Nov 1st, 2025

Uncertainty Principle

Author: Yu Jiang, Fangke Li, Yang Qi, Jinxuan Zhu

Abstract

This report presents a study of the Uncertainty Principle across different mathematical domains. For finite abelian groups, we prove the textbook multiplicative uncertainty principle, and Tao's additive bound $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geq p+1$, leveraging Chebotarëv's lemma on the non-singularity of all submatrices of Fourier matrices. Then we generalize these principles to non-abelian finite groups using representation theory, where the Fourier transform is defined via irreducible representations. Relevant definitions and proofs constitute Section 1.

In the continuous setting of Section 2, we establish Heisenberg's inequality for Schwarz functions, provide an operator-theoretic interpretation from a physicist's perspective, and prove the Amrein-Berthier theorem on the impossibility of simultaneous concentration on sets of finite measure.

These principles admit further powerful generalizations in Section 3. We demonstrate extensions including uncertainty relations for numerically sparse vectors, bounds for the zeros of sparse polynomials over finite fields, and the Kahn-Kalai-Linial theorem on influences in Boolean functions, connecting harmonic analysis to combinatorics and number theory.

1 Discrete Uncertainty Principle

For the finite group, we can define its Fourier transform. For simplicity, the finite abelian group is considered first. Fix a finite abelian group, and define the Pontryagin dual $\hat{G}$ to be the group of all characters (a function $\chi : G \to \mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ is called a character if it obeys the multiplicative properties $\chi(x+x') = \chi(x)\chi(x')$). Clearly, the $\widehat{G}$ is an abelian group with $(\chi + \chi')(x) = \chi(x) \cdot \chi'(x)$. Besides, the number of elements in $\widehat{G}$ is just $|G|$. After these preparations, we can now give a definition of the Fourier transform for the finite abelian group.

Definition 1 *Let $f : G \to \mathbb{C}$, we may define the Fourier transform $\hat{f} : \widehat{G} \to \mathbb{C}$ as*

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

And if $\hat{f} : \hat{G} \to \mathbb{C}$, we can define the inverse Fourier transform by

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

1.1 Multiplicative Uncertainty Principle

To establish the uncertainty principle, let $\mathrm{supp}(f) = \{x \in G : f(x) \neq 0\}$. This can be similarly defined for $\hat{f}$. The following result is the uncertainty principle for the finite abelian group.

Theorem 2 *Let $f : G \to \mathbb{C}$ and $f \neq 0$, we have*

$$|\mathrm{supp}(f)||\mathrm{supp}(\hat{f})| \geq |G|.$$

Proof. By the inverse Fourier transform, we have

$$|f(x)| = \left| \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi(x) \right| \leq \sum_{\chi \in \widehat{G}} |\hat{f}(\chi)| = \sum_{\chi \in \mathrm{supp}(\hat{f})} |\hat{f}(\chi)|.$$

By the Cauchy-Schwarz inequality,

$$\|f\|_\infty^2 \leq \left(\sum_{\chi \in \widehat{G}} \mathbf{1}_{\chi \in \mathrm{supp}(\hat{f})} |\hat{f}(\chi)| \right)^2 \leq |\mathrm{supp}(\hat{f})| \left(\sum_{\chi \in \widehat{G}} |\hat{f}(\chi)|^2 \right).$$

Now using Plancherel's identity on the finite abelian group,

$$\|f\|_\infty^2 \leq |\mathrm{supp}(\hat{f})| \left(\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 \right) \leq \frac{1}{|G|} |\mathrm{supp}(\hat{f})||\mathrm{supp}(f)| \cdot \|f\|_\infty^2. \tag{1}$$

Now we have proved our result. ■

The above result for the multiplication of support is actually optimal. In fact, if we choose a function δ_H satisfies $\delta_H(x) = \mathbf{1}_{x\in H}$, where H is any subgroup of a cyclic group G, a directed calculation shows that

$$|\operatorname{supp}(\delta_H)| = |H|, \quad |\operatorname{supp}(\widehat{\delta_H})| = |G|/|H|.$$

Proposition 3 *Conversely, for a cyclic group G, if there exists a function $f : G \mapsto \mathbb{C}$ that satisfies $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| = |G|$, with $0 \in \operatorname{supp}(f)$ and $\mathbf{1}_G \in \operatorname{supp}(\hat{f})$, then $\operatorname{supp}(f)$ must be a subgroup of G, and $\operatorname{supp}(\hat{f})$ is a subgroup of $\hat{G}$.*

Proof. Let $M = |\operatorname{supp}(f)|$ and $N = |G|$. We may assume that $G = \mathbb{Z}/N\mathbb{Z}$. Suppose $\operatorname{supp}(f) = \{x_1, \ldots, x_M\} \subseteq G$. We define the homomorphism $\phi : G \mapsto \hat{G}$ by $\phi(k)(r) = e^{2\pi ikr/N}$. Our goal is to prove that $\hat{f} \circ \phi$ does not have M consecutive zeros.

We represent the M consecutive terms in $\hat{f}$ using a vector $w^{(p)} \in \mathbb{C}^M$, where

$$w_k^{(p)} = \hat{f}(\phi(p+k)) = \frac{1}{N}\sum_{j=1}^{M} f(x_j)e^{-2\pi i(p+k)x_j/N}.$$

Next, we can write the Fourier transform in matrix form:

$$w^{(p)} = \frac{1}{N}\begin{pmatrix} e^{-2\pi i(p+1)x_1/N} & \cdots & e^{-2\pi i(p+1)x_M/N} \\ \vdots & \ddots & \vdots \\ e^{-2\pi i(p+M)x_1/N} & \cdots & e^{-2\pi i(p+M)x_M/N} \end{pmatrix}\begin{pmatrix} f(x_1) \\ \vdots \\ f(x_M) \end{pmatrix} = \frac{1}{N}(z_j^{p+i})_{1\le i,j\le M}\boldsymbol{u}.$$

Thus $w^{(p)} = \mathbf{0}$ if and only if $\boldsymbol{u}$ is in the kernel of the matrix $(z_j^{p+i})_{1\le i,j\le M}$. Since $\boldsymbol{u} \neq \mathbf{0}$, it suffices to show that $\det(z_j^{p+i})_{1\le i,j\le M} \neq 0$ to prove that $w^{(p)} \neq \mathbf{0}$. We compute the determinant:

$$\det(z_j^{p+i})_{1\le i,j\le M} = z_1^p \cdots z_M^p \begin{vmatrix} z_1 & \cdots & z_M \\ \vdots & \ddots & \vdots \\ z_1^M & \cdots & z_M^M \end{vmatrix} = z_1^{p+1}\cdots z_M^{p+1}\prod_{1\le j<k\le M}(z_j - z_k) \neq 0.$$

Here, we directly use the result of the Vandermonde determinant. Thus, $\hat{f} \circ \phi$ does not have M consecutive zeros. By assumption, $\phi(0) = \mathbf{1}_G \in \operatorname{supp}(\hat{f})$. Since $|\operatorname{supp}(\hat{f})| = N/M$, we have

$$\operatorname{supp}(\hat{f}) = \{\phi(0), \phi(M), \phi(2M), \ldots, \phi(N-M)\}.$$

This is a subgroup of $\hat{G}$. Similarily, $\operatorname{supp}(f)$ is a subgroup of G. ■

However, some refinement of this result is also possible for a special class of abelian groups. If we consider $|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})|$ instead of $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})|$, this uncertainty principle can only give the lower bound $2\sqrt{|G|}$. It is already best for the general finite abelian group, but we can achieve a stronger result in the case that G is a cyclic group of prime order.

1.2 Refined Uncertainty Principle for Cyclic Group of Prime Order

Now consider the case where $G = \mathbb{Z}/p\mathbb{Z}$ is a cyclic group of prime order. In this case, G has no subgroups other than the trivial ones $\{0\}$ and G, so we expect to improve the result upon (1). Indeed, we can obtain a sharp additive uncertainty principle concerning $\operatorname{supp}(f)$ and $\operatorname{supp}(\hat{f})$. In this section, a proof of the following theorem by Terence Tao is given.

Theorem 4 (Tao) *Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is not always zero, then*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \ge p + 1.$$

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \ge p + 1$, there exists a function function f such that $\operatorname{supp}(f) = A, \operatorname{supp}(\hat{f}) = B$. (Note that there exists an isomorphism $\mathbb{Z}/p\mathbb{Z} \to \widehat{\mathbb{Z}/p\mathbb{Z}}$.)

An intuitive interpretation is that the function $f : \mathbb{Z}/p\mathbb{Z} \mapsto \mathbb{C}$ has exactly p degrees of freedom, whether considered with delta functions as a basis or with character functions as a basis. Requiring that $\operatorname{supp}(f) = A$ removes $p - |A|$ of these degrees, and requiring that $\operatorname{supp}(\hat{f}) = B$ takes away another $p - |B|$. This uncertainty principle thus asserts that the Dirac deltas basis and Fourier basis are "totally full rank," so that $p-|A|+p-|B| \le p - 1$.

More concretely and precisely, if we write the discrete inverse Fourier transform in matrix form:

$$\begin{pmatrix} f(0) \\ \vdots \\ f(p-1) \end{pmatrix} = \begin{pmatrix} e^{2\pi i \cdot 0 \cdot 0/p} & \cdots & e^{2\pi i \cdot 0 \cdot (p-1)/p} \\ \vdots & \ddots & \vdots \\ e^{2\pi i \cdot (p-1) \cdot 0/p} & \cdots & e^{2\pi i \cdot (p-1) \cdot (p-1)/p} \end{pmatrix} \begin{pmatrix} \hat{f}(0) \\ \vdots \\ \hat{f}(p-1) \end{pmatrix} = (e^{2\pi ijk/p})_{0 \le j,k < p} \begin{pmatrix} \hat{f}(0) \\ \vdots \\ \hat{f}(p-1) \end{pmatrix},$$

then we aim to prove that all the minors of the transformation matrix $(e^{2\pi ijk/p})_{0 \le j,k<p}$ are non-zero, a result known as Chebotarëv's lemma.

