical Heisenberg uncertainty principle being the most famous one; it said that the position and velocity of an object cannot both be measured precisely at the same time. Drawing inspiration from that, over the last hundred years, people have tried to extend the idea to many other fields. All of them try to relate the function and its Fourier transform, and conclude that both the function and its Fourier transform can not both be *very small*. In 1989, Donoho and Stark [4] studied this phenomenon for functions on finite groups. It states that if G is a finite abelian group and $\hat{G}$ is its dual group, $f : G \longrightarrow \mathbb{C}$ is a nonzero function, $\hat{f} : \hat{G} \longrightarrow \mathbb{C}$ is its Fourier transform, then

$$|\operatorname{supp}(f)| \cdot |\operatorname{supp}(\hat{f})| \geq |G|$$

This result is discussed in 3. The main resource used in this section is [15] and [3].

Recently, Tao improved on this result [14] for a cyclic group of prime order by proving that

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq |G| + 1$$

The proof of this result relies on a very crucial result which says that the determinant of any minor in the Fourier transform matrix does not vanish. In this document, I have presented two proofs of this fact due to Tao [14] and Frenkel [5]. The main resources used in this section are [14], [5] and [16].

In section 5, building on the idea of Tao, Murty and Whang prove a similar result

$$|\mathrm{supp}\,(f)| + |\mathrm{supp}\,(\hat{f})| \geq |G| + 1$$

for cyclic group G of composite order given a certain property (proposition 5.7) is satisfied [11]. The proof in this section uses some results from Lie groups and representation theory such as Weyl character formula. I have tried to make the document as self contained as possible but for more material on (compact) Lie groups and representations, please use [1][12][6] [2]. A lot of the arguments in this section is the same as Tao.

Next, in section 6, as noted by Tao in his paper [14], we present another proof of Cauchy Davenport theorem and a variant of Cauchy Davenport as proven in [11]. We also look at some observations made about sparse polynomials in [11] and [14].

In section 7, we study a result by Meschulam which also relates the support size of a function on finite abelian group and support size of the Fourier transform of the function, but it is special because the proof is seemingly different from the two previous proofs as seen in the previous sections. It uses submultiplicativity of certain quantities and manages to relate these quantities to get a wonderful result.

3 Preliminary Uncertainty Principle

Theorem 3.1. *Let G be a finite abelian group. Say $f : G \to \mathbb{C}$ is a function on G that is not identically zero. If $\hat{f}$ is the corresponding Fourier transform, then we have*

$$|\mathrm{supp}\, f| \cdot |\mathrm{supp}\, \hat{f}| \geq |G|$$

Proof. Notice that we have a inner product on the space $L(G)$ given by

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)}$$

This inner product induces a norm given by

$$||f||_2^2 = \sum_{x \in G} |f(x)|^2$$

Let $||f||_\infty = \sup_{x \in G} |f(x)|$, then we have the observation

$$||f||_2^2 \leq |\mathrm{supp}\, f| \cdot ||f||_\infty^2 \tag{1}$$

Since $|\chi(x)| \leq 1 \; \forall x \in G$,

$$||f||_\infty \leq \frac{1}{|G|} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)| \tag{2}$$

Now, using Cauchy Schwartz inequality we have

$$\begin{aligned} ||f||_\infty^2 &\leq \frac{1}{|G|^2} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)^2| \sum_{\chi \in \operatorname{supp} \hat{f}} 1^2 \\ &\leq \frac{1}{|G|^2} ||\hat{f}||_2^2 \cdot |\operatorname{supp} \hat{f}| \end{aligned}$$

$$||f||_\infty^2 \leq \frac{1}{|G|^2} \cdot ||\hat{f}||_2^2 \cdot |\operatorname{supp} \hat{f}| \tag{3}$$

Using Plancherel's identity we have $||f||_2^2 = \frac{1}{|G|}||\hat{f}||_2^2$, after we plug this into (3) and use (1) we have

$$\begin{aligned} ||f||_\infty^2 &\leq \frac{1}{|G|} \cdot ||\hat{f}||_2^2 \cdot |\operatorname{supp} \hat{f}| \\ ||f||_2^2 &\leq \frac{1}{|G|} ||f||_2^2 \cdot |\operatorname{supp} f| \cdot |\operatorname{supp} \hat{f}| \end{aligned}$$

Finally, we have our required result which is

$$|\operatorname{supp} f| \cdot |\operatorname{supp} \hat{f}| \geq |G|$$

□

Proof of Plancherel's identity:

$$\begin{aligned} ||f||_2^2 &= \langle f, f \rangle \\ &= \sum_{x \in G} f(x) \cdot \overline{f(x)} \\ &= \sum_{x \in G} \left[\frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x) \right] \cdot \left[\frac{1}{|G|} \sum_{\psi \in \hat{G}} \overline{\hat{f}(\psi)}\overline{\psi(x)} \right] \\ &= \frac{1}{|G|^2} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \sum_{\psi \in \hat{G}} \overline{\hat{f}(\psi)} \sum_{x \in G} \chi(x)\overline{\psi(x)} \\ &= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\overline{\hat{f}(\chi)} \qquad \text{from orthogonality relations} \\ &= \frac{1}{|G|} ||\hat{f}||_2^2 \end{aligned}$$

□

4 Tao's result

4.1 Theorem statement and key proposition

Theorem 4.1. *Let p be a prime. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a nonzero function, then*

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \geq p + 1$$

Conversely, if A, B are two nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a function f such that $\operatorname{supp} f = A, \operatorname{supp} \hat{f} = B$.

The proof of this theorem is based on the following proposition.

Proposition 4.2. *Let p be a prime number and $1 \leq n \leq p$. Let $\{x_1, \dots, x_n\}$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$ and $\{\xi_1, \dots, \xi_n\}$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$ as well. If $\omega := e^{2\pi i/p}$, then the matrix $(\omega^{x_i \xi_j})_{1 \leq i,j \leq n}$ has nonzero determinant.*

I will present two proofs of this proposition, one due to Tao and the other due to Frenkel.

4.2 Tao's proof of the main proposition

Lemma 4.3. *Let p be a prime, $n \in \mathbb{Z}_{>0}$. Let $P(z_1, \dots, z_n)$ be a polynomial with integer coefficients. Suppose that we have n p-th roots of unity $\omega_1, \dots, \omega_n$ such that $P(\omega_1, \dots, \omega_n) = 0$, then $p | P(1, \dots, 1)$.*

Proof. Since ω_j is a p-th root of unity, we have $\omega_j = \omega^{k_j}$ for some $0 \leq k_j \leq p$. Define a new polynomial $Q(z)$ as follows:

$$Q(z) = P(z^{k_1}, \dots, z^{k_n}) \pmod{z^p - 1}$$

$Q(z)$ is also a polynomial with integer coefficients of degree less than p. Note that Q vanishes at ω and $Q(1) = P(1, \dots, 1)$. Since $Q(\omega) = 0$, therefore the minimal polynomial of ω $(1 + z + \cdots + z^{p-1})$ divides $Q(z)$. This implies $(1 + z + \cdots + z^{p-1})R(z) = Q(z)$. Evalutating at $z = 1$, we have $p \cdot R(1) = Q(1) = P(1, \dots, 1)$. As $R(z)$ also has integer coefficients, we note that $R(1)$ is an integer and conclude that $p | P(1, \dots, 1)$. □

