Uncertainty Principles for Finite Abelian Groups

Matthew J. Hirn

Norbert Wiener Center
University of Maryland

September 20, 2007

Outline

Outline

The Fourier Transform on $\mathbb{Z}/N\mathbb{Z}$

- $l^2(\mathbb{Z}/N\mathbb{Z}) := \{f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}\}$

Definition

Let $f \in l^2(\mathbb{Z}/N\mathbb{Z})$. The *Fourier transform* of f, denoted $\hat{f}$, is

$$\hat{f}(\omega) := \frac{1}{\sqrt{N}} \sum_{t \in \mathbb{Z}/N\mathbb{Z}} f(t) e^{-2\pi i \omega t/N}, \qquad \omega \in \mathbb{Z}/N\mathbb{Z}$$

The Donoho-Stark Uncertainty Principle

- $\text{supp}(f) := \{t \in \mathbb{Z}/N\mathbb{Z} : f(t) \neq 0\}$
- Let $N_t = |\text{supp}(f)|$ and $N_\omega = |\text{supp}(\hat{f})|$

Theorem (Donoho and Stark 1989)

If $f \in l^2(\mathbb{Z}/N\mathbb{Z})$ is a non-zero function, then

$$\begin{aligned} N_t N_\omega &\geq N \\ N_t + N_\omega &\geq 2\sqrt{N} \end{aligned}$$

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Proof of D-S Uncertainty Principle

Lemma

If $|\mathrm{supp}(f)| = N_t$, *then* $\hat{f}$ *cannot have* N_t *consecutive zeroes.*

Proof of D-S Uncertainty Principle.

- Suppose N_t divides N
- Partition $\mathbb{Z}/N\mathbb{Z}$ into N/N_t intervals of length N_t
- By the lemma, each interval contains at least one element of $\mathrm{supp}(\hat{f})$
- Thus $N_\omega \geq N/N_t$
- Argument for when N_t does not divide N is similar

Application to Signal Recovery I

- Let $s \in l^2(\mathbb{Z}/N\mathbb{Z})$ be a signal
- If we sample at every frequency, i.e., we know $\hat{s}(\omega)$ for all $\omega \in \mathbb{Z}/N\mathbb{Z}$, then we can reconstruct s via Fourier inversion

$$s(t) = \frac{1}{\sqrt{N}} \sum_{\omega \in \mathbb{Z}/N\mathbb{Z}} \hat{s}(\omega) e^{2\pi i \omega t/N}$$

Application to Signal Recovery I

- Suppose instead we only have knowledge of $r \in l^2(\mathbb{Z}/N\mathbb{Z})$, a bandlimited version of s, i.e. $r = P_B s$
- Assume

$$r(t) = P_B s(t) = \frac{1}{\sqrt{N}} \sum_{\omega \in B} \hat{s}(\omega) e^{2\pi i \omega t/N}$$

- $$\hat{r}(\omega) = \begin{cases} \hat{s}(\omega) & \omega \in B \\ 0 & \text{otherwise} \end{cases}$$

- Set $N_\omega = |B^c|$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_t N_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_t N_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0.$
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_tN_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_tN_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_t N_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_t N_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

Theorem (Donoho and Stark 1989)

If it is known that s has only N_t non-zero elements, and if $2N_tN_\omega < N$, then s can be uniquely reconstructed from r.

Proof.

We will show uniqueness:

- Suppose that s_1 also generates r, i.e. $P_B s_1 = r = P_B s$
- Set $h := s_1 - s \Longrightarrow P_B h = 0$.
- $\text{supp}(s_1), \text{supp}(s) \leq N_t \Longrightarrow \text{supp}(h) \leq 2N_t = N_t'$
- $P_B h = 0 \Longrightarrow \text{supp}(\hat{h}) \subset B^c \Longrightarrow |\text{supp}(\hat{h})| \leq N_\omega$
- $N_t' N_\omega = 2N_tN_\omega < N \Longrightarrow h \equiv 0$

Application to Signal Recovery I

- The restriction $2N_tN_\omega < N$ is extremely limiting.
- For example, even if $N_\omega = N/10$, then $N_t < 5$ is needed.
- In practice, however, if the spike positions of a signal s are scattered at random, results showed that it is possible to recover many more spikes than $2N_tN_\omega < N$ indicates.
- In fact this turns out to be true, see research on *compressed sensing*.