Lemma 5 (Chebotarëv) *Let q be a prime number, and select $1 \le k < p$ be an integer. Suppose $\omega_1, \ldots, \omega_k$ are distinct q-th roots of unity, and let $n_1, \ldots, n_k$ be distinct integers modulo p. Then the determinant of the $k \times k$ submatrix of $(e^{2\pi ijk/p})_{0 \le j,k<p}$ formed by the entries $(\omega_i^{n_j})_{1 \le k < p}$ is non-zero.*

Tao used a lemma about cyclotomic polynomials to prove Lemma 5.

Lemma 6 *Let p be a prime, n be a positive integer, and let $P(z_1, \ldots, z_n)$ be a polynomial with integer coefficients. If $\omega_1, \ldots, \omega_n$ are p-th roots of unity (not necessarily distinct) such that $P(\omega_1, \ldots, \omega_n) = 0$, then $P(1, \ldots, 1)$ is a multiple of p.*

Proof. Let $\omega = e^{2\pi i/p}$. Then for each $1 \le j \le n$, we can write $\omega_j = \omega^{k_j}$ for some integers $0 \le k_j < p$. Define the single-variable polynomial $Q(z) \in \mathbb{Z}[z]$ by

$$Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \bmod z^p - 1,$$

to be the reminder when $P(z^{k_1}, \ldots, z^{k_n})$ is divided by $z^p - 1$. Thus, we have $Q(\omega) = 0$ and $Q(1) = P(1, \ldots, 1)$. Since p is prime and $Q(z)$ is a polynomial of degree at most $p-1$ with integer coefficients, it must be an integer multiple of the minimal polynomial of ω, which is $\Phi_p(z) = 1 + z + \cdots + z^{p-1}$. Therefore, $Q(1)$ is an integer multiple of $\Phi_p(1) = p$. ∎

Proof of Lemma 5. First, define $D(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$ by $D(z_1, \ldots, z_n) = \det(z_j^{\xi_k})_{1 \le j,k \le n}$. Certainly, $D(z_1, \ldots, z_n) = 0$ when $z_i = z_j$ for any $1 \le i < j \le n$¿ Therefore we can write

$$D(z_1, \ldots, z_n) = P(z_1, \ldots, z_n) \prod_{1 \le i < j \le n} (z_j - z_i).$$

Observe that

$$\left(\frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{n-1} \prod_{1 \le i < j \le n} (z_j - z_i) = (n-1)! \prod_{1 \le i < j < n} (z_j - z_i),$$

and thus

$$\left(\frac{\mathrm{d}}{\mathrm{d}z_2}\right) \cdots \left(\frac{\mathrm{d}}{\mathrm{d}z_{n-1}}\right)^{n-2} \left(\frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{n-1} \prod_{1 \le i < j \le n} (z_j - z_i) = (n-1)!(n-2)! \cdots 1.$$

Consider operator $\left(z \dfrac{\mathrm{d}}{\mathrm{d}z}\right)$, we can write

$$\left(z \frac{\mathrm{d}}{\mathrm{d}z}\right)^n = \sum_{k=1}^{n} S(n,k) z^k \left(\frac{\mathrm{d}}{\mathrm{d}z_n}\right)^k,$$

where $S(n,k)$ are the Stirling numbers of the second kind. They may be defined using the recurrence $S(n,k) = kS(n-1,k) + S(n-1,k-1)$, with the initial conditions $S(n,n) = S(n,1) = 1$. Then

$$\left(z_2 \frac{\mathrm{d}}{\mathrm{d}z_2}\right) \cdots \left(z_{n-1} \frac{\mathrm{d}}{\mathrm{d}z_{n-1}}\right)^{n-2} \left(z_n \frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{n-1} = \left(S(1,1) z_2 \frac{\mathrm{d}}{\mathrm{d}z_2}\right) \cdots \left(\sum_{k_{n-1}=1}^{n-2} S(n-2, k_{n-1}) z_{n-1}^{k_{n-1}} \left(\frac{\mathrm{d}}{\mathrm{d}z_{n-1}}\right)^{k_{n-1}}\right) \cdot \left(\sum_{k_n=1}^{n-1} S(n-1, k_n) z_n^{k_n} \left(\frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{k_n}\right).$$

When the above is applied to $D(z_1, \ldots, z_n)$ at the point $z_1 = \cdots = z_n = 1$, only the term in which all the differential operators are applied to $\prod_{1 \le i < j \le n} (z_j - z_i)$ is non-zero, as otherwise there are factors $(z_j - z_i)$ that are equal to 0. Therefore the applied result is equal to $P(1, \ldots, 1)(n-1)!(n-2)! \cdots 1$.

By the definition of $D(z_1, \ldots, z_n)$,

$$\begin{aligned}
&\left(z_2 \frac{\mathrm{d}}{\mathrm{d}z_2}\right) \cdots \left(z_{n-1} \frac{\mathrm{d}}{\mathrm{d}z_{n-1}}\right)^{n-2} \left(z_n \frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{n-1} D(z_1, \ldots, z_n) \\
&\quad = \left(z_2 \frac{\mathrm{d}}{\mathrm{d}z_2}\right) \cdots \left(z_{n-1} \frac{\mathrm{d}}{\mathrm{d}z_{n-1}}\right)^{n-2} \left(z_n \frac{\mathrm{d}}{\mathrm{d}z_n}\right)^{n-1} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} z_j^{\xi_{\sigma(j)}} \\
&\quad = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \xi_{\sigma(n)}^{n-1} \xi_{\sigma(n-1)}^{n-2} \cdots \xi_{\sigma(2)} \cdot 1 \cdot \prod_{j=1}^{n} z_j^{\xi_{\sigma(j)}}.
\end{aligned}$$

Evaluated result at the point $z_1 = \cdots = z_n = 1$ is equal to

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \xi_{\sigma(n)}^{n-1} \xi_{\sigma(n-1)}^{n-2} \cdots \xi_{\sigma(2)} \cdot 1 = \det \begin{pmatrix} 1 & \xi_1 & \cdots & \xi_1^{n-1} \\ 1 & \xi_2 & \cdots & \xi_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_n & \cdots & \xi_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (\xi_j - \xi_i).$$

Therefore $P(1, \ldots, 1)$ is not divisible by p. Thus by Lemma 6, $P(\omega_1, \ldots, \omega_n) \neq 0$. So $D(\omega_1, \ldots, \omega_n) \neq 0$. ■

Now we have proven Lemma 5. Then, we will formalize the concept of "degree of freedom."

Proposition 7 *Let p be prime and take $A \subseteq G$ and $\tilde{A} \subseteq \hat{G}$ with $|A| = |\tilde{A}|$, and define $\pi : L(G) \mapsto L(\tilde{A})$ by $\pi(\hat{f}) = \pi(\sum_{\chi \in \hat{G}} \hat{f}(\chi)\mathbf{1}_\chi) = \sum_{\chi \in \tilde{A}} \hat{f}(\chi)\mathbf{1}_\chi$. For $\mathcal{F} : L(G) \mapsto L(\hat{G})$ the Fourier transform and $\eta : L(A) \mapsto L(\tilde{A})$ the inclusion map, let $\mathcal{G} = \pi \circ \mathcal{F} \circ \eta$.*

$$\begin{array}{ccc} L(G) & \xrightarrow{\mathcal{F}} & L(\hat{G}) \\ {\scriptstyle\eta}\uparrow & & \downarrow{\scriptstyle\pi} \\ L(A) & \xrightarrow{\mathcal{G}} & L(\tilde{A}) \end{array}$$

The map $\mathcal{G} : L(A) \mapsto L(\tilde{A})$ defined above is an isomorphism.

Proof of Theorem 4. Suppose by contradiction that there are some non-trivial $f \in L(G)$ such that $|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \le p$. Let $A = \operatorname{supp}(f)$. Then $|\hat{G} - \operatorname{supp}(\hat{f})| \ge |A|$, so there is a subset $\tilde{A} \subseteq \hat{G} \backslash \operatorname{supp}(f)$ with $|\tilde{A}| = |A|$. But $\mathcal{G}(f) = 0$ yet $f|_A \neq 0$, contradicting that $\mathcal{G} : L(A) \mapsto L(\tilde{A})$ is an isomorphism.

Now we prove the converse. It will suffice to prove the claim when $|A| + |B| = p + 1$, since the claim for $|A| + |B| > p + 1$ then follows by applying the claim to subsets $A' \subset A$, $B' \subset B$ respectively for which $|A'| + |B'| = p + 1$, and then taking generic linear combinations as A', B' vary.

We can then choose an $\tilde{A}$ in $\mathbf{Z}/p\mathbf{Z}$ of cardinality $|\tilde{A}| = |A|$ such that $\tilde{A}$ intersects B in only one point, say $\tilde{A} \cap B = \{\xi\}$. But by **Proposition 7**, the map $\mathcal{G}$ is invertible, and in particular we can find a non-zero $f \in l^2(A)$ such that $\hat{f}$ vanishes on $\tilde{A} \setminus \{\xi\}$ and is non-zero on ξ. Such a function must then be non-zero on all of A and non-zero on all of B since this would violate the first part of the uncertainty principle proven in the previous paragraph. Thus $\operatorname{supp}(f) = A$ and $\operatorname{supp}(\hat{f}) = B$ as desired. ■

1.3 Uncertainty Principle for Non-Abelian Finite Group

For a general finite group, the one-dimensional multiplicative characters are not enough to cover all the information of the group. For example, if G is chosen to be the symmetric group $\mathfrak{S}_3$ (it is not an abelian group), we only have two different one-dimensional multiplicative characters:

$$\chi_0(\sigma) = 1, \chi_1(\sigma) = \operatorname{sgn}(\sigma).$$

The group formed by these two characters is just $\mathbb{Z}/2\mathbb{Z}$. This tells us that we cannot define an inverse Fourier transform since we can construct $f, g : \mathfrak{S}_3 \to \mathbb{C}, f \neq g$ with $\hat{f}(\chi_0) = \hat{g}(\chi_0), \hat{f}(\chi_1) = \hat{g}(\chi_1)$.