Proof of proposition 4.2. Let $\omega_j := e^{e\pi i x_j/p}$. Each ω_j is a distinct p-th root of unity and we want to show that

$$\det(\omega_j^{\xi_k})_{1 \leq j,k \leq n} \neq 0$$

Define the polynomial $D(z_1, \dots, z_n) := \det(z_j^{\xi_k})_{1 \leq i,j \leq n}$

- $D(z_1, \dots, z_n)$ is a polynomial with integer coefficients

- D vanishes when $z_j = z_{j'}$ for $j \neq j'$, therefore D factors in the following manner
$$D(z_1, \dots, z_n) = P(z_1, \dots, z_n) \prod_{1 \leq j \leq j' \leq n} (z_j - z_{j'})$$
- $D(1, \dots, 1) = 0$ and $p \mid 0$ therefore we cannot use lemma 4.3 to conclude that $D(\omega_1, \dots, \omega_n) \neq 0$. Instead we will prove that $P(1, \dots, 1)$ is not a multiple of p which will imply $P(\omega_1, \dots, \omega_n) \neq 0 \Rightarrow D(\omega_1, \dots, \omega_n) \neq 0$ and we get our required claim.

To find $P(1, \dots, 1)$ we do the following. We apply the following operator
$$\left(z_1 \frac{d}{dz_1}\right)^0 \left(z_2 \frac{d}{dz_2}\right)^1 \left(z_3 \frac{d}{dz_3}\right)^2 \cdots \left(z_{n-1} \frac{d}{dz_{n-1}}\right)^{n-2} \left(z_n \frac{d}{dz_n}\right)^{n-1}$$
to $D(z_1, \dots, z_n)$ and then evaluate at $(1, \dots, 1)$.
There are $0+1+2+\cdots+n-1 = (n-1)n/2$ many differential operators. The same as the number of linear factors in the factorisation of $P(z_1, \dots, z_n)$. Moreover, after we apply the differential operators, the only terms that contribute to the sum are those where there are no linear factors (the ones with even one linear factor vanish because $1-1=0$). Therefore $\left(z_n \frac{d}{dz_n}\right)^{n-1}$ must eliminate all the $n-1$ linear factors $(z_j - z_n)$ and this can be done in $(n-1)!$ ways (just chain rule written in a fancy manner). Similarly, $\left(z_{n-1} \frac{d}{dz_{n-1}}\right)^{n-2}$ eliminates all the $n-2$ linear factors $(z_j - z_{n-1})$ in $(n-2)!$ ways. Finally, after appling all the differential operators and evaluating at $(1, \dots, 1)$ we get
$$(n-1)! \cdot (n-2)! \cdots 3! \cdot 2! \cdot 1! \cdot 0! \cdot P(1, \dots, 1) = (*)$$
We still need more information to conclude what we want about $P(1, \dots, 1)$. So, let us apply the differential operator to the definition of $D(z_1, \dots, z_n)$. We keep a small result in mind, $z_k \frac{d}{dz_k} z_k^{\xi_l} = \xi_l z_k^{\xi_l}$.

$$z_n \frac{d}{dz_n} \begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ z_2^{\xi_1} & z_2^{\xi_2} & z_2^{\xi_3} & \cdots & z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n^{\xi_1} & z_n^{\xi_2} & z_n^{\xi_3} & \cdots & z_n^{\xi_n} \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & \cdots & 0 \\ z_2^{\xi_1} & z_2^{\xi_2} & z_2^{\xi_3} & \cdots & z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n^{\xi_1} & z_n^{\xi_2} & z_n^{\xi_3} & \cdots & z_n^{\xi_n} \end{vmatrix} + \begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n^{\xi_1} & z_n^{\xi_2} & z_n^{\xi_3} & \cdots & z_n^{\xi_n} \end{vmatrix} + \cdots\cdots$$
$$\cdots + \begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ z_2^{\xi_1} & z_2^{\xi_2} & z_2^{\xi_3} & \cdots & z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_1 z_n^{\xi_1} & \xi_2 z_n^{\xi_2} & \xi_3 z_n^{\xi_3} & \cdots & \xi_n z_n^{\xi_n} \end{vmatrix}$$
Continue this to get
$$\left(z_n \frac{d}{dz_n}\right)^2 \begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ z_2^{\xi_1} & z_2^{\xi_2} & z_2^{\xi_3} & \cdots & z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n^{\xi_1} & z_n^{\xi_2} & z_n^{\xi_3} & \cdots & z_n^{\xi_n} \end{vmatrix} = \begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ z_2^{\xi_1} & z_2^{\xi_2} & z_2^{\xi_3} & \cdots & z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_1^2 z_n^{\xi_1} & \xi_2^2 z_n^{\xi_2} & \xi_3^2 z_n^{\xi_3} & \cdots & \xi_n^2 z_n^{\xi_n} \end{vmatrix}$$

Now that we understand the pattern, when we apply all the operators we are left with the following matrix

$$\begin{vmatrix} z_1^{\xi_1} & z_1^{\xi_2} & z_1^{\xi_3} & \cdots & z_1^{\xi_n} \\ \xi_1 z_2^{\xi_1} & \xi_2 z_2^{\xi_2} & \xi_3 z_2^{\xi_3} & \cdots & \xi_n z_2^{\xi_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_1^{n-1} z_n^{\xi_1} & \xi_2^{n-1} z_n^{\xi_2} & \xi_3^{n-1} z_n^{\xi_3} & \cdots & \xi_{n-1} z_n^{\xi_n} \end{vmatrix}$$

Next, when we evaluate this at $(1, \ldots, 1)$ we get the Vandermonde determinant $\det(\xi_j^{k-1})_{1\leq j,k\leq n}$. This determinant evaluates to

$$(*) = \pm \prod_{1\leq j,j'\leq n} (\xi_j - \xi_{j'})$$

Since all the ξ_j are distinct, the product is nonzero and is not 0 modulo p. Moreover $n < p$ and therefore all the elements in the product $(n-1)! \cdot (n-2)! \cdots 1!$ are not 0 modulo p, therefore it follows that p does not divide $P(1, \ldots, 1)$ and we have proven our claim. □

4.3 Frenkel's proof of the main proposition

Lemma 4.4. $\mathbb{Z}[\omega]/\langle 1-\omega\rangle = \mathbb{F}_p$

Proof. Take $f(X) = 1 + X + X^2 + \cdots + X^{p-1}$.