Outline

Preliminary Definitions

- Let G be a finite abelian additive group

Definition

Let $e : G \times G \to S^1 := \{z \in \mathbb{C} : |z| = 1\}$. We say e is a nondegenerate *bi-character* of G if it has the following properties:

- $e(t + t', \omega) = e(t, \omega)e(t', \omega)$
- $e(t, \omega + \omega') = e(t, \omega)e(t, \omega')$
- For every $t \neq 0$ there exists an $\omega \in G$ such that $e(t, \omega) \neq 1$
- For every $\omega \neq 0$ there exists a $t \in G$ such that $e(t, \omega) \neq 1$

The Fourier Transform on G

- Let $|G|$ denote the cardinality of G
- $l^2(G) := \{f : G \to \mathbb{C}\}$

Definition

Let $f \in l^2(G)$. The *Fourier transform* of f, denoted $\hat{f}$, is

$$\hat{f}(\omega) := \frac{1}{\sqrt{|G|}} \sum_{t \in G} f(t)\overline{e(t,\omega)}, \qquad \omega \in G$$

An Uncertainty Principle for G

- $\text{supp}(f) = \{t \in G : f(t) \neq 0\}$

Theorem (K.T. Smith 1990)

If $f \in l^2(G)$ is a non-zero function, then

$$\begin{aligned} |\text{supp}(f)||\text{supp}(\hat{f})| &\geq |G| \\ |\text{supp}(f)| + |\text{supp}(\hat{f})| &\geq 2\sqrt{|G|} \end{aligned}$$

Outline

Limiting Examples

Example

- $f(t) = \delta_0(t) \Longrightarrow |\text{supp}(f)| = 1$
- $\hat{f}(\omega) = \frac{1}{\sqrt{|G|}}$ for all $\omega \in G \Longrightarrow |\text{supp}(\hat{f})| = |G|$

Example

- Let H be a subgroup of G
- $f = \chi_H \Longrightarrow |\text{supp}(f)| = |H|$
- It's not hard to show that $|\text{supp}(\hat{f})| = |G|/|H|$
- Up to translation, modulation, and scalar multiplication, this is the only example where equality is attained.

Limiting Examples

Example

- $f(t) = \delta_0(t) \Longrightarrow |\text{supp}(f)| = 1$
- $\hat{f}(\omega) = \frac{1}{\sqrt{|G|}}$ for all $\omega \in G \Longrightarrow |\text{supp}(\hat{f})| = |G|$

Example

- Let H be a subgroup of G
- $f = \chi_H \Longrightarrow |\text{supp}(f)| = |H|$
- It's not hard to show that $|\text{supp}(\hat{f})| = |G|/|H|$
- Up to translation, modulation, and scalar multiplication, this is the only example where equality is attained.

Outline

The Uncertainty Principle for $\mathbb{Z}/p\mathbb{Z}$

- Consider the special case when $G = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number.
- Since $\mathbb{Z}/p\mathbb{Z}$ has no non-trivial subgroups, we'd hope to improve upon the D-S Uncertainty Principle.

Theorem (Biró; Meshulam; Tao 2005)

Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a non-zero function, then

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

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a function f such that $\mathrm{supp}(f) = A$ and $\mathrm{supp}(\hat{f}) = B$.

The Uncertainty Principle for $\mathbb{Z}/p\mathbb{Z}$

- Consider the special case when $G = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number.
- Since $\mathbb{Z}/p\mathbb{Z}$ has no non-trivial subgroups, we'd hope to improve upon the D-S Uncertainty Principle.

Theorem (Biró; Meshulam; Tao 2005)

Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a non-zero function, then

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

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a function f such that $\mathrm{supp}(f) = A$ and $\mathrm{supp}(\hat{f}) = B$.