In order to fix this problem, a generalization of multiplicative characters is required.

Definition 8 (Representation) *A representation ρ of G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a finite dimension $\mathbb{C}$-vector space and $\mathrm{GL}(V)$ is the group of invertible linear operators on V. The dimension $\dim(V)$ is called the dimension of ρ, which is denoted by d_ρ.*

A basic example is the associative permutation representation. It is defined on the vector space generated by $\{e_g\}_{g\in G}$ with the group action $\rho(g)\left(\sum_{g\in G} a_g e_g\right) = \sum_{g\in G} a_g e_{gx}$.

Definition 9 *Two representations of a group G, $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$ are called equivalent if there exists an invertible linear operator $T : V \to W$ such that $T \circ \rho_g = \sigma_g \circ T$ for any $g \in G$.*

Fix a representation $\rho : G \to \mathrm{GL}(V)$. A subspace $W \subseteq V$ is called G-invariant if $\rho_g(W) \subseteq W$ for any $g \in G$. The restricted representation $\rho|_W$ is called a subrepresentation. One important result about the subrepresentation is Maschke's theorem.

Theorem 10 (Maschke) *Let $\rho : G \to \mathrm{GL}(V)$ be a representation and $W \subseteq V$ be a G-invariant subspace. There exists a complementary G-invariant subspace $W' \subseteq V$ ($V = W \oplus W'$).*

Proof. Choose a subspace $W'' \subseteq V$ (not necessarily G-invariant) such that $W \oplus W'' = V$. Consider the projector $P : V \to V$ onto W with kernel W''. Now we construct a new operator:

$$\overline{P} = \frac{1}{|G|}\sum_{g\in G} \rho(g) \circ P \circ \rho(g)^{-1}.$$

It is clear that $\rho(g) \circ \overline{P} = \overline{P} \circ \rho(g)$. Besides, $\overline{P}|_W = \mathrm{Id}, \mathrm{Im}(\overline{P}) = W$, which implies that $\overline{P}$ is a projector.

We claim that $W' = \mathrm{Ker}\,\overline{P}$ is a G-invariant subspace. Indeed, $\overline{P}(\rho(g)w) = \rho(g)\overline{P}(w) = 0$ for all $g \in G$, hence $\rho(g)(w) \in W'$. Since $\overline{P}$ is a projector, we have $V = W \oplus W'$. ■

Therefore, we need only consider irreducible representations. A representation is called irreducible if it contains no non-trivial G-invariant subspace. For the irreducible representation, we have the Schur lemma (the proof is quite simple and is ignored here).

Lemma 11 *Let $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$ be two representations. If $T : V \to W$ is a G-invariant operator ($\sigma(g) \circ T = T \circ \rho(g)$), then either $T = 0$ or T is an isomorphism.*

This Schur lemma tells us that the decomposition of a representation is unique up to isomorphism.

Now we define $\widehat{G}$ to be the set of all irreducible representations. This is a finite set. In fact, every irreducible representation is a subrepresentation of the associative permutation representation and $\sum_{\rho\in\widehat{G}} d_\rho^2 = |G|$. Besides, every irreducible representation is unitary ($(\rho(g)\rho(g)^\dagger = \mathrm{Id}$ for every $g \in G$). For simplicity, we do not give the proof of these results. Now we can define the Fourier transform on the non-abelian group.

Definition 12 *Let G be a group and $f : G \to \mathbb{C}$, we may define the Fourier transform $\hat{f}$ at an irreducible representation ρ as*

$$\hat{f}(\rho) = \frac{1}{|G|}\sum_{a\in G} f(a)\rho(a).$$

And the inverse Fourier transform can be deduced as

$$f(a) = \sum_{\rho\in\widehat{G}} d_\rho \,\mathrm{Tr}\left(\rho(a^{-1})\hat{f}(\rho)\right).$$

We also have the Plancherel identity:

$$\frac{1}{|G|}\sum_{a\in G} f(a)\overline{g(a)} = \sum_{\rho\in\widehat{G}} d_\rho \,\mathrm{Tr}\left(\hat{f}(\rho)\hat{g}(\rho)^\dagger\right). \tag{2}$$

The proof of the inverse Fourier transform and the Plancherel identity will not be given in this paper for the sake of simplicity.

Another problem is to replace the $\mathrm{supp}(\hat{f})$ since the value of $\hat{f}$ is actually a matrix. Note that $\sum_{\rho\in\widehat{G}} d_\rho^2 = |G|$, we may define the size of support to be $\sum_{\rho\in\widehat{G}} d_\rho^2 \cdot \mathbf{1}_{\hat{f}(\rho)\neq 0}$. However, this is not good enough. Suppose H is a subgroup of G and consider the $\delta_H(a) = \mathbf{1}_{a\in H}$. Note that

$$\widehat{\delta_H}(\rho)^2 = \frac{1}{|G|^2}\sum_{a\in H}\sum_{b\in H}\rho(ab) = \frac{|H|}{|G|^2}\sum_{a\in H}\rho(a) = \frac{|H|}{|G|}\widehat{\delta_H}(\rho).$$

The Plancherel formula tells us that

$$\frac{|H|}{|G|} = \sum_{\rho\in\widehat{G}} d_\rho \operatorname{Tr}\left(\widehat{\delta_H}\widehat{\delta_H}^\dagger\right) = \sum_{\rho\in\widehat{G}} d_\rho \operatorname{rank}\left(\widehat{\delta_H}\right)\cdot\frac{|H|^2}{|G|^2}.$$

Therefore,

$$|\operatorname{supp}\delta_H|\sum_{\rho\in\widehat{G}} d_\rho \operatorname{rank}\left(\widehat{\delta_H}\right) = |G|.$$

On the other hand, we have the following proposition from [1].

Proposition 13 *Let H be a subgroup of the finite group G. Then* $\operatorname{rank}\widehat{\delta_H}(\rho)$ *is either d_ρ or zero for every $\rho\in\widehat{G}$ if and only if H is a normal group.*

Proof. First, we assume that H is normal. And define $H^\perp = \{\rho\in\widehat{G} : H\subseteq\operatorname{Ker}(\rho)\}$. Now a directed calculation shows that $\widehat{\delta_H}(\rho) = \frac{|H|}{|G|}\operatorname{Id}_\rho$. Since H is normal, $\widehat{G/H}$ is just $H^\perp$.

$$\begin{aligned}\sum_{\rho\in H^\perp} d_\rho \operatorname{Tr}\left(\widehat{\delta_H}(\rho)\widehat{\delta_H}(\rho)^\dagger\right) &= \sum_{\rho\in\widehat{G/H}} d_\rho^2\cdot\left(\frac{|H|}{|G|}\right)^2\\ &= |G/H|\cdot\frac{|H|^2}{|G|^2}\\ &= \frac{|H|}{|G|}\\ &= \frac{1}{|G|}\sum_{a\in G}|\delta_H(a)|^2.\end{aligned}$$

Now, the Plancherel identity implies the fact that $H^\perp$ is the support of $\widehat{\delta_H}$ and $\operatorname{rank}\widehat{\delta_H}(\rho)$ for ρ is just d_ρ.

On the other side, suppose that the ranks of the Fourier transform of δ_H are either full or zero. Let $H^\perp$ be the set of all irreducible representations ρ for which $\operatorname{rank}(\widehat{\delta_H}(\rho)) = d_\rho$. We claim that H is just the intersection of $\operatorname{Ker}\rho$ for $\rho\in H^\perp$. If this is true, H is the intersection of normal subgroups. Therefore, H is normal. Given $h\in H$ and $\rho\in H^\perp$, we have $\rho(h)\widehat{\delta_H}(\rho) = \widehat{\delta_H}(\rho)$ since H is a subgroup. By the definition of $H^\perp$, $\widehat{\delta_H}(\rho)$ is invertible. Hence, $\rho(h) = \operatorname{Id}_\rho$. This implies $H\subseteq\bigcap_{\rho\in H^\perp}\operatorname{Ker}\rho$. For the other direction, the Fourier inversion formula suggests that for g in the intersection of kernels:

$$\delta_H(g) = \sum_{\rho\in\widehat{G}} d_\rho\operatorname{Tr}\left(\widehat{\delta_H}(\rho)\rho(g)\right) = \frac{|H|}{|G|}\sum_{\rho\in H^\perp} d_\rho\operatorname{Tr}\left(\rho(g)\right) = \frac{|H|}{|G|}\sum_{\rho\in H^\perp} d_\rho^2 = \delta_H(e) = 1,$$

where the e above is the identity element of G. And this completes our proof. ■

We calculate a simple example here. Choose the group $G = \mathfrak{S}_3$. We have already mentioned two one-dimensional representations. This group also has a two-dimensional irreducible representation ρ, which can be generated by

$$\rho((1,2)) = \begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix}, \rho((1,2,3)) = \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}.$$

The subgroup $C_3 = \{e,(1,2,3),(1,3,2)\}$ is a normal subgroup, and the Fourier transform of its characteristic function is

$$\widehat{\delta_{C_3}}(\chi_0) = \frac{1}{2}, \widehat{\delta_{C_3}}(\chi_1) = \frac{1}{2}, \widehat{\delta_{C_3}}(\rho) = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

The support is 2 and the equality holds. On the other side, if we consider the group $H = \{e,(1,2)\}$ (this is not a normal subgroup), the Fourier transform becomes

$$\widehat{\delta_H}(\chi_0) = \frac{1}{3}, \widehat{\delta_H}(\chi_1) = 0, \widehat{\delta_H}(\rho) = \begin{pmatrix}0 & \frac{1}{6}\\ 0 & \frac{1}{3}\end{pmatrix}.$$

The summation of d_ρ with $\widehat{\delta_H}$ non-zero is 5. However, $\sum_{\sigma\in\widehat{\mathfrak{S}_3}} d_\sigma\operatorname{rank}(\widehat{\delta_H}(\sigma))$ is 3 since $\operatorname{rank}(\delta_H(\rho)) = 1$.