- $f(\omega) = 0$
- f is irreducible due to Eisenstein at p

This tells us that f must be the minimal polynomial of ω.
Consider the maps

$$\begin{tikzcd} \varphi : & \mathbb{Z}[X] \arrow[r, "\sim"] & \mathbb{Z}[X]/\langle f(X)\rangle = \mathbb{Z}[\omega] \\ & \mathbb{Z} \ni r \arrow[r] & r \\ & X \arrow[r] & \omega \end{tikzcd}$$

$$\begin{tikzcd} \psi : & \mathbb{Z}[X] \arrow[r, "\sim"] & \mathbb{Z}[X]/\langle 1-X, p\rangle = \mathbb{F}_p \\ & \mathbb{Z} \ni r \arrow[r] & r \pmod p \\ & X \arrow[r] & 1 \end{tikzcd}$$

Next, we note that $\langle p\rangle, \langle 1-X\rangle \subseteq \mathrm{Ker}\psi$, and $f(1) = p$

$$\begin{aligned}
\Rightarrow f(X) &\equiv p \pmod{1-X}\\
\Rightarrow f(X) &= p + g(X)(1-X)\\
\Rightarrow \langle f(X)\rangle &= \langle p + g(X)(1-X)\rangle\\
&\subseteq \langle p, 1-X\rangle\\
\mathrm{Ker}(\varphi) &\subseteq \mathrm{Ker}(\psi)
\end{aligned}$$

This means that ψ factors through φ.

I will take a slight detour and explain what factors through means.
If $\varphi : G \to K$ is a group homomorphism and $\pi : G \to H$ is a surjective group homomorphism such that $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(\varphi)$. Then we say that φ factors through π if there is function η such that $\varphi = \eta \circ \pi$.

$$\begin{tikzcd}
G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & K \\
& H \arrow[ur, dashed, "\eta"'] &
\end{tikzcd}$$

s.t. $\varphi = \eta \circ \pi$

We can define η as follows: For each $h \in H$ there is a $g \in G$ such that $\pi(g) = h$, we can then define $\eta(h) = f(g)$. It can be checked that this is a well defined group homomorphism. Next, let us look at the kernel of this map η. I claim that $\mathrm{Ker}(\eta) = \pi(\mathrm{Ker}(\varphi))$. If $x \in \mathrm{Ker}(\eta)$ then $\eta(x) = 0$, since π is a surjective map therefore there exists a $y \in G$ such that $\pi(y) = x \Rightarrow \varphi(y) = \eta(\pi(y)) = \eta(x) = 0 \Rightarrow y \in \mathrm{Ker}(\varphi) \Rightarrow \pi(y) = x \in \pi(\mathrm{Ker}(\varphi)) \Rightarrow \mathrm{Ker}(\eta) \subseteq \pi(\mathrm{Ker}(\varphi))$. For the other direction, suppose $x \in \pi(\mathrm{Ker}(\varphi))$, then there exists $y \in \mathrm{Ker}(\varphi)$ such that $\pi(y) = x \Rightarrow \eta(x) = \eta(\pi(y)) = \eta(x) = 0 \Rightarrow x \in \mathrm{Ker}(\eta) \Rightarrow \pi(\mathrm{Ker}(\varphi)) \subseteq \mathrm{Ker}(\varphi)$. Moreover, from the first isomorphism theorem we have $\mathrm{Ker}(\varphi)/\mathrm{Ker}(\phi) \cap \mathrm{Ker}(\pi) \cong \pi(\mathrm{Ker}(\varphi)) \Rightarrow \mathrm{Ker}(\varphi)/\mathrm{Ker}(\pi) \cong \pi(\mathrm{Ker}(\varphi))$.

Now, let us go back to our proof of the lemma and use this result. We observed that ψ factors through φ and therefore we have the following diagram

$$\begin{tikzcd}
\mathbb{Z}[X] \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & \mathbb{Z}[X]/\langle 1-X, p\rangle = \mathbb{F}_p \\
& \mathbb{Z}[X]/\langle f(X)\rangle = \mathbb{Z}[\omega] \arrow[ur, dashed, "\eta"'] &
\end{tikzcd}$$

s.t. $\eta = \psi \circ \varphi$

From the claim proven in the previous paragraph we have $\mathrm{Ker}(\eta) = \mathrm{Ker}(\psi)/\mathrm{Ker}(\varphi) = \langle 1-X, p\rangle/\langle f(X)\rangle = \langle 1-\omega, p\rangle = \langle 1-\omega\rangle$ since $p \equiv f(\omega) \equiv 0 \pmod{1-\omega}$. Therefore by the first isomorphism theorem again we have $\mathbb{Z}[\omega]/\langle 1-\omega\rangle \cong \mathbb{F}_p$. $\square$

Lemma 4.5. *Let $0 \not\equiv g(x) \in \mathbb{F}_p[X]$ be a polynomial of degree less than p. Then, the multiplicity of any element $0 \neq a \in \mathbb{F}_p$ as a root of $g(X)$ is strictly less than the number of nonzero coefficients of $g(X)$.*

Proof. Proof by induction. Say $g(x)$ were constant, then our proposition is trivially true. Now, suppose the proposition is true for all polynomials of degree less than $\deg(g) = k, 1 \leq k \leq p$. Consider the case when $g(0) = 0$ (has no constant term). Here, $g(X)/X$ is a nonzero polynomial with degree less than k, therefore by the induction hypothesis, the proposition is true for $g(X)/X$, but $g(X)$ and $g(X)/X$ have the same number of nonzero coefficients, therefore the claim is true for $g(X)$ as well. Next, say $g(0) \neq 0$. Take the derivative of $g(X)$ that is $g'(X)$. $g'(X)$ is a nonzero polynomial with degree less than k and therefore by induction hypothesis, the proposition is true for $g'(X)$. Since, the multiplicity of $0 \neq a \in \mathbb{F}_p$ as a root of $g(X)$ can exceed that of $g'(X)$ by atmost 1, therefore the proposition is true for $g(X)$ as well. And, we are done. □

Proof of proposition 4.2. Take $J, K \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|J| = |K|$. We want to say that

$$\det(\omega^{j \cdot k})_{j \in J, k \in K} \neq 0$$

OR, in terms of simple linear algebra

$$\begin{pmatrix} \omega^{1\cdot 1} & \omega^{1\cdot 2} \cdots & \omega^{1\cdot |K|} \\ \omega^{2\cdot 1} & \omega^{2\cdot 2} \cdots & \omega^{2\cdot |K|} \\ \vdots & \vdots & \vdots \\ \omega^{|J|\cdot 1} & \omega^{|J|\cdot 2} \cdots & \omega^{|J|\cdot |K|} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{|K|} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

the system above has no nontrivial solution.
So, let us focus attention on the polynomial $P(z) = \sum_{k \in K} x_k z^k \in \mathbb{Z}[\omega][X]$. Since $P(z)$ vanishes at $\omega^j \ \forall \ j \in J$, therefore $\prod_{j \in J}(z - \omega^j) \mid P(z)$. Applying lemma 4.4 to the coefficients of $P(z)$ we obtain the polynomial $\bar{P}(z)$ divisible by $(z-1)^{|J|}$. Next, we observe that $\bar{P}(z)$ has atmost $|K|$ nonzero coefficients and $|J| = |K|$, therefore $\bar{P}(z)$ has atleast $|K|$ multiplicity for a nonzero root which is a contradiction to lemma 4.5. This implies that $\bar{P}(z) \equiv 0$ which means $1 - \omega \mid P(z)$. Divide $P(z)$ by $1 - \omega$ and repeat the argument. We can keep doing this indefinitely unless $x_k = 0 \ \forall \ k \in K$. Thus, we have proven what we wanted. □

Now that we have proved proposition 4.2, let us proceed with the proof of theorem 4.1.
A simple consequence of proposition 4.2 is

Corollary 4.6. *Let p be a prime, $A, \tilde{A}$ be nonzero subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| = |\tilde{A}|$. The linear transform $T : \ell^2(A) \longrightarrow \ell^2(\tilde{A})$ defined by $Tf = \hat{f}|_{\tilde{A}}$ is invertible.*
$\ell^2(A)$ denotes all the functions f that vanish outside A.

