Nov 1st, 2025

Uncertainty Principle and Applications
Author: Fangke Li

1 Textbook 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*

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

Proof. By the inverse Fourier transform, we have

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

By the Cauchy-Schwarz inequality,

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

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

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

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*

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

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, 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 $p - |A| + p - |B| \leq p - 1$.

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 $(e^{2\pi ijk/p})_{0\leq j,k<p}$ are non-zero, a result known as Chebotarëv's lemma.

Lemma 5 (Chebotarëv) *Let q be a prime number, and select $1 \leq k < p$ be an integer. Suppose $\omega_1, \dots, \omega_k$ are distinct q-th roots of unity, and let $n_1, \dots, n_k$ be distinct integers modulo p. Then the determinant of the $k \times k$ submatrix of $(e^{2\pi ijk/p})_{0\leq j,k<p}$ formed by the entries $(\omega_i^{n_j})_{1\leq k<p}$ 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 $P(z_1, \dots, z_n)$ be a polynomial with integer coefficients. If $\omega_1, \dots, \omega_n$ are p-th roots of unity (not necessarily distinct) such that $P(\omega_1, \dots, \omega_n) = 0$, then $P(1, \dots, 1)$ is a multiple of p.*

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

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

to be the reminder when $P(z^{k_1}, \dots, z^{k_n})$ is divided by $z^p - 1$. Thus, we have $Q(\omega) = 0$ and $Q(1) = P(1, \dots, 1)$. 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 $D(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$ by $D(z_1, \dots, z_n) = \det(z_j^{\xi_k})_{1\leq j,k\leq n}$. Certainly, $D(z_1, \dots, z_n) = 0$ when $z_i = z_j$ for any $1 \leq i < j \leq n$¿ Therefore we can write

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

Observe that

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

and thus

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

Consider operator $\left(z\frac{\mathrm{d}}{\mathrm{d}z}\right)$, 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 $D(z_1, \dots, z_n)$ at the point $z_1 = \cdots = z_n = 1$, only the term in which all the differential operators are applied to $\prod_{1\leq i<j\leq n} (z_j - z_i)$ is non-zero, as otherwise there are factors $(z_j - z_i)$ that are equal to 0. Therefore the applied result is equal to $P(1, \dots, 1)(n-1)!(n-2)! \cdots 1$.

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

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

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 $\mathcal{G} = \pi \circ \mathcal{F} \circ \eta$.*

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

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 $\tilde{A} \subseteq \hat{G} \setminus \operatorname{supp}(f)$ 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 Heisenberg's Uncertainty Principle

Definition 8 *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 9 *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.*

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

Theorem 10 (Heisenberg's uncertainty principle) *Let* $\psi \in \mathcal{S}(\mathbb{R})$*. Then we have*

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

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 $\Re(x) \le x$ along with $|\int f| \le \int |f|$, denoting $\psi'(x) = \dfrac{\mathrm{d}\psi(x)}{\mathrm{d}x}$, we have

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

To conclude,

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

■

A physicist might view the uncertainty principle 10 as a result of

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

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

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

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

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

and

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

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 Further Generalizations of Uncertainty Principle

2.1 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 11 (Paley-Wiener, single direction) *Let $f \in L^2(\mathbb{R})$ with $\operatorname{supp}(f) \subseteq B_R$ 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 $z \in \mathbb{C}$,*
$$|F(z)| \leq C e^{2\pi R |\operatorname{Im}(z)|}.$$

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 $|\operatorname{Im} z| \leq M$ for all $z \in K$. Then

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

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 $|z - z_0| < \delta$,

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

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:

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

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

Corollary 12 *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 11**, 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 13 (Amrein-Berthier) *Let $f \in L^2(\mathbb{R}^d)$, $E, F \subseteq \mathbb{R}$ have finite measure. Then*

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

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

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

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

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

Proof of Theorem 13. Fix E, F as above. We consider the operator T given by

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

If the L^2 operator norm of T is less than 1, then the hypothesis of **Lemma 14** holds with $C' = \dfrac{1}{1 - \|T\|}$, due to a simple calculation when $\operatorname{supp}(\hat{f}) \subseteq F$:

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

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 14** 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. ■

2.2 Uncertainty over Finite Fields

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

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

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 15 *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 [4], we know that if q is large enough, every minor of this matrix in **Definition 15** is non-zero. (**Corollary 17** in [1] 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 16 (Theorem A in [4])) *Let p, q be distinct odd primes such that $\mathrm{ord}_p(q) = p - 1$ and $q > \Gamma$, where*

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

and

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

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 [3], we have

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

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

Theorem 17 (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 15***. *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 16****). Then we have the following uncertainty relation:*

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

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

2.2.1 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 $j \in \mathbb{Z}_p$,

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

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 [3], which may be of interest for cryptographic applications.

2.3 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 [2] by Ryan O'Donnell, but the **Proof 2.3** 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

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

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

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

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

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

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 18 *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 19 *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 20 *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 21 (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 22 *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 21**. i.e. the final statement is $\mathbf{MaxInf}[f]\geq\Omega\left(\frac{1}{n}\right)$.

Lemma 23 *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 21, a loose version. Assume that for all i, $\mathbf{Inf}_i[f]=o\left(\frac{1}{n}\right)$, thus $\mathbf{I}[f]=o\left(1\right)$.

Taking $\rho=e^{-t(n)}$ in **Lemma 22**,

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

Thus

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

However, from **Lemma 23** we have $\langle f,T_{e^{-t(n)}}f\rangle\leq e^{-t(n)}$, which is a contradiction. ■

References

[1] 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`.

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

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

[4] 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`.