So the support of $\hat{f}$ should be $\sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho))$. The following theorem from [5] is a generalization of the uncertainty theorem 2.

Theorem 14 *Let $f : G \to \mathbb{C}$ be a function on G with non-empty support. Then*

$$|\operatorname{supp}(f)| \cdot \sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)) \geq |G|.$$

Proof. By the inverse Fourier transform, we have

$$|f(a)| = \left| \sum_{\rho \in \widehat{G}} d_\rho \operatorname{Tr}\left(\rho(a^{-1})\hat{f}(\rho)\right) \right| \leq \sum_{\rho \in \widehat{G}} d_\rho \left| \operatorname{Tr}\left(\rho(a^{-1})\hat{f}(\rho)\right) \right|.$$

For an endomorphism T, define $\Lambda(T)$ to be the multiset of eigenvalues of T counting algebraic multiplicity. By the Cauchy-Schwarz inequality and the inequality $\sum_{\lambda \in \Lambda(T)} |\lambda|^2 \leq \operatorname{Tr}(TT^\dagger)$,

$$\begin{aligned}
|f(a)|^2 &\leq \left(\sum_{\rho \in \widehat{G}} \sum_{\lambda \in \Lambda(\rho(a^{-1})\hat{f}(\rho))} d_\rho \cdot |\lambda| \right)^2 \\
&\leq \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)) \right) \cdot \left(\sum_{\rho \in \widehat{G}} d_\rho \sum_{\lambda \in \Lambda(\rho(a^{-1})\hat{f}(\rho))} |\lambda|^2 \right) \\
&\leq \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)) \right) \cdot \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{Tr}\left(\hat{f}(\rho)\rho(a^{-1})\rho(a^{-1})^\dagger \hat{f}(\rho)^\dagger\right) \right).
\end{aligned}$$

Since these representations are unitary, we have

$$\|f\|_\infty^2 \leq \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)) \right) \cdot \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{Tr}\left(\hat{f}(\rho)\hat{f}(\rho)^\dagger\right) \right).$$

Now using the Plancherel identity 2,

$$\|f\|_\infty^2 \leq \left(\sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)) \right) \cdot \left(\frac{1}{|G|} \sum_{a \in G} |f(a)|^2 \right) \leq \|f\|_\infty^2 \cdot |\operatorname{supp}(f)| \sum_{\rho \in \widehat{G}} d_\rho \operatorname{rank}(\hat{f}(\rho)),$$

which completes the proof of this uncertainty principle. ∎

2 Continuous Uncertainty Principle

This section, we provide a textbook proof of the Heisenberg Uncertainty Principle, and establish an additive generalization.

Definition 15 *Let $f : \mathbb{R}^d \to \mathbb{C}$. We define the Fourier transform $\hat{f}$ of f by*

$$\hat{f}(\xi) = \int_{\mathbb{R}^d} e^{-2\pi i \xi \cdot x} f(x) \, \mathrm{d}x$$

and the inverse Fourier transform $\check{f}$ of f by

$$\check{f}(\xi) = \int_{\mathbb{R}^d} e^{2\pi i \xi \cdot x} f(x) \, \mathrm{d}x$$

whenever these integrals make sense.

Definition 16 *We define the Schwarz space to be*

$$\mathcal{S}(\mathbb{R}^d) = \{f \in C^\infty(\mathbb{R}^d) \mid x^\alpha \partial^\beta f \in L^\infty(\mathbb{R}^d) \ \forall \alpha, \beta\}$$

where $\alpha, \beta \in \mathbb{N}^d$ above are arbitrary multi-indices. We call a function $f \in \mathcal{S}(\mathbb{R}^d)$ a Schwarz function.

2.1 Heisenberg's Uncertainty Principle

The following result tells us that the masses of a function and its Fourier transform cannot simultaneously be concentrated around points.

Theorem 17 (Heisenberg's uncertainty principle) *Let $\psi \in \mathcal{S}(\mathbb{R})$. Then we have*

$$\|\psi\|_2^2 \leq 4\pi \|x\psi(x)\|_2 \|\xi\hat{\psi}(\xi)\|_2.$$

Proof. We do the computation as follows:

$$\begin{aligned}
\|\psi\|_2^2 &= \int_{\mathbb{R}} |\psi(x)|^2 \,\mathrm{d}x \\
\text{(integration by parts)} &= [x|\psi(x)|^2]_{x=-\infty}^{+\infty} - \int_{\mathbb{R}} x \,\mathrm{d}\psi(x)\overline{\psi(x)} \\
\text{(rapid decay of } \psi\text{, by definition)} &= -\int_{\mathbb{R}} 2x \,\mathrm{Re}[\overline{\psi(x)} \frac{\mathrm{d}\psi(x)}{\mathrm{d}x}] \,\mathrm{d}x
\end{aligned}$$

Taking the absolute value and use $\Re(x) \leq x$ along with $|\int f| \leq \int |f|$, denoting $\psi'(x) = \dfrac{\mathrm{d}\psi(x)}{\mathrm{d}x}$, we have

$$\begin{aligned}
\|\psi\|_2^2 &\leq \int_{\mathbb{R}} 2x \left|\overline{\psi(x)}\right| \left|\psi'(x)\right| \,\mathrm{d}x \\
\text{(Cauche-Schwarz)} &\leq 2\int_{\mathbb{R}} |x\psi(x)|^2 \,\mathrm{d}x \int_{\mathbb{R}} \left|\psi'(x)\right|^2 \,\mathrm{d}x \\
\text{(Plancherel's Identity)} &\leq 2\sqrt{\int_{\mathbb{R}} |x\psi(x)|^2 \,\mathrm{d}x \int_{\mathbb{R}} \left|\hat{\psi}'(\xi)\right|^2 \,\mathrm{d}\xi} \\
&\leq 2\sqrt{\int_{\mathbb{R}} |x\psi(x)|^2 \,\mathrm{d}x \int_{\mathbb{R}} \left|2\pi i\xi\hat{\psi}(\xi)\right|^2 \,\mathrm{d}\xi} \\
&= 4\pi\sqrt{\int_{\mathbb{R}} |x\psi(x)|^2 \,\mathrm{d}x \int_{\mathbb{R}} \left|\xi\hat{\psi}(\xi)\right|^2 \,\mathrm{d}\xi}.
\end{aligned}$$

To conclude,

$$\|\psi\|_2^2 \leq 4\pi \|x\psi(x)\|_2 \|\xi\hat{\psi}(\xi)\|_2.$$

■

If you are not interested in how physicists view and prove the uncertainty principle, just skip **Section 2.2**.

2.2 Uncertainty, via Operator

A physicist might view the uncertainty principle 17 as a result of

$$\|\psi\|_2^2 \leq 4\pi \|X\psi\|_2 \|D\psi\|_2$$

where X and D above are self-adjoint linear operators on $L^2(\mathbb{R})$ over inner product $\langle f, g\rangle = \displaystyle\int_{\mathbb{R}} f(x)\overline{g(x)} \,\mathrm{d}x$ defined by

$$(X\psi)(x) = x\psi(x), \quad (D\psi)(x) = \frac{1}{2\pi i} \left.\frac{\mathrm{d}\psi}{\mathrm{d}x}\right|_x.$$

For the commutator of D and X:

$$([D, X]\psi)(x) = \frac{x}{2\pi i}\psi'(x) + \frac{1}{2\pi i}\psi(x) - \frac{x}{2\pi i}\psi'(x) = \frac{1}{2\pi i}\psi(x)$$

so, by substitution, we obtain

$$\|\psi\|_2^2 = \langle\psi, \psi\rangle = 2\pi i\langle[D, X]\psi, \psi\rangle = 2\pi i(\langle X\psi, D\psi\rangle - \langle D\psi, X\psi\rangle) = 4\pi \,\mathrm{Im}(\langle X\psi, D\psi\rangle) \leq 4\pi\|X\psi\|_2\|D\psi\|_2$$

as desired.

In fact, the uncertainty of two operators A, B is strongly related to their commutator $[A, B] = AB - BA$.

Let A and B be self-adjoint operators on a complex Hilbert space $\mathcal{H}$, and let ψ be a normalized state, $\langle\psi,\psi\rangle = 1$. We define the expectation values

$$\langle A\rangle = \langle\psi, A\psi\rangle, \quad \langle B\rangle = \langle\psi, B\psi\rangle,$$

and the deviation operators

$$\Delta A = A - \langle A\rangle, \quad \Delta B = B - \langle B\rangle.$$

The variances are defined as

$$\langle(\Delta A)^2\rangle = \langle\Delta A\psi, \Delta A\psi\rangle, \quad \langle(\Delta B)^2\rangle = \langle\Delta B\psi, \Delta B\psi\rangle.$$

Now consider the inner product

$$\langle\phi_A, \phi_B\rangle = \langle\Delta A\psi, \Delta B\psi\rangle,$$

where $\phi_A = \Delta A\psi$ and $\phi_B = \Delta B\psi$.

By the Cauchy–Schwarz inequality,

$$|\langle\phi_A, \phi_B\rangle|^2 \le \langle\phi_A, \phi_A\rangle\,\langle\phi_B, \phi_B\rangle = \langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle.$$

Write $\langle\phi_A, \phi_B\rangle$ in terms of commutator and anti-commutator:

$$\langle\phi_A, \phi_B\rangle = \langle\psi, \Delta A\Delta B\psi\rangle = \frac{1}{2}\langle\{\Delta A, \Delta B\}\rangle + \frac{1}{2}\langle[\Delta A, \Delta B]\rangle,$$

where the anti-commutator $\{A, B\} = AB+BA$, the commutator $[A, B] = AB-BA$, and from conjugacy symmetry of inner product,

$$\langle[\Delta A, \Delta B]\rangle = \langle\psi, (\Delta A\Delta B - \Delta B\Delta A)\psi\rangle = \langle\Delta A\psi, \Delta B\psi\rangle - \langle\Delta B\psi, \Delta A\psi\rangle$$

is a pure imaginary number.