Proof. If we look at the fourier transform matrix, then this corollary follows directly from proposition 4.2. □

4.4 Proof of the main theorem of Tao

Proof of theorem 4.1. The first part is a proof by contradiction. Suppose

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \leq p$$

Let $A = \operatorname{supp} f$. We choose a set $\tilde{A}$ disjoint from $\operatorname{supp} \hat{f}$ such that $|A| = |\hat{A}|$ (this can be done because once we remove all the elements of $\operatorname{supp} \hat{f}$ from $\mathbb{Z}/p\mathbb{Z}$, we are left with $p - |\operatorname{supp} \hat{f}| \geq |A|$ elements). This means $Tf = \hat{f}|_{\tilde{A}} = 0$ but $f \neq 0$ which is a contradiction to corollary corollary 4.6. Therefore our assumption is wrong. We must have

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \geq p + 1$$

For the second part, it suffices to prove the theorem for the case $|A| + |B| = p + 1$. Say $|A| = k$. If we choose an $\tilde{A}$ of size k as disjoint as possible from B (if we remove all the elements of B from $\mathbb{Z}/p\mathbb{Z}$, we are left with $p - |B| = |A| - 1$ elements), then we get $\tilde{A}$ such that $\tilde{A} \cap B = \{\xi\}$. By the corollary corollary 4.6, T is invertible, that is we can find a $f \in \ell^2(A)$ such that $\hat{f}$ vanishes on $\tilde{A} \backslash \{\xi\}$ and is nonzero on ξ. Such a function is nontrivial, must be nonzero on all of A and nonzero on all of B. Since this contradicts the uncertainty principle proved in the first part, we must have

$$\operatorname{supp} f = A, \operatorname{supp} \hat{f} = B$$

This completes the proof. □

5 Generalisation of Tao's result

Well, we see that the key idea in Tao's paper is the non vanishing nature of the determinant of the Fourier transform matrix. After the simple case of $\mathbb{Z}/p\mathbb{Z}$, the question is: for what other group does this condition hold (with or without extra conditions). It turns out that such a condition is true for $\mathbb{Z}/m\mathbb{Z}$ where m is composite, albeit with an extra condition. We will see what the condition and the result is.

Theorem 5.1. *Let $m > 1$ be an integer and let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ be a nonzero function. If $P(\operatorname{supp} f)$ or $P(\operatorname{supp} \hat{f})$ holds, then*

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \geq m + 1$$

Conversely, suppose A, B are nonzero subsets of $\mathbb{Z}/m\mathbb{Z}$ satisfying $|A| + |B| \geq m + 1$. If $P(A)$ holds, then there is a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that $\operatorname{supp} f \subseteq A$ and $\operatorname{supp} \hat{f} = B$. Furthermore, if $P(B)$ holds, then f can be made to satisfy $\operatorname{supp} f = A$.

Here as well, we try to get a proposition similar to the one due to Tao (proposition 4.2). But before we state the proposition, let us note down a result on vanishing sums of roots of unity which is turn out to be useful later on.

Lemma 5.2. *Let $m = p_1^{a_1} \cdots p_r^{a_r}$. If $W(m) = \{n \in \mathbb{Z}_{\geq 0} : \omega_1 + \cdots + \omega_n = 0\}$ where ω_i is a primitive m-th root of unity, then*

$$W(m) = \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$$

This result is due to [8].

5.1 Main proposition

5.1.1 Background on $U(n)$, its representation, Weyl formulae

Let n be a positive integer, and $U(n)$ be the group of complex unitary matrices. We know that $U(n)$ is a compact, connected and real Lie group.

Proposition 5.3. *Every compact, connected Lie group has a maximal torus.*

Proof. Every group has a tori, namely $\{e\}$. Let $\{e\} = T_1 \subseteq T_2 \subseteq \cdots \subseteq T_i \subseteq \cdots$ be a sequence of tori. Then, we note that the increasing sequence $\dim(T_i)$ is bounded by $\dim(G)$ and thus the sequence has to be constant after a while and therefore a maximal torus has to exist. □

Proposition 5.4. *The maximal torus of $U(n)$ is the group of all diagonal matrices T, where an element of T is of the form $t = \operatorname{diag}(e^{it_1}, \cdots, e^{it_n})$ with $t_i \in \mathbb{R}$.*

Proof. This group T is definitely isormorphic to $\mathbb{T}^n$. Say there is another maximal torus that is strictly larger than than T. Take an element $g \in U(n)$ that commutes with every element of T. But then g has to have the same eigenvalues as T and therefore diagonal. Hence, proved. □

For the rest of this section, we will use the following notation.
By *weight*, we mean a sequence $\kappa = (\kappa_1, \ldots, \kappa_n) \in \mathbb{Z}^n$. We call the weight *dominant* if $\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_n$ and strictly dominant if the inequalities are strict. Given a weight κ, we define a function $f_\kappa : T \to \mathbb{C}$ by setting $f_\kappa(t) = d_1^{\kappa_1} \cdot d_2^{\kappa_2} \cdots d_n^{\kappa_n}$ for $t \in T$

Proposition 5.5. *Any element of a compact, connected Lie group is a conjugate to an element of its maximal torus.*

Proof. This is called the Cartan's theorem and proof can be found in [2]'s chapter 16-17. □

Using this Proposition, we note that any element of $U(n)$ is conjugate to some element $t \in T$. And since character is a class function, it is defined by its behaviour on T. Next, we note a really powerful and useful formula that will come in handy later in the section.

Proposition 5.6 (Weyl Character Formula)**.** *Each dominant weight λ corresponds to a unique irreducible χ_λ of $U(n)$, given by*

$$\chi_\lambda(t) = \frac{\sum_{s\in S_n} \mathrm{sgn}(s) e^{s\cdot(\lambda+\rho)}(t)}{\sum_{s\in S_n} \mathrm{sgn}(s) e^{s\cdot\rho}(t)} = \frac{\det(d_i^{\lambda_j+\rho_j})}{\det(d_i^{\rho_j})}$$

In the above theorem, the action of $s \in S_n$ on κ is given by $s \cdot \kappa = (\kappa_{s^{-1}(1)}, \ldots, \kappa_{s^{-1}(n)})$. The proof of this theorem is standard and can be found in [6].
For more theory of compact Lie groups and representation theory, please refer to [1], [2], [12].