The Uncertainty Principle for $\mathbb{Z}/p\mathbb{Z}$

Example

- This uncertainty principle is a vast improvement over the D-S uncertainty principle, when N is a prime number.
- Take $N = p = 101$
- D-S UP: $|\text{supp}(f)| + |\text{supp}(\hat{f})| \geq 2\sqrt{101} > 20$
- UP for $\mathbb{Z}/p\mathbb{Z}$: $|\text{supp}(f)| + |\text{supp}(\hat{f})| \geq 101 + 1 = 102$

First Lemma

Lemma

Let p be a prime number, n a positive integer, and let $P(z_1, \ldots, z_n)$ be a polynomial with integer coefficients. Suppose that we have n p^{th} roots of unity $\zeta_1, \ldots, \zeta_n$ (not necessarily distinct) such that $P(\zeta_1, \ldots, \zeta_n) = 0$. Then $P(1, \ldots, 1)$ is a multiple of p.

Proof of First Lemma

Proof.

- $\zeta := e^{2\pi i/p} \Longrightarrow \zeta_j = \zeta^{k_j}, \quad 0 \leq k_j < p$
- $Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \mod z^p - 1$
- $Q(\zeta) = 0$ and $Q(1) = P(1, \ldots, 1)$
- $\deg(Q) \leq p - 1$ and Q has integer coefficients
- Q is an integer multiple of the minimal polynomial of ζ, $1 + z + \ldots + z^{p-1}$

Proof of First Lemma

Proof.

- $\zeta := e^{2\pi i/p} \Longrightarrow \zeta_j = \zeta^{k_j}, \quad 0 \leq k_j < p$
- $Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \mod z^p - 1$
- $Q(\zeta) = 0$ and $Q(1) = P(1, \ldots, 1)$
- $\deg(Q) \leq p - 1$ and Q has integer coefficients
- Q is an integer multiple of the minimal polynomial of ζ, $1 + z + \ldots + z^{p-1}$

Proof of First Lemma

Proof.

- $\zeta := e^{2\pi i/p} \Longrightarrow \zeta_j = \zeta^{k_j}, \quad 0 \leq k_j < p$
- $Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \mod z^p - 1$
- $Q(\zeta) = 0$ and $Q(1) = P(1, \ldots, 1)$
- $\deg(Q) \leq p - 1$ and Q has integer coefficients
- Q is an integer multiple of the minimal polynomial of ζ, $1 + z + \ldots + z^{p-1}$

Proof of First Lemma

Proof.

- $\zeta := e^{2\pi i/p} \Longrightarrow \zeta_j = \zeta^{k_j}, \quad 0 \leq k_j < p$
- $Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \mod z^p - 1$
- $Q(\zeta) = 0$ and $Q(1) = P(1, \ldots, 1)$
- $\deg(Q) \leq p - 1$ and Q has integer coefficients
- Q is an integer multiple of the minimal polynomial of ζ, $1 + z + \ldots + z^{p-1}$

Proof of First Lemma

Proof.

- $\zeta := e^{2\pi i/p} \Longrightarrow \zeta_j = \zeta^{k_j}, \quad 0 \leq k_j < p$
- $Q(z) := P(z^{k_1}, \ldots, z^{k_n}) \mod z^p - 1$
- $Q(\zeta) = 0$ and $Q(1) = P(1, \ldots, 1)$
- $\deg(Q) \leq p - 1$ and Q has integer coefficients
- Q is an integer multiple of the minimal polynomial of ζ, $1 + z + \ldots + z^{p-1}$

Key Lemma

Lemma (Chebotarëv 1926)

Let p be a prime number and $1 \leq n \leq p$. Let $t_1, \ldots, t_n$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$ and let $\omega_1, \ldots, \omega_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Then the matrix $(e^{2\pi i t_j \omega_k / p})_{1 \leq j,k \leq n}$ has non-zero determinant.

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Proof of Key Lemma

Proof.