Finally, we take the imaginary part

$$\mathrm{Im}\langle\phi_A|\phi_B\rangle = \frac{1}{2i}\langle[A, B]\rangle.$$

and

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle \ge \big(\mathrm{Im}\langle\phi_A|\phi_B\rangle\big)^2 = \frac{1}{4}\big|\langle[A, B]\rangle\big|^2.$$

In conclusion, if the commutator $[A, B]$ is nonzero, then the product of uncertainties cannot vanish. For position operator $\hat{x} = x$ and momentum operator $\hat{p} = -i\hbar\frac{\mathrm{d}}{\mathrm{d}x}$ (both in the position representation) which satisfies $[\hat{x}, \hat{p}] = i\hbar$, the above inequality gives

$$\Delta x\,\Delta p \ge \frac{\hbar}{2}$$

which is widely known from senior high school.

2.3 Amrein-Berthier Theorem

We will now consider the question of simultaneous localization on sets and show that, for appropriate notions of "smallness," if a function vanishes outside a small set then its Fourier transform cannot. If we take "small" to mean "compact," then this result falls out of our consideration of the complex Fourier transform.

Lemma 18 (Paley-Wiener, single direction) *Let $f \in L^2(\mathbb{R})$ with $\mathrm{supp}(f) \subseteq B_R$ for some $R > 0$, where $B_R = [-R, R]$. Define the function $F : \mathbb{C} \to \mathbb{C}$ by*

$$F(z) = \int_{B_R} e^{-2\pi i z\cdot x} f(x)\,\mathrm{d}x, \quad z \in \mathbb{C}.$$

Then the following hold:

1. *F is an entire function on $\mathbb{C}$.*
2. *F is an analytic continuation of $\hat{f}$, i.e., for all $\xi \in \mathbb{R}$, we have*

$$F(\xi) = \hat{f}(\xi).$$

3. *There exists a constant $C > 0$ such that for all $z \in \mathbb{C}$,*

$$|F(z)| \le Ce^{2\pi R|\,\mathrm{Im}(z)|}.$$

Proof. Since B_R has finite measure and $f \in L^2(\mathbb{R})$, we have $f \in L^1(\mathbb{R})$ by Hölder.

Let $T \subseteq \mathbb{C}$ be any triangle. By Fubini's theorem:

$$\oint_T F(z)\,dz = \int_{B_R} f(x) \left[\oint_T e^{-2\pi i z x}\,\mathrm{d}z \right] \mathrm{d}x.$$

For each fixed x, the function $z \mapsto e^{-2\pi i z x}$ is entire, so by Cauchy's theorem:

$$\oint_T e^{-2\pi i z x}\,\mathrm{d}z = 0.$$

Hence $\oint_T F(z)\,\mathrm{d}z = 0$.

For any compact set $K \subseteq \mathbb{C}$, there exists $M > 0$ such that $|\operatorname{Im} z| \le M$ for all $z \in K$. Then

$$|f(x)e^{-2\pi i z x}| \le |f(x)|e^{2\pi R M}.$$

Since $f \in L^1(B_R)$, by the uniform continuity of $g(x) = e^{-2\pi i z x}$, if we fix z_0, for all $\varepsilon > 0$ there exists δ, for all $|z - z_0| < \delta$,

$$\begin{aligned} |F(z) - F(z_0)| &= \left| \int_{B_R} (e^{-2\pi i z \cdot x} - e^{-2\pi i z_0 \cdot x}) f(x)\,\mathrm{d}x \right| \\ &\le \varepsilon \|f(x)\|_{L^1(B_R)}, \end{aligned}$$

thus $F(z)$ is continuous. By Morera's theorem, F is entire.

For $z = \xi \in \mathbb{R}$, the definition of $F(\xi)$ coincides with the Fourier transform $\hat{f}(\xi)$ since $\operatorname{supp}(f) \subseteq B_R$.

Using the support condition and Cauchy-Schwarz inequality:

$$\begin{aligned} |F(z)| &\le \int_{B_R} |f(x)| e^{2\pi |\eta \cdot x|}\,\mathrm{d}x \\ &\le \int_{B_R} |f(x)| e^{2\pi R |\eta|}\,\mathrm{d}x \\ &\le e^{2\pi R|\eta|} \|f\|_{L^1(B_R)} \\ &\le C e^{2\pi R |\operatorname{Im}(z)|}, \end{aligned}$$

where $C = \|f\|_{L^1(B_R)} < \infty$. ∎

Corollary 19 *If $f \in L^2(\mathbb{R})$ is compactly supported and $\hat{f}$ is compactly supported, then $f = 0$.*

Proof. If $\hat{f}$ is compactly supported, then, by **Lemma 18**, f is the restriction to $\mathbb{R}$ of an analytic function. If f is compactly supported, then its zeroes are clearly not isolated, so the analyticity of f implies $f = 0$. ∎

We now consider the case when "small" is taken to mean "of finite measure." Every real compact set has finite measure, of course, but sets of finite measure need not be bounded.

Theorem 20 (Amrein-Berthier) *Let $f \in L^2(\mathbb{R}^d)$, $E, F \subseteq \mathbb{R}$ have finite measure. Then*

$$\|f\|_{L^2(\mathbb{R}^d)} \le C(\|f\|_{L^2(E^c)} + \|\hat{f}\|_{L^2(F^c)})$$

where C depends only on E, F, d. In particular, if both f and $\hat{f}$ are supported on sets of finite measure, then $f = 0$.

Before we prove this result, we require a lemma.

Lemma 21 *Let $E \subseteq \mathbb{R}^d$, $F \subseteq \mathbb{R}^d$ have finite measure. If there exists a constant C' such that $\operatorname{supp}(\hat{f}) \subseteq F \implies \|f\|_2 \le C'\|f\|_{L^2(E^c)}$, then there exists a constant C such that, for all $f \in L^2(\mathbb{R}^d)$, $\|f\|_2 \le C(\|f\|_{L^2(E^c)} + \|\hat{f}\|_{L^2(F^c)})$.*

Proof. Define $P_F(f) = \widehat{\mathbf{1}_F \hat{f}}$.

$$\begin{aligned} \|f\|_2 &= \|P_F f + P_{F^c} f\|_2 \\ &\le \|P_f f\|_2 + \|P_{F^c} f\|_2 \\ (\operatorname{supp}(\mathbf{1}_F \hat{f}) \subseteq F \text{ and Plancherel}) &\le C' \|P_F f\|_{L^2(E^c)} + \|\mathbf{1}_{F^c} f\|_2 \\ &\le C' \|f\|_{L^2(E^c)} + \|f\|_{L^2(F^c)} \end{aligned}$$

Using $C = \max\{1, C'\}$ finishes the proof. ■

Proof of Theorem 20. Fix E, F as above. We consider the operator T given by

$$Tf = \mathbf{1}_E(\widetilde{\mathbf{1}_F \hat{f}}).$$

If the L^2 operator norm of T is less than 1, then the hypothesis of **Lemma 21** holds with $C' = \frac{1}{1-\|T\|}$, due to a simple calculation when $\mathrm{supp}(\hat{f}) \subseteq F$:

$$\|f - Tf\|_2 = \|f - \mathbf{1}_E(\check{\hat{f}})\|_2 = \|\mathbf{1}_{E^c} f\|_2 = \|f\|_{L^2(E^c)} \geq \|f\|_2 - \|Tf\|_2 \geq (1 - \|T\|)\|f\|_2.$$

Thus, it suffices to show that $\|T\| < 1$.

Observe that T is a Hilbert-Schmidt integral operator

$$(Tf)(x) = \mathbf{1}_E(x)(\check{\mathbf{1}_F} * f)(x) = \mathbf{1}_E(x) \int_{\mathbb{R}^d} \check{\mathbf{1}_F}(x-y) f(y)\, \mathrm{d}y$$

with kernel

$$K(x,y) = \mathbf{1}_E(x)\check{\mathbf{1}}_F(x-y)$$

and Hilbert-Schmidt norm σ given by

$$\sigma^2 = \|K\|^2_{L^2(\mathbb{R}^{2d})} = \int_{\mathbb{R}^{2d}} \mathbf{1}^2_E(x)\check{\mathbf{1}}^2_F(x-y)\, \mathrm{d}x\, \mathrm{d}y = |E||F|,$$

where we use Plancherel for $\|\mathbf{1}_F\|_2 = \|\check{\mathbf{1}_F}\|_2 = |F|$. It follows that T is a compact operator.

Note that, by compactness, the L^2 operator norm of T is 1 if and only if there exists a function $f \in L^2(\mathbb{R}^d)$ such that f is supported on E and $\hat{f}$ is supported on F. Therefore, the quantitative bound of **Lemma 21** is in fact equivalent to the claim that a non-zero function and its Fourier transform cannot both be supported on sets of finite measure.

We now show that the norm of T is less than 1. Since T is the product of projections, we know it has L^2 operator norm less than or equal to 1. Suppose by way of contradiction that $\|T\| = 1$, i.e. that there exists a $f \in L^2(\mathbb{R})$ with $\mathrm{supp}(f) \subseteq E$ and $\mathrm{supp}(\hat{f}) \subseteq F$. By repeatedly translating f by sufficiently small and vanishing amounts (say, 2^{-k}), we obtain an infinite collection of linearly independent functions compactly supported in some set E' of finite measure and whose Fourier transforms are all supported in F. It follows that these functions are eigenfunctions of the operator T' obtained by substituting E' for E in the definition of T with eigenvalue 1. But since T' is a compact operator, like T, its eigenspaces with non-zero eigenvalue are all finite-dimensional, so we have obtained a contradiction. ■

3 Further Generalizations of Uncertainty Principle

3.1 Sparse Discrete Uncertainty Principles

One could analogously argue that, in some sense, Theorem 4 is "barely true" when $|G|$ is prime. As a fact, the Gaussian function in $L^2(\mathbb{R})$ with a proper width is fixed by the Fourier transform. Let's now look at its discretized version, which is constructed by first periodizing the function $f(t) = e^{-n\pi t^2}$ over the real line to have a unit period, and then sampling this periodized function at multiples of $1/n$. Given the rapidly decaying nature of the Gaussian function over $\mathbb{R}$, it's no surprise that many of its entries are nearly zero. For example, we take $n = 211$ (which is prime). Assuming the discretized function takes values in the range $\{0, \frac{1}{211}, \ldots, \frac{210}{211}\}$, its value at $t = \frac{60}{211}$ is $e^{-1800\pi/211}$, approximately 2.77×10^{-46}, which is already smaller than the computational limitation of single-precision floating-point format, which is $2^{-149} \approx 1.40 \times 10^{-45}$. And so from a numerical perspective, this function appears to contradict Theorem 4: $61 + 61 = 122 < 212 = 211 + 1$.