5.1.2 Proof of the main proposition

Proposition 5.7. *Let $m = p_1^{a_1} \cdots p_r^{a_r}$. Let $\iota_1, \ldots, \iota_n$ and $\kappa_1, \ldots, \kappa_n$ be integers distinct modulo m such that*

$$\frac{\prod_{1\le i<j\le n} |\kappa_i - \kappa_j|}{\prod_{1\le i<j\le n} (j-i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$$

Then $\det(\omega^{\iota_i \cdot \kappa_j}) \neq 0$, where m-th root of unity.

Proof. Let $\omega_i = \omega^{\iota_i}$. Rearrange $\kappa_1, \ldots, \kappa_n$ if necessary to obtain a dominant weight $\kappa = (\kappa_1, \ldots, \kappa_n)$. Now, we want to prove that $\chi_\lambda(\omega_1, \ldots, \omega_n) \neq 0$ where $\lambda = \kappa - \rho$.
Let the representation of $U(n)$ corresponding to χ_λ be π_λ. Denote $\Omega = \mathrm{diag}(\omega_1, \ldots, \omega_n) \in U(n)$. Since a representation is a group homomorphism, and $\Omega^m = 1 \Rightarrow \pi_\lambda(\Omega)^m = 1$. Thus, every eigenvalue of π_λ is a m-th root of unity. Since $\chi_\lambda(\Omega) = \mathrm{tr}(\pi_\lambda)$ is a sum of m-th roots of unity, there are exactly $\deg(\chi_\lambda)$ of them (with multiplicity). If $\chi_\lambda(\Omega)$ were indeed 0, then by lemma 5.2 we have $\deg(\chi_\lambda) \in \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$. Using the dimension formula leads to a contradiction to our hypothesis. Thus, our assumption is wrong. We must have $\chi_\lambda(\Omega) \neq 0$. □

Now that we have a "Tao-like" proposition, we expect a corollary similar as corollary 4.6. We obtain the following

Corollary 5.8. *Let $A, \tilde{A} \subseteq \mathbb{Z}/m\mathbb{Z}$ be nonempty subsets of equal cardinalities. If $P(\mathrm{supp}\, f)$ or $P(\mathrm{supp}\, \hat{f})$ holds, then the linear map $T : \ell^2(A) \longrightarrow \ell^2(\tilde{A})$ given by $Tf = \hat{f}\mid_{\tilde{A}}$ is an isomorphism.*

Proof. The coefficient matrix of T is exactly the one we have in lemma 5.2 and the result follows from lemma 5.2. □

Proof of theorem 5.1. We proceed in a similar manner as Tao. For the first statement, we shall assume to the contrary that $|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \leq m$. First, let us solve for the case $P(\operatorname{supp} f)$ holds. Get a set $\tilde{A} \subseteq \mathbb{Z}/m\mathbb{Z}$ such that $|\operatorname{supp} f| = |\tilde{A}|$ and $\tilde{A} \cap \operatorname{supp} \hat{f} = \phi$. Since f is nonzero, we have $Tf \neq 0$ due to corollary 5.8, but $\operatorname{supp} \hat{f} \cap \tilde{A} = \operatorname{supp} Tf \neq \emptyset$, a contradiction to our assumption. Thus, our assumption must be wrong and we have the required claim. In the case that $P(\operatorname{supp} \hat{f})$ holds, the same reasoning will give us what we need but we consider a different function using the fourier inversion formula. Let g be the function given by $g(x) = \hat{f}(-x)$. Here, $\operatorname{supp} g = \{-x : x \in \operatorname{supp} \hat{f}\}$, this implies $P(\operatorname{supp} g)$ holds, therefore from the earlier part we have

$$|\operatorname{supp} g| + |\operatorname{supp} \hat{g}| \geq m + 1$$

And, from Fourier inversion formula

$$\mathcal{F}(\hat{g})(x) = \mathcal{F}(\mathcal{F}(g))(x) = \frac{1}{m} g(-x) = \frac{1}{m} \hat{f}(x)$$

This means that $m\hat{g} = f$ by the uniqueness of Fourier transform, and thus we get $|\operatorname{supp} \hat{g}| = |\operatorname{supp} f|$. Finally, we have

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \leq m + 1$$

Now, for the converse. It suffices to prove the claim for the case $|A| + |B| = m + 1$. When $|A| + |B| > m + 1$, we can simply apply the claim to the pair $A, B' \subseteq B$ such that $|A| + |B'| = m + 1$ and take generic linear combinations to get the required function f as in the case of Tao.
Therefore, assume $|A| + |B| = m + 1$ and let $P(A)$ holds. For every $\beta \in B$, let $A_\beta = \mathbb{Z}/m\mathbb{Z} \backslash (B \backslash \{\beta\})$. Note that $|A = |\tilde{A}|$ and by corollary 5.8 there exists $f_\beta \in \ell^2(A)$ such that $\hat{f}_\beta$ vanishes on $A \backslash \{\beta\}$ and nonzero at β. Thus we have $\operatorname{supp} \hat{f}_\beta \subseteq B$ for each $\beta \in B$. Taking linear combinations of each such f_β we can obtain a function $f \in \ell^2(A)$ such that $\operatorname{supp} \hat{f} = B$.
Now, suppose $P(\operatorname{supp} \hat{f})$ holds as well. Then $P(-B)$ also holds and thus by the observation made just before this, we can find a function $g \in \ell^2(B)$ such that $\operatorname{supp} \hat{g} = A$. Let $h_1 = \hat{g}$, so that $\operatorname{supp} h_1 = \operatorname{supp} \hat{g} = A$. From the Fourier inversion formula, we obtain $\operatorname{supp} \hat{h_1} \subseteq B$. If $h_2 \in \ell^2(A)$ be such that $\operatorname{supp} \hat{h_2} = B$. Taking linear combination of h_1, h_2 gives us the required function $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that $\operatorname{supp} \varphi = A, \operatorname{supp} \hat{\varphi} = B$ as we wanted. Hence, we have proved the theorem. □

6 Applications of the Uncertainty Principles thus obtained

6.1 Classical Cauchy-Davenport theorem and a variant

Theorem 6.1. *If* $0 \neq A, B \subseteq \mathbb{Z}/p\mathbb{Z}$*, then the sumset* $A + B = \{a + b | a \in A, b \in B\}$ *has the bound*

$$|A + B| \geq \min\{|A| + |B| - 1, p\}$$

Proof. Let A, B be the required subsets of $\mathbb{Z}/p\mathbb{Z}$. Now, take two subsets X, Y of A, B respectively such that $|X| = p + 1 - |A|, |Y| = p + 1 - |B|$. Using the result in theorem 4.1 we get two functions f, g such that $\operatorname{supp} f = X, \operatorname{supp} \hat{f} = A$ and $\operatorname{supp} g = Y, \operatorname{supp} \hat{g} = B$. Let us investigate the convolution $f * g$. If $x \notin A + B$, then for any $y \in B$ we have a $x - y \in A$, this means $f(x - y)g(y) = 0 \ \forall y \in B$ and therefore $z \notin \operatorname{supp}(f * g)$, this implies $\operatorname{supp}(f * g) \subseteq A + B$. From the convolution theorem we have $\widehat{f * g}(\chi) = \hat{f}(\chi) \cdot \hat{g}(\chi)$. This means $\operatorname{supp}(\widehat{f * g}) = X \cap Y$. Note that

$$|X \cap Y| = |X| + |Y| - |X \cup Y|$$

and therefore

$$|X \cap Y| = \max\{|X| + |Y| - p, 1\}$$

Using all this information we have

$$\begin{aligned} |\operatorname{supp}(f * g)| + |\operatorname{supp}(\widehat{f * g})| &\geq p + 1 \\ |A + B| + |X \cap Y| &\geq p + 1 \\ |A + B| &\geq p + 1 - \max\{|X| + |Y| - p, 1\} \\ |A + B| &\geq \min\{|A| + |B| - 1, p\} \end{aligned}$$