- $\zeta_j := e^{2\pi i t_j/p} \Longrightarrow$ we want $\det(\zeta_j^{\omega_k})_{1\leq j,k\leq n} \neq 0$
- $D(z_1,\ldots,z_n) := \det(z_j^{\omega_k})_{1\leq j,k\leq n}$
- D has integer coefficients; however $D(1,\ldots,1) = 0$
- $D(z_1,\ldots,z_n) = P(z_1,\ldots,z_n)\prod_{1\leq j<j'\leq n}(z_j - z_{j'})$
- P is a polynomial with integer coefficients; we will show $P(1,\ldots,1)$ is not a multiple of p
- $I := (z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1\cdots(z_n\frac{d}{dz_n})^{n-1}D(z_1,\ldots,z_n)|_{z_1=\ldots=z_n=1}$
- $I = (n-1)!(n-2)!\cdots 0!P(1,\ldots,1)$
- Therefore it suffices to show I is not a multiple of p.
- $I = \det(\omega_k^{j-1})_{1\leq j,k\leq n} = \pm\prod_{1\leq k<k'\leq n}(\omega_k - \omega_{k'})$

Corollary to Key Lemma

Corollary

Let p be a prime number and T, Ω subsets of $\mathbb{Z}/p\mathbb{Z}$. Let $l^2(T)$ (resp. $l^2(\Omega)$) be the space of functions that are zero outside of T (resp. Ω). The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l^2(T) \to l^2(\Omega)$ is defined as

$$\mathcal{F}_{T\to\Omega} f := \hat{f}|_\Omega \text{ for all } f \in l^2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection.

Proof of Theorem.

- Suppose $|\text{supp}(f)| + |\text{supp}(\hat{f})| \leq p$
- $T := \text{supp}(f)$
- $\exists\, \Omega \subset \mathbb{Z}/p\mathbb{Z}$, disjoint from $\text{supp}(\hat{f})$ and $|\Omega| = |T|$.
- $\mathcal{F}_{T\to\Omega} f = 0 \longrightarrow f = 0$ $\square$

Corollary to Key Lemma

Corollary

Let p be a prime number and T, Ω subsets of $\mathbb{Z}/p\mathbb{Z}$. Let $l^2(T)$ (resp. $l^2(\Omega)$) be the space of functions that are zero outside of T (resp. Ω). The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l^2(T) \to l^2(\Omega)$ is defined as

$$\mathcal{F}_{T\to\Omega} f := \hat{f}|_\Omega \text{ for all } f \in l^2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection.

Proof of Theorem.

- Suppose $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \leq p$
- $T := \mathrm{supp}(f)$
- $\exists \Omega \subset \mathbb{Z}/p\mathbb{Z}$, disjoint from $\mathrm{supp}(\hat{f})$ and $|\Omega| = |T|$.
- $\mathcal{F}_{T\to\Omega} f = 0 \Longrightarrow f \equiv 0$ $\square$

Corollary to Key Lemma

Corollary

Let p be a prime number and T, Ω subsets of $\mathbb{Z}/p\mathbb{Z}$. Let $l^2(T)$ (resp. $l^2(\Omega)$) be the space of functions that are zero outside of T (resp. Ω). The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l^2(T) \to l^2(\Omega)$ is defined as

$$\mathcal{F}_{T\to\Omega} f := \hat{f}|_\Omega \text{ for all } f \in l^2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection.

Proof of Theorem.

- Suppose $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \leq p$
- $T := \mathrm{supp}(f)$
- $\exists \Omega \subset \mathbb{Z}/p\mathbb{Z}$, disjoint from $\mathrm{supp}(\hat{f})$ and $|\Omega| = |T|$.
- $\mathcal{F}_{T\to\Omega} f = 0 \Longrightarrow f \equiv 0$ $\square$

Corollary to Key Lemma

Corollary

Let p be a prime number and T, Ω subsets of $\mathbb{Z}/p\mathbb{Z}$. Let $l^2(T)$ (resp. $l^2(\Omega)$) be the space of functions that are zero outside of T (resp. Ω). The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l^2(T) \to l^2(\Omega)$ is defined as

$$\mathcal{F}_{T\to\Omega} f := \hat{f}|_\Omega \text{ for all } f \in l^2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection.

Proof of Theorem.