To help resolve this discrepancy, we consider a numerical version of sparsity rather than 0-norm, which is named **numerical sparsity**:

$$\mathrm{ns}(x) := \frac{\|x\|_1^2}{\|x\|_2^2}, \quad \forall x \in \mathbb{C}^n \backslash \{0\}.$$

We note that numerical sparsity is invariant under non-zero scaling. In addition, 0-norm bounds the other: $\mathrm{ns}(x) \leq \|x\|_0$. To see this, apply Cauchy-Schwarz to get

$$\|x\|_1 = \left\langle |x|, \mathbf{1}_{\mathrm{supp}(x)} \right\rangle \leq \|x\|_2 \|\mathbf{1}_{\mathrm{supp}(x)}\|_2 = \|x\|_2 \sqrt{\|x\|_0}.$$

Theorem 22 *Let U be an $n \times n$ unitary matrix. Then*

$$\mathrm{ns}(x)\,\mathrm{ns}(Ux) \geq \frac{1}{\|U\|_{1\to\infty}^2}, \quad \forall x \in \mathbb{C}^n \backslash \{0\},$$

where $\|A\|_{1\to\infty}$ denotes the induced matrix norm: $\|A\|_{1\to\infty} = \max_x \dfrac{\|Ux\|_1}{\|x\|_\infty}$.

Proof. The proof is rather straightforward: Apply Hölder's inequality to get

$$\mathrm{ns}(x)\,\mathrm{ns}(Ux) = \frac{\|x\|_1^2}{\|x\|_2^2} \cdot \frac{\|Ux\|_1^2}{\|Ux\|_2^2} \geq \frac{\|x\|_1^2}{\|x\|_2^2} \cdot \frac{\|Ux\|_2^2}{\|Ux\|_\infty^2} = \frac{\|x\|_1^2}{\|Ux\|_\infty^2} \geq \frac{1}{\|U\|_{1\to\infty}^2}. \tag{3}$$

■

We further study functions which achieve either exact or near equality in our multiplicative uncertainty principle in the case where the unitary matrix U is the discrete Fourier transform, in which case $\|U\|_{1\to\infty} = 1/\sqrt{n}$.

Theorem 23 *Suppose $f \in L(\mathbb{Z}_n)$. Then $\mathrm{ns}(f)\,\mathrm{ns}(\mathcal{F}f) = n$ if and only if $\|f\|_0\|\mathcal{F}f\|_0 = n$.*

Proof. ($\Leftarrow$) This follows directly from the inequality $\mathrm{ns}(f) \leq \|f\|_0$, along with Theorem 2 and 22.

($\Rightarrow$) It suffices to show that $\mathrm{ns}(f) = \|f\|_0$ and $\mathrm{ns}(\mathcal{F}f) = \|\mathcal{F}f\|_0$. Note that both $\mathcal{F}$ and $\mathcal{F}^{-1}$ are unitary operators and $\|\mathcal{F}\|_{1\to\infty}^2 = \|\mathcal{F}^{-1}\|_{1\to\infty}^2 = 1/n$. By assumption, taking $\hat{f} = \mathcal{F}f$, then gives

$$\mathrm{ns}(\mathcal{F}^{-1}\hat{f})\,\mathrm{ns}(\hat{f}) = \mathrm{ns}(f)\,\mathrm{ns}(\mathcal{F}f) = n.$$

We will use the fact that f and $\hat{f}$ each achieve equality in the Theorem 22 with $U = F$ and $U = F^{-1}$, respectively. Notice from the proof (3) that equality occurs only if f and $\hat{f}$ satisfy equality in Hólder's inequality, that is,

$$\|f\|_1\|f\|_\infty = \|f\|_2^2, \quad \|\hat{f}\|\|\hat{f}\|_\infty = \|\hat{f}\|_2^2. \tag{4}$$

To achieve the first equality in (4),

$$\sum_{j\in\mathbb{Z}_n} |f(j)|^2 = \|f\|_2^2 = \|f\|_1\|f\|_\infty = \sum_{j\in\mathbb{Z}_n} |f(j)| \max_{k\in\mathbb{Z}_n} |f(k)|.$$

This implies that $|f(j)| = \max_{k\in\mathbb{Z}_n} |f(k)|$ for every j with $f(j) \neq 0$. As such, $|f| = a\mathbf{1}_A$ and $\hat{f} = b\mathbf{1}_B$ for some $a, b > 0$ and $A, B \subseteq \mathbb{Z}_n$. Then

$$\mathrm{ns}(f) = \frac{\|f\|_1^2}{\|f\|_2^2} = \frac{(a|A|)^2}{a^2|A|} = |A| = \|f\|_0,$$

and similarly, $\mathrm{ns}(\hat{f}) = \|\hat{f}\|_0$. ■

Having established that equality in the new multiplicative uncertainty principle (Theorem 22) is equivalent to equality in the principle (Theorem 2), we wish to separate these principles by focusing on near equality. We expect the new principle to accommodate nearly sparse vectors, and so we appeal to the discrete Gaussian depicted above:

Theorem 24 *Define $f \in L(\mathbb{Z}_n)$ by*

$$f(j) := \sum_{j'\in\mathbb{Z}} e^{-n\pi(\frac{j}{n}+j')^2}, \quad \forall j \in \mathbb{Z}_n. \tag{5}$$

Then $\mathcal{F}f = f$ and $\mathrm{ns}(f)\,\mathrm{ns}(\mathcal{F}f) \leq (2 + o(1))n$.

In words, the discrete Gaussian achieves near equality in the multiplicative uncertainty principle. We need a sampling lemma for Schwarz function.

Lemma 25 *Suppose $f \in C^\infty(\mathbb{R})$ is Schwarz and construct a discrete function $g \in L(\mathbb{Z}_n)$ by periodizing and sampling f as follows:*

$$g(j) = \sum_{j'\in\mathbb{Z}} f(\frac{j}{n} + j'), \quad \forall j \in \mathbb{Z}_n. \tag{6}$$

Then the discrete Fourier transform of g is determined by $\hat{f}(\xi) = \displaystyle\int_{\mathbb{R}} f(t)e^{-2\pi i\xi t}\,\mathrm{d}t$:

$$(\mathcal{F}g)(k) = \sqrt{n} \sum_{k'\in\mathbb{Z}} \hat{f}(k + k'n), \quad \forall k \in \mathbb{Z}_n.$$

Proof. Since f is Schwarz, we could apply the Poisson summation formula:

$$g(j) = \sum_{j' \in \mathbb{Z}} f(\frac{j}{n} + j') = \sum_{l \in \mathbb{Z}} \hat{f}(l) e^{2\pi i j l / n}.$$

Next,

$$\begin{aligned}(\mathcal{F}g)(k) &= \frac{1}{\sqrt{n}} \sum_{j \in \mathbb{Z}_n} \left(\sum_{l \in \mathbb{Z}} \hat{f}(l) e^{2\pi i j l / n} \right) e^{-2\pi i j k / n} \\ &= \frac{1}{\sqrt{n}} \sum_{l \in \mathbb{Z}} \hat{f}(l) \sum_{j \in \mathbb{Z}_n} \left(e^{2\pi i (l-k)/n} \right)^j = \sqrt{n} \sum_{\substack{l \in \mathbb{Z} \\ l \equiv k \bmod n}} \hat{f}(l).\end{aligned}$$

The result then follows from a change of variables. ■

Proof of Theorem 24. It is easy to verify that the Gaussian function $G(t) = e^{-n\pi t^2}$ is Schwarz. Note that defining f according to (6) then produces (5). Considering $\hat{G} = n^{-1/2} e^{-\pi \xi^2 / n}$, we use Lemma 25 to verify that $\mathcal{F}f = f$. To prove Theorem 24, it then suffices to show that $\mathrm{ns}(f) \leq (\sqrt{2} + o(1))\sqrt{n}$. We accomplish this by bounding $\|f\|_2$ and $\|f\|_1$ separately.

To bound $\|f\|_2$, we first expand a square to get

$$\|f\|_2^2 = \sum_{j \in \mathbb{Z}_n} \left(\sum_{j' \in \mathbb{Z}} e^{-n\pi (\frac{j}{n} + j')^2} \right)^2 = \sum_{j \in \mathbb{Z}_n} \sum_{j' \in \mathbb{Z}} \sum_{j'' \in \mathbb{Z}} e^{-n\pi [(\frac{j}{n} + j')^2 + (\frac{j}{n} + j'')^2]}.$$

Since all of the term in the sum are non-negative, we infer a lower bound by discarding the terms for which $j' \neq j''$. This yields that

$$\|f\|_2^2 \geq \sum_{j \in \mathbb{Z}_n} \sum_{j' \in \mathbb{Z}} e^{-2n\pi (\frac{j}{n} + j')^2} = \sum_{k \in \mathbb{Z}} e^{-2\pi k^2 / n} \geq \int_{\mathbb{R}} e^{-2\pi x^2 / n} \, \mathrm{d}x - 1 = \sqrt{\frac{n}{2}} - 1.$$

Next, we bound $\|f\|_1$ using a similar integral comparison:

$$\|f\|_1 = \sum_{j \in \mathbb{Z}_n} \sum_{j' \in \mathbb{Z}} e^{-n\pi (\frac{j}{n} + j')^2} = \sum_{k \in \mathbb{Z}} e^{-\pi k^2 / n} \leq \int_{\mathbb{R}} e^{-\pi x^2 / n} \, \mathrm{d}x + 1 = \sqrt{n} + 1.$$

Overall, we have

$$\mathrm{ns}(f) = \frac{\|f\|_1^2}{\|f\|_2^2} \leq \frac{(\sqrt{n}+1)^2}{\sqrt{n/2} - 1} = (\sqrt{2} + o(1))\sqrt{n}.$$

■

In fact, under this measure of numerical sparsity, an additive uncertainty principle also exists [2]. However, its proof is not as straightforward, so we will omit it here and simply present its results.