This finishes the proof. □

Theorem 6.2. *If* $0 \neq A, B \subseteq \mathbb{Z}/m\mathbb{Z}$*, then the sumset* $A + B = \{a + b | a \in A, b \in B\}$ *has the bound*

$$|A + B| \geq \min\{|A| + |B| - 1, m\}$$

Proof. We proceed as in theorem 6.1. Let A, B be the required subsets of $\mathbb{Z}/m\mathbb{Z}$. Now, take two subsets X, Y of A, B respectively such that $|X| = m + 1 - |A|, |Y| = m + 1 - |B|$. Note that

$$|X \cap Y| = |X| + |Y| - |X \cup Y|$$

and therefore

$$|X \cap Y| = \max\{|X| + |Y| - m, 1\}$$

Note that we can choose X, Y such that $P(X \cap Y)$ holds (choose X, Y such that $X \cap Y$ is an arithmetic progression with common difference 1). By theorem 5.1 we can get functions f, g such that

$$\operatorname{supp} f \subseteq A, \operatorname{supp} \hat{f} = X, \operatorname{supp} g = B, \operatorname{supp} \hat{g} = Y$$

Next, due to arguments similar to the proof in theorem 6.1 $\text{supp}\,(f * g) \subseteq A + B, \text{supp}\,(\widehat{f * g}) = X \cap Y$. Since $P(X \cap Y)$ holds and $f * g$ is nonzero, due to theorem 5.1 we have

$$\begin{aligned} |\text{supp}\,(f * g)| + |\text{supp}\,(\widehat{f * g})| &\geq m + 1 \\ |A + B| + |X \cap Y| &\geq m + 1 \\ |A + B| &\geq p + 1 - \max\{|X| + |Y| - m, 1\} \\ |A + B| &\geq \min\{|A| + |B| - 1, m\} \end{aligned}$$

□

6.2 Roots of sparse polynomials

An immediate consequence of Tao's result is as follows. Any sparse polynomial $p(z) = \sum_{j=1}^{k} c_k z^{n_j}$ with $k+1$ nonzero coefficients and $0 < n_0 < \cdots < n_k < p$ when restricted to the p-th roots of unity, can have atmost k roots. For if we view $p(\omega^i)$ as a function of $i \in \mathbb{Z}/p\mathbb{Z}$ with ω being a p-th root of unity, we notice that $p(z)$ has a Fourier transform whose support size is $k + 1$, and therefore the support of the polynomial is atleast $p - k$ by theorem 4.1. This implies that $p(z)$ has atmost k zeroes.

Since, we also saw the generalisation of Tao's result, a natural question to ask is whether a similar result holds there as well. Indeed, there is a similar result. Any sparse polynomial $p(z) = \sum_{j=1}^{k} c_k z^{\kappa_j}$ with $k + 1$ nonzero coefficients, when restricted to the m-th roots of unity, and

$$\frac{\prod_{1 \leq i < j \leq n} |\kappa_i - \kappa_j|}{\prod_{1 \leq i < j \leq n} (j - i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$$

can have atmost k roots. For if we view $p(\omega^i)$ as a function of $i \in \mathbb{Z}/m\mathbb{Z}$ with ω being a m-th root of unity, we notice that $p(z)$ has a Fourier transform whose support size is $k + 1$, and therefore the support of the polynomial is atleast $m - k$ by theorem 5.1. This implies that $p(z)$ has atmost k zeroes.

7 Further result

Meschulam proves a very special result for a general finite abelian group. He proves that

Theorem 7.1. *Let $f \in L(G)$ s.t. $0 \neq |\text{supp} = k|$ and let $d_i = d_i(n, k)$ for $i = 1, 2$. Then,*

$$|\text{supp}\,\hat{f}| \geq \frac{n}{d_1 d_2}(d_1 + d_2 - k)$$

To prove this theorem, we will need the following lemmas.

Lemma 7.2. *Let H be a subgroup of G and $1 \leq k \leq |G| = n$. Then there exists integers $1 \leq s \leq |H|$ and $1 \leq t \leq |G/H|$ such that $st \leq k$ and*

$$\theta(G, k) \geq \theta(H, s) \cdot \theta(G/H, t)$$

The proof of this lemma requires us to define what the functions look like in $L(H)$ and $L(G/H)$ given that a function in $L(G)$ is given. And we also need to look at the corresponding fourier transforms. So, let us do that first.

Lemma 7.3. $H^{\perp} \cong \widehat{G/H}$

Proof. If $\chi \in H^{\perp}$, then it gives rise to a character $\tilde{\chi} \in \widehat{G/H}$ defined by $\tilde{\chi}(\overline{y}) = \chi(y)$. This gives the required isomorphism. □

Lemma 7.4. *For $\eta \in \hat{H}$ and $\chi \in H^{\perp}$,*

$$\hat{f}(\tilde{\eta} \cdot \chi) = \widehat{F_{\eta}}(\tilde{\chi})$$

Proof. Say $[G : H] = r$ and let $\{y_i \mid 1 \leq i \leq r\}$ be the left coset representatives of H.

$$\begin{aligned}
\hat{f}(\tilde{\eta} \cdot \chi) &= \sum_{x \in G} f(x)\tilde{\eta}(-x)\chi(-x) \\
&= \sum_{i=1}^{r} \sum_{z \in H} f(z + y_i)\tilde{\eta}(-z - y_i)\chi(-z - y_i) \\
&= \sum_{i=1}^{r} \left(\sum_{z \in H} f_{y_i}(z)\tilde{\eta}(-z) \right) \tilde{\eta}(-y_i)\chi(-z - y_i) \\
&= \sum_{i=1}^{r} \hat{f}_{y_i} \tilde{\eta}(-y_i)\chi(-y_i) \\
&= \sum_{i=1}^{r} F_{\eta}(\overline{y_i})\tilde{\chi}(-\overline{y_i}) \\
&= \widehat{F_{\eta}}(\tilde{\chi})
\end{aligned}$$

□

Proof of lemma 7.2. Let $f \in L(G), |\operatorname{supp} f| = k > 0$ and keep the notations same as in lemma 7.4. Next we define a set

$$I = \{i \mid 1 \leq i \leq r, \operatorname{supp} f \cap (y_i + H) \neq \phi\}$$

Say $|I| = t$. For $\eta \in \widehat{H}$, if $j \notin I$ then $\operatorname{supp} f \cap (y_j + H) = \phi \Rightarrow f(z + y_j) = 0 \forall z \in H \Rightarrow f_{y_j}(z) = 0 forall z \in H \Rightarrow F_{\eta}(\overline{y}_j) = 0 \Rightarrow |\operatorname{supp} F_{\eta}| \leq |I| = t$. Next, by definition of $\theta(G/H, t)$ we have

$$|\operatorname{supp} \widehat{F}_{\eta}| \geq \theta(G/H, t)$$

Before we proceed further let us make a small observation: If the sum of p things is atmost q, then atleast one of them is atmost q/p.
This means there is an $i \in I$ such that $1 \leq |\operatorname{supp} f_{y_i}| \leq k/t$. Next, we choose an integer s appropriately such that $st \leq k$. Let $A = \operatorname{supp} \widehat{f_{y_i}} \subset \widehat{H}$. By definition, we have $|A| \geq \theta(H, s)$.
Since $F_\eta(\overline{y_i}) = \widehat{f_{y_i}} \tilde{\eta}(y_i) \neq 0 \ \forall \ \eta \in A$. Using lemma 7.4 and the other two bounds we obtained above, we have

$$|\operatorname{supp} \widehat{f}| = \sum_{\eta \in \widehat{H}} |\operatorname{supp} \widehat{F}_\eta| \geq \sum_{\eta \in A} |\operatorname{supp} \widehat{F}_\eta| \geq \theta(H, s)\theta(G/H, t)$$

□

Lemma 7.5. *For any divisor d of n and for any $1 \leq s \leq d, 1 \leq t \leq n/d$, we have*

$$u(d, s) \cdot u\left(\frac{n}{d}, t\right) \geq u(n, st)$$

Proof. Let $k = st, a_i = d_i(d, s), b_i = d_i(n/d, t), c_i = d_i(n, k)$ for $i = 1, 2$.

- $a_1 \leq s \leq a_2$
- $b_1 \leq t \leq b_2$
- $sb_1 \leq k \leq sb_2$

$$\therefore m_1 = \max\{a_1, k/b_2\} \leq s \leq \min\{a_2, k/b_1\} = m_2$$

We want to show that

$$\frac{a_1 + a_2 - s}{a_1 a_2} \cdot \frac{b_1 + b_2 - k/s}{b_1 b_2} \geq \frac{c_1 + c_2 - k}{c_1 c_2}$$

Without loss of generality, less us assume that $a_1 b_1 \leq a_1 b_2 \leq a_2 b_1 \leq a_2 b_2$. Let us investigate the three cases

1. $a_1 b_1 \leq k \leq a_1 b_2$
   Since both $a_1 b_1, a_1 b_2$ are divisors of n, we must have $a_1 b_1 \leq c_1 \leq k \leq c_2 \leq a_1 b_2$. Convexity of u means we just have to prove

   $$\frac{a_1 + a_2 - s}{a_1 a_2} \cdot \frac{b_1 + b_2 - k/s}{b_1 b_2} \geq \frac{a_1 b_1 + a_1 b_2 - k}{a_1 b_1 a_1 b_2}$$

   or equivalently

   $$a_1(a_1 + a_2 - k)(b_1 + b_2 - k/s) \geq a_1 a_2 b_1 + a_1 a_2 b_2 - a_2 k$$

   In this case we have $m_1 = a_1 \leq s \leq m_2 = k/b_1$. By convexity, we just have to check the extreme cases

   (a) For $s = a_1$, the condition holds with equality

   (b) For $s = k/b_1$, we have $a_1(a_1 + a_2 - s)b_2 \geq a_1a_2b_1 + a_1a_2b_2 - a_2b_1s \Rightarrow a_1^2b_2 - a_1b_2s - a_1a_2b_1 + a_2b_1s \geq 0 \Rightarrow a_1(a_1b_2 - a_2b_1) - s(a_1b_2 - a_2b_1) \geq 0 \Rightarrow (a_1b_2 - a_2b_1)(a_1 - s) \geq 0$ which definitely holds.

2. $a_1b_2 \leq k \leq a_2b_1$
   Since both a_1b_2, a_2b_1 are divisors of n, we must have $a_1b_2 \leq c_1 \leq k \leq c_2 \leq a_2b_1$. Convexity of u means we just have to prove

   $$\frac{a_1 + a_2 - s}{a_1a_2} \cdot \frac{b_1 + b_2 - k/s}{b_1b_2} \geq \frac{a_1b_2 + a_2b_1 - k}{a_1b_2a_2b_1}$$

   or equivalently

   $$(a_1 + a_2 - s)(b_1 + b_2 - k/s) \geq a_1b_2 + a_2b_1 - k$$

   In this case we have $m_1 = k/b_2 \leq s \leq m_2 = k/b_1$. By convexity, we just have to check the extreme cases

   (a) For $s = k/b_2$, the condition is $a_1b_1 - sb_1 \geq a_1b_2 - sb_2 \Rightarrow a_1(b_1 - b_2) - s(b_1 - b_2) \geq 0 \Rightarrow (b_2 - b_1)(s - a_1) \geq 0$. This is obviously true.

   (b) For $s = k/b_1$, we have $a_2b_2 - sb_2 \geq a_2b_1 - sb_1 \Rightarrow a_2(b_2 - b_1) - s(b_2 - b_1) \geq 0 \Rightarrow (b_2 - b_1)(a_2 - s) \geq 0$ which definitely holds.

3. $a_2b_1 \leq k \leq a_2b_2$
   Since both a_2b_1, a_2b_2 are divisors of n, we must have $a_2b_1 \leq c_1 \leq k \leq c_2 \leq a_2b_2$. Convexity of u means we just have to prove

   $$\frac{a_1 + a_2 - s}{a_1a_2} \cdot \frac{b_1 + b_2 - k/s}{b_1b_2} \geq \frac{a_2b_1 + a_2b_2 - k}{a_2b_1a_2b_2}$$

   or equivalently

   $$a_2(a_1 + a_2 - k)(b_1 + b_2 - k/s) \geq a_1a_2b_1 + a_1a_2b_2 - a_1k$$

   In this case we have $m_1 = k/b_2 \leq s \leq m_2 = a_2$. By convexity, we just have to check the extreme cases

   (a) For $s = k/b_2$, we have $a_2(a_1 + a_2 - s)b_1 \geq a_1a_2b_1 + a_1a_2b_2 - a_2b_1s \Rightarrow a_2^2b_1 - a_2b_1s - a_1a_2b_2 + a_1b_2s \geq 0 \Rightarrow a_2(a_2b_1 - a_1b_2) - s(a_2b_1 - a_1b_2) \geq 0 \Rightarrow (a_2b_1 - a_1b_2)(a_2 - s) \geq 0$ which definitely holds.

   (b) item For $s = a_2$, the condition holds with equality.