Theorem 26 *There exists a universal constant $c > 0$ such that if U is drawn uniformly from the unitary group $U(n \times n)$, then with probability $1 - e^{-\Omega(n)}$,*

$$\mathrm{ns}(x) + \mathrm{ns}(Ux) \geq (c - o(1))n, \quad \forall x \in \mathbb{C}^n \backslash \{0\}. \tag{7}$$

As shown in Theorem 24, the discrete Gaussian function has numerical sparsity $O(\sqrt{n})$, thereby violating (7). Interestingly, this additive uncertainty principle establishes that the Fourier transform is rare, as in the worst case, most unitary matrices introduce significantly greater uncertainty.

3.2 Uncertainty on Finite Fields

In finite settings, the Fourier series of a function $f : G \mapsto \mathbb{C}$ is presented as a linear combination of characters:

$$\begin{aligned}\widehat{f}(\chi) &= \frac{1}{|G|} \sum_{x \in G} f(x) \overline{\chi(x)}, \\ f(x) &= \sum_{\chi \in \widehat{G}} \hat{f}(\chi) \chi(x).\end{aligned}$$

Here $\chi : G \mapsto \mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ is a character. If G is Abelian, each character takes values in a finite subgroup of $\mathbb{S}^1$, i.e. in some set of roots of unity.

Analogously, we observe that there is cyclic structures in complex fields $\mathbb{C}$, and the multiplicative group of a finite field $\mathbb{F}_{q^r}^\times = \langle g \rangle$ is also cyclic. In this section, we consider functions $f : \mathbb{Z}_p \mapsto \mathbb{F}_{q^r}$ with prime p, q and some $r \in \mathbb{Z}^+$, and define a new transformation (similar to NTT). Let g be a generator of $\mathbb{F}_{q^r}^\times$, which has an order of $q^r - 1$.

First, we consider what the "characters" from $\mathbb{Z}_p$ to $\mathbb{F}_{q^r}^\times$ are like. It depends on $\chi(1)$, and $\chi(1)^p = \chi(0) = 1 = g^{k(q^r-1)}$. If we assume $p \mid q^r - 1$ and $sp = q^r - 1$, then $\chi(1) = g^{ks}$. To make sure all the χ's only appear once, we require $k \in \mathbb{Z}_p$. In conclusion, every character is of the form $\chi_k(x) = g^{ksx}$ for some $k \in \mathbb{Z}_p$.

Definition 27 *Let $f : \mathbb{Z}_p \mapsto \mathbb{F}_{q^r}$ where $sp = q^r - 1$ for $s, p \in \mathbb{Z} \cap [0, q^r)$ with p, q odd prime numbers. Define the* ***Number Theoretic Transform*** *$\hat{f} : \widehat{\mathbb{Z}}_p \mapsto \mathbb{F}_{q^r}$ as*

$$\widehat{f}(\chi) = p^{-1} \sum_{x \in \mathbb{Z}_p} f(x)\chi(x)^{-1}.$$

and the inverse transform by

$$f(x) = \sum_{\chi \in \widehat{\mathbb{Z}}_p} \hat{f}(\chi)\chi(x).$$

where p^{-1} denotes the inverse of p in the field $\mathbb{F}_{q^r}$.

Writing functions in vectors, and χ_k's as k's, we have a matrix interpretation for inverse transform

$$\begin{pmatrix} f(0) \\ \vdots \\ f(p-1) \end{pmatrix} = \begin{pmatrix} g^{0\cdot s\cdot 0} & \cdots & g^{0\cdot s\cdot (p-1)} \\ \vdots & \ddots & \vdots \\ g^{(p-1)\cdot s\cdot 0} & \cdots & g^{(p-1)\cdot s\cdot (p-1)} \end{pmatrix} \begin{pmatrix} \hat{f}(0) \\ \vdots \\ \hat{f}(p-1) \end{pmatrix},$$

where all entries of the matrix are in $\mathbb{F}_{q^r}^\times$.

Now using the **Theorem A** in [7], we know that if q is large enough, every minor of this matrix in **Definition 27** is non-zero. (**Corollary 17** in [3] is an attempt to generalize it, but the paper was pointed out a flaw and has been revised by Sep. 2025). We present the theorem as follows:

Theorem 28 (Theorem A in [7])) *Let p, q be distinct odd primes such that $\mathrm{ord}_p(q) = p - 1$ and $q > \Gamma$, where*

$$\Gamma = \max\{\gamma_n \mid 2 \le n \le p-1\}$$

and

$$\gamma_n = \max\left\{ \frac{V_s(a_1, a_2, \cdots, a_n)}{V_s(0, 1, \cdots, n-1)} \mid 0 \le a_1 < a_2 < \cdots < a_n \le p-1 \right\}$$

with $V_s(x_1, \ldots, x_n) = \prod_{i<j}(x_j - x_i)$.

Suppose that ω is a primitive p-th root of unity in $\mathbb{F}_{q^{p-1}}$. Then all square submatrices of the Vandermonde matrix

$$V_p = (\omega^{ij})_{i,j=0}^{p-1}$$

have nonzero determinant.

Through the same arguments to Tao's [6], we have

$$\mathrm{supp}(f) + \mathrm{supp}(\hat{f}) \ge p + 1.$$

And we have a formal theorem, using $r = p - 1$:

Theorem 29 (Uncertainty Principle over Finite Fields) *Let $f : \mathbb{Z}_p \to \mathbb{F}_{q^{p-1}}$ be a nonzero function, and let $\hat{f}$ denote its Number Theoretic Transform defined in* ***Definition 27****. Assume $p < q$ are two prime numbers, $p \mid (q^{p-1} - 1)$ (which is exactly $q^{p-1} \equiv 1 \mod p$ and $\mathrm{ord}_p(q) = p - 1$), and that q is sufficiently large so that every square submatrix of the NTT matrix is nonsingular (as ensured by* ***Theorem 28****). Then we have the following uncertainty relation:*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \ge p + 1.$$

Here, $\mathrm{supp}(f) = \{x \in \mathbb{Z}_p : f(x) \neq 0\}$ *and* $\mathrm{supp}(\hat{f}) = \{\chi \in \widehat{\mathbb{Z}_p} : \hat{f}(\chi) \neq 0\}$.

3.2.1 Zeros of Sparse Polynomials

An application arises in bounding the number of zeros of sparse polynomials over finite fields. Let

$$P(X) = \sum_{j \in A} a_j X^j \in \mathbb{F}_{q^{p-1}}[X],$$

where $A \subseteq \mathbb{Z}$, and $|A| = k$ is small (a k-sparse polynomial). Define $f(x) = P(g^{sx}) = \sum_{j \in A} a_j g^{xsj}$ on $x \in \mathbb{Z}_p$. With simple calculation we have for $j \in \mathbb{Z}_p$,

$$\hat{f}(j) = \sum_{i \in A,\ p | i-j} a_i.$$

Then $\hat{f}$ is supported on a set $B \subseteq A \subseteq \widehat{\mathbb{Z}_p}$ of size at most k, i.e. $\mathrm{supp}(\hat{f}) \leq k$.

If f vanishes on T, applying the uncertainty principle gives

$$(p - |T|) + k \geq (p - |T|) + \mathrm{supp}(\hat{f}) \geq p + 1,$$

thus

$$|T| \leq k - 1.$$

Hence, a nonzero k-sparse polynomial over $\mathbb{F}_{q^r}$ has at most $k - 1$ distinct zeros in any p-order multiplicative subgroup of $\mathbb{F}_{q^{p-1}}$.

This argument may provide a harmonic-analytic proof of a combinatorial sparsity bound for polynomial roots. The application is mentioned in the ending of Tao's [6], which may be of interest for cryptographic applications.

3.3 Influence of Single Variable in Boolean Functions

Let $f : \{-1, 1\}^n \to \{-1, 1\}$ be a Boolean function. f is called *balanced* iff $\#\{x : f(x) = -1\} = \#\{x : f(x) = 1\}$. In this section, the goal is to establish a lower bound about the influence of the input x on the output of $f(x)$. In this section, definitions and theorems are due to the notes [4] by Ryan O'Donnell, but the **Proof 3.3** is original.

We define $\mathbf{Inf}_i[f]$ to be the influence of the i-th coordinate on the output:

$$\mathbf{Inf}_i[f] := \mathbb{P}_{x \sim U(\{-1,1\}^n)}[f(x) \neq f(x^{\oplus i})],$$

where $x^{\oplus i}$ flips the i-th bit of x. Using the definition of the "influence," we define $\mathbf{I}[f] = \sum_{i=1}^{n} \mathbf{Inf}_i[f]$ as the total influence of f, and $\mathbf{MaxInf}[f] = \max_{1 \leq i \leq n} \mathbf{Inf}_i[f]$ as the maximum influence of all coordinates.

Then we introduce the notations of Fourier series on $G = (\{-1, 1\}^n, *) \cong C_2^n$, where C_2 is the 2-order cyclic group.