□

Lemma 7.6. *If ℓ is an integer such that $\ell \leq k$, then $u(n, \ell) \geq u(n, k)$*

Proof. Let $d_i = d_i(n, k), \tilde{d}_i = d_i(n, \ell)$.
By definition, $\tilde{d}_i \leq d_i, i = 1, 2$.

$$\frac{1}{\tilde{d}_i} \geq \frac{1}{d_i}$$
$$\frac{n}{\tilde{d}_1} + \frac{n}{\tilde{d}_2} \geq \frac{n}{d_1} + \frac{n}{d_2}$$
$$\frac{-n\ell}{\tilde{d}_1\tilde{d}_2} \geq \frac{-nk}{d_1 d_2}$$

Using the equations above, we can conclude the following

$$\frac{n}{\tilde{d}_1} + \frac{n}{\tilde{d}_2} - \frac{n\ell}{\tilde{d}_1\tilde{d}_2} \geq \frac{n}{d_1} + \frac{n}{d_2} - \frac{nk}{d_1 d_2}$$
$$\frac{n}{\tilde{d}_1\tilde{d}_2}(\tilde{d}_1 + \tilde{d}_2 - l) \geq \frac{n}{d_1 d_2}(d_1 + d_2 - k)$$
$$u(n, \ell) \geq u(n, k)$$

□

Lemma 7.7. *Let G be a finite abelian group with $|G| = n$. If d is a divisor of n, then there is a subgroup of G of order d.*

Proof. Let $n = p_1^{a_1} \cdots p_r^{a_r}$, and say $d \mid n$. If $d = 1$, then we are trivially done. Say $d \neq 1$, then $p_i \mid d$ for some i. By Cauchy's theorem, there is a subgroup K of G such that $|K| = p_i$. $|G/K| < |G|$ and therefore by induction hypothesis, there is a subgroup H/K of G/K such that $|H/K| = d/p_i$. By the third isomorphism theorem,

$$\frac{G/K}{H/K} \cong G/H$$

This corresponds to finding subgroup H of G such that $|H| = d$. □

Proof of theorem 7.1. We want to prove $\theta(G, k) \geq u(n, k)$ by induction. The case $n = p$ translates to Tao's claim. Suppose the proposition is true for all groups of order less than $|G| = n$. Let H be the subgroup of order d by lemma 7.7. By lemma 7.2, there exists integers $1 \leq s \leq |H|$ and $1 \leq t \leq |G/H|$ such that $st \leq k$ and $\theta(G, k) \geq \theta(H, s) \cdot \theta(G/H, t)$. Invoking the induction hypothesis and using lemma 7.6 for $H, G/H$, we get

$$\theta(G, k) \geq \theta(H, s) \cdot \theta(G/H, t) \geq u(d, s)u(n/d, t) \geq u(n, st) \geq u(n, k)$$

This proves our claim. □

References

[1] Theodor Bröcker et al. *Representations of Compact Lie Groups*. eng. Nachdr. Graduate Texts in Mathematics 98. New York: Springer, 2010. ISBN: 9783642057250.

[2] Daniel Bump. *Lie Groups*. Springer New York, 2013.

[3] Keith Conrad. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf.

[4] David L. Donoho and Philip B. Stark. "Uncertainty Principles and Signal Recovery". en. In: *SIAM Journal on Applied Mathematics* 49.3 (June 1989), pp. 906–931. ISSN: 0036-1399, 1095-712X. DOI: 10.1137/0149053. URL: http://epubs.siam.org/doi/10.1137/0149053.

[5] P. E. Frenkel. *Simple proof of Chebotarev's theorem on roots of unity*. Tech. rep. arXiv:math/0312398. arXiv:math/0312398 type: article. arXiv, July 2004. URL: http://arxiv.org/abs/math/0312398.

[6] James E. Humphreys. *Introduction to Lie algebras and representation theory*. Graduate texts in mathematics 9. New York: Springer-Verlag, 1972. ISBN: 9780387900537 9780387900520.

[7] Shigeru Kanemitsu and Michel Waldschmidt. "MATRICES OF FINITE ABELIAN GROUPS, FINITE FOURIER TRANSFORM AND CODES". en. In: *Number Theory: Arithmetic in Shangri-La*. Shanghai, China: WORLD SCIENTIFIC, Apr. 2013, pp. 90–106. ISBN: 9789814452441 9789814452458. DOI: 10.1142/9789814452458_0005. URL: http://www.worldscientific.com/doi/abs/10.1142/9789814452458_0005.

[8] T. Y. Lam and K. H. Leung. *On vanishing sums for roots of unity*. Tech. rep. arXiv:math/9511209. arXiv:math/9511209 type: article. arXiv, Nov. 1995. URL: http://arxiv.org/abs/math/9511209.

[9] Roy Meshulam. "An uncertainty inequality and zero subsums". en. In: *Discrete Mathematics* 84.2 (Sept. 1990), pp. 197–200. ISSN: 0012365X. DOI: 10.1016/0012-365X(90)90375-R. URL: https://linkinghub.elsevier.com/retrieve/pii/0012365X9090375R.

[10] Roy Meshulam. *An uncertainty inequality for finite abelian groups*. Tech. rep. arXiv:math/0312407. arXiv:math/0312407 type: article. arXiv, Dec. 2003. URL: http://arxiv.org/abs/math/0312407.

[11] M. Ram Murty and Junho Peter Whang. "The uncertainty principle and a generalization of a theorem of Tao". en. In: *Linear Algebra and its Applications* 437.1 (July 2012), pp. 214–220. ISSN: 00243795. DOI: 10.1016/j.laa.2012.02.009. URL: https://linkinghub.elsevier.com/retrieve/pii/S0024379512001395.

[12] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Vol. 42. Graduate Texts in Mathematics. New York, NY: Springer New York, 1977. ISBN: 9781468494600 9781468494587. DOI: 10.1007/978-1-4684-9458-7. URL: http://link.springer.com/10.1007/978-1-4684-9458-7.

[13] P. Stevenhagen and H. W. Lenstra. “Chebotarëv and his density theorem”. en. In: *The Mathematical Intelligencer* 18.2 (Mar. 1996), pp. 26–37. ISSN: 0343-6993. DOI: 10.1007/BF03027290. URL: http://link.springer.com/10.1007/BF03027290.

[14] Terence Tao. “An uncertainty principle for cyclic groups of prime order”. en. In: *Mathematical Research Letters* 12.1 (2005), pp. 121–127. ISSN: 10732780, 1945001X. DOI: 10.4310/MRL.2005.v12.n1.a11. URL: http://www.intlpress.com/site/pub/pages/journals/items/mrl/content/vols/0012/0001/a011/.

[15] Audrey Terras. *Fourier analysis on finite groups and applications*. London Mathematical Society student texts 43. Cambridge ; New York: Cambridge University Press, 1999. ISBN: 9780521451086.

[16] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Vol. 83. Graduate Texts in Mathematics. New York, NY: Springer New York, 1997. ISBN: 9781461273462 9781461219347. DOI: 10.1007/978-1-4612-1934-7. URL: http://link.springer.com/10.1007/978-1-4612-1934-7.