Since C_2^n is finite Abelian, let χ be a homomorphism from $\{-1, 1\}^n$ to $\mathbb{C}$. A representation of C_2 is either trivial representation $\chi_0(-1) = \chi_0(1) = 1$ or sign representation $\chi_1(1) = 1, \chi_1(-1) = -1$. The dual group $\{\chi_0, \chi_1\}$ is isomorphic to C_2. So a representation of $G \cong C_2^n$ is some tensor product of n χ_0 or χ_1's, since all these are 1-dimension, every character, which is the trace of the above representation, is of the form

$$\chi(x_1, \ldots, x_n) = \chi_{a_1}(x_1) \ldots \chi_{a_n}(x_n).$$

To simplify, a character is uniquely determined by $S = \{i : a_i = 1\}$. So any character can be written as

$$\chi_S = \prod_{i \in S} x_i.$$

In such sense, the Fourier series and its reverse are

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S(x),$$
$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x) \chi_S(x).$$

With Fourier series we have:

$$\begin{aligned} f(x^{i \leftarrow 1}) - f(x^{i \leftarrow -1}) &= \sum_{S \subseteq [n]} \hat{f}(S) \left(\chi_S(x^{i \leftarrow 1}) - \chi_S(x^{i \leftarrow -1}) \right) \\ &= \sum_{i \in S} 2 \hat{f}(S) \chi_{S \setminus \{i\}}(x), \end{aligned}$$

and we rewrite $\mathbf{Inf}_i[f]$ as:

$$\begin{aligned}\mathbf{Inf}_i[f] &= \mathbb{P}_{x\sim U(\{-1,1\}^n)}[f(x) \neq f(x^{\oplus i})] \\ &= \frac{1}{4}\mathbf{E}\left[\left(f(x^{i\leftarrow 1}) - f(x^{i\leftarrow -1})\right)^2\right] \\ &= \mathbf{E}\left[\left(\sum_{i\in S}\hat{f}(S)\chi_{S\setminus\{i\}}(x)\right)^2\right].\end{aligned}$$

Since the characters are mutually orthogonal and normalized with respect to the inner product

$$\langle f, g\rangle = \frac{1}{2^n}\sum_{x\in\{-1,1\}^n} f(x)g(x) = \mathbf{E}_{x\sim U(\{-1,1\}^n)}\left[f(x)g(x)\right]$$

so we have by Parseval Identity

$$\begin{aligned}\mathbf{Inf}_i[f] &= \left\|\sum_{i\in S}\hat{f}(S)\chi_{S\setminus\{i\}}\right\|_2^2 \\ &= \sum_{i\in S}\hat{f}(S)^2,\end{aligned}$$

and to sum it up, we have

$$\begin{aligned}\mathbf{I}[f] &= \sum_i\sum_{i\in S}\hat{f}(S)^2 \\ &= \sum_{S\subseteq[n]}|S|\hat{f}(S)^2.\end{aligned}$$

Definition 30 *Let $\rho \in [0,1]$. For fixed $x \in \{-1,1\}^n$ we write $y \sim N_\rho(x)$ to denote that the random string y is drawn as follows: for each $i \in [n]$ independently,*

$$y_i = \begin{cases} x_i, & \text{with probability } \frac{1+\rho}{2}, \\ -x_i, & \text{with probability } \frac{1-\rho}{2}, \end{cases}$$

i.e. with probability ρ the i-th coordinate remains the same, otherwise y_i is uniform on $\{0,1\}$.

Definition 31 *For $\rho \in [0,1]$, the noise operator with parameter ρ is the linear operator T_ρ on functions $f : \{-1,1\}^n \to \mathbb{R}$ defined by*

$$T_\rho f(x) = \mathop{\mathbf{E}}_{y\sim N_\rho(x)}[f(y)].$$

Claim 32 *For $f : \{-1,1\}^n \to \mathbb{R}$, the Fourier expansion of $T_\rho f$ is given by*

$$T_\rho f = \sum_{S\subseteq[n]}\rho^{|S|}\hat{f}(S)\chi_S.$$

Proof. Since T_ρ is a linear operator, it suffices to verify that

$$T_\rho\chi_S(x) = \prod_{i\in S}\mathop{\mathbf{E}}_{y\sim N_\rho(x)}[y_i] = \prod_{i\in S}(\rho x_i) = \rho^{|S|}\chi_S(x).$$

Here we used the fact that for $y \sim N_\rho(x)$ the bits y_i are independent and satisfy $\mathbf{E}[y_i] = \rho x_i$. ■

Theorem 33 (Kahn-Kalai-Linial) *For any balanced boolean function $f : \{-1,1\}^n \to \{-1,1\}$,*

$$\mathbf{MaxInf}[f] \geq \Omega\left(\frac{\log n}{n}\right).$$

Before we prove a weaker version of the theorem above, we need a lemma.

Lemma 34 *For all balanced boolean function $f : \{-1,1\}^n \mapsto \{-1,1\}$, we have*

$$\mathbf{I}[f] \geq \frac{\mathbf{Var}[f]}{-\log\rho}\log\frac{\mathbf{Var}[f]}{\langle f, T_\rho f\rangle}.$$

where for balanced f, $\mathbf{Var}[f] = \mathbf{E}[f(x)^2] - \mathbf{E}[f(x)]^2 = 1$.

Proof. Let $\varphi(t) = \langle f, T_{e^{-t}} f \rangle$. From the orthogonal decomposition of both functions, we derive the expression in Fourier coefficients and then compute the first and second derivatives of t:

$$\begin{aligned}
\varphi(t) &= \sum_{S \subseteq [n]} e^{-t|S|} \hat{f}(S)^2, \\
\varphi'(t) &= -\sum_{S \subseteq [n]} |S| e^{-t|S|} \hat{f}(S)^2, \\
\varphi''(t) &= \sum_{S \subseteq [n]} |S|^2 e^{-t|S|} \hat{f}(S)^2.
\end{aligned}$$

So we have the convexity of $\log \varphi(t)$ by Cauchy-Schwarz inequality:

$$\frac{\mathrm{d}^2 \log \varphi(t)}{\mathrm{d}t^2} = \frac{\varphi''(t)\varphi(t) - \varphi'(t)^2}{\varphi(t)^2} \geq 0.$$

As a result,

$$\begin{aligned}
\log \varphi(t) - \log \varphi(0) &\geq t \left. \frac{\mathrm{d} \log \varphi(t)}{\mathrm{d}t} \right|_{t=0} = \frac{t\varphi'(0)}{\varphi(0)} \\
&= -\frac{t \sum_{S \subseteq [n]} |S| \hat{f}(S)^2}{\sum_{S \subseteq [n]} \hat{f}(S)^2} \\
&= -\frac{t\mathbf{I}[f]}{\mathbf{Var}[f]}.
\end{aligned}$$

using Parseval Identity again.

Then we use the original notation to obtain

$$\mathbf{I}[f] \geq \frac{\mathbf{Var}[f]}{-\log \rho} \log \frac{\mathbf{Var}[f]}{\langle f, T_\rho f \rangle}.$$

■

We interpret this as another "uncertainty" lemma. $\mathbf{I}[f]$ is about how large the difference is when we flip the input; $\langle f, T_\rho f \rangle$ is about the influence of a noise, i.e. the difference of the difference. The lemma states that, if $\langle f, T_\rho f \rangle$ is close enough to 0, then $\mathbf{I}[f]$ will become large.

Here we prove a loose version of **KKL Theorem 33**. i.e. the final statement is $\mathbf{MaxInf}[f] \geq \Omega\left(\frac{1}{n}\right)$.

Lemma 35 *Let $\rho \in (0,1)$, if f is balanced, then $\langle f, T_\rho f \rangle \leq \rho$, with equality iff $f = \pm\chi_{\{i\}}$ for some $i \in [n]$.*

Proof of Theorem 33, a loose version. Assume that for all i, $\mathbf{Inf}_i[f] = o\left(\frac{1}{n}\right)$, thus $\mathbf{I}[f] = o(1)$.

Taking $\rho = e^{-t(n)}$ in **Lemma 34**,

$$\log \frac{1}{\langle f, T_{e^{-t(n)}} f \rangle} \leq t(n)\mathbf{I}[f] = o(t(n)).$$

Thus

$$\langle f, T_{e^{-t(n)}} f \rangle \geq \omega\left(e^{-t(n)}\right).$$

However, from **Lemma 35** we have $\langle f, T_{e^{-t(n)}} f \rangle \leq e^{-t(n)}$, which is a contradiction. ■

References

[1] Gorjan Alagic and Alexander Russell. *Uncertainty Principles for Compact Groups*. 2008. arXiv: `math/0608702 [math.RT]`. URL: `https://arxiv.org/abs/math/0608702`.

[2] Afonso S Bandeira, Megan E Lewis, and Dustin G Mixon. "Discrete uncertainty principles and sparse signal processing". In: *Journal of Fourier Analysis and Applications* 24.4 (2018), pp. 935–956.

[3] Tarek Emmrich and Stefan Kunis. *Real and finite field versions of Chebotarev's theorem*. 2025. arXiv: `2506.02947`. URL: `https://arxiv.org/abs/2506.02947`.

[4] Ryan O'Donnell. *Analysis of Boolean Functions*. 2021. arXiv: 2105.10386. URL: https://arxiv.org/abs/2105.10386.

[5] Alexander Russell and Igor E. Shparlinski. "Classical and quantum function reconstruction via character evaluation". In: *Journal of Complexity* 20.2 (2004). Festschrift for Harald Niederreiter, Special Issue on Coding and Cryptography, pp. 404–422. ISSN: 0885-064X. DOI: https://doi.org/10.1016/j.jco.2003.08.019. URL: https://www.sciencedirect.com/science/article/pii/S0885064X03001286.

[6] Terence Tao. *An uncertainty principle for cyclic groups of prime order*. 2004. arXiv: math/0308286 [math.CA]. URL: https://arxiv.org/abs/math/0308286.

[7] Guanghui Zhang. *On the Chebotarëv theorem over finite fields*. 2019. DOI: https://doi.org/10.1016/j.ffa.2018.11.004. URL: https://www.sciencedirect.com/science/article/pii/S1071579718301448.