- Suppose $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \leq p$
- $T := \mathrm{supp}(f)$
- $\exists\, \Omega \subset \mathbb{Z}/p\mathbb{Z}$, disjoint from $\mathrm{supp}(\hat{f})$ and $|\Omega| = |T|$.
- $\mathcal{F}_{T\to\Omega} f = 0 \Longrightarrow f \equiv 0$ $\square$

Corollary to Key Lemma

Corollary

Let p be a prime number and T, Ω subsets of $\mathbb{Z}/p\mathbb{Z}$. Let $l^2(T)$ (resp. $l^2(\Omega)$) be the space of functions that are zero outside of T (resp. Ω). The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l^2(T) \to l^2(\Omega)$ is defined as

$$\mathcal{F}_{T\to\Omega} f := \hat{f}|_\Omega \text{ for all } f \in l^2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection.

Proof of Theorem.

- Suppose $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \leq p$
- $T := \mathrm{supp}(f)$
- $\exists\, \Omega \subset \mathbb{Z}/p\mathbb{Z}$, disjoint from $\mathrm{supp}(\hat{f})$ and $|\Omega| = |T|$.
- $\mathcal{F}_{T\to\Omega} f = 0 \Longrightarrow f \equiv 0$ $\square$

Outline

Sparse Polynomials/Cauchy-Davenport Inequality

Proposition

Let $P(z) = \sum_{j=0}^{k} c_j z^{n_j}$ *with* $c_j \neq 0$ *and* $0 \leq n_0 < \ldots < n_k < p$. *If* P *is restricted to the* p^{th} *roots of unity* $\{z : z^p = 1\}$, *then* P *can have at most* k *zeroes.*

Theorem (Cauchy-Davenport Inequality)

Let A *and* B *be non-empty subsets of* $\mathbb{Z}/p\mathbb{Z}$ *and set* $A + B := \{a + b : a \in A, b \in B\}$. *Then*

$$|A + B| \geq \min(|A| + |B| - 1, p)$$

Sparse Polynomials/Cauchy-Davenport Inequality

Proposition

Let $P(z) = \sum_{j=0}^{k} c_j z^{n_j}$ *with* $c_j \neq 0$ *and* $0 \leq n_0 < \ldots < n_k < p$. *If* P *is restricted to the* p^{th} *roots of unity* $\{z : z^p = 1\}$, *then* P *can have at most* k *zeroes.*

Theorem (Cauchy-Davenport Inequality)

Let A *and* B *be non-empty subsets of* $\mathbb{Z}/p\mathbb{Z}$ *and set* $A + B := \{a + b : a \in A, b \in B\}$. *Then*

$$|A + B| \geq \min(|A| + |B| - 1, p)$$

Application to Signal Recovery II

Theorem (Candes, Romberg, and Tao 2006)

Suppose that the signal length N is a prime number. Let $\Omega \subset \mathbb{Z}/N\mathbb{Z}$, and let $f \in l^2(\mathbb{Z}/N\mathbb{Z})$ be a signal supported on T such that

$$|T| \leq \frac{|\Omega|}{2}$$

Then f can be reconstructed uniquely from Ω and $\hat{f}|_\Omega$. Conversely, if Ω is not the set of all N frequencies, then there exist distinct f and g such that $|\mathrm{supp}(f)|, |\mathrm{supp}(g)| \leq |\Omega|/2 + 1$ and such that $\hat{f}|_\Omega = \hat{g}|_\Omega$.

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \Longrightarrow$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\Longrightarrow \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_\Omega \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \Longrightarrow$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\Longrightarrow \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_{\Omega} \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \implies$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\implies \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_\Omega \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \Longrightarrow$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\Longrightarrow \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_\Omega \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \Longrightarrow$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\Longrightarrow \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_{\Omega} \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Proof.

We prove the second part:

- $|\Omega| < N \Longrightarrow$ we can find disjoint subsets T, S of Ω such that
  - $|T|, |S| \leq |\Omega|/2 + 1$
  - $|T| + |S| = |\Omega| + 1$
- Let $\omega_0 \in \mathbb{Z}/N\mathbb{Z}$, $\omega_0 \notin \Omega$
- Corollary $\Longrightarrow \mathcal{F}_{T \cup S \to \Omega \cup \{\omega_0\}}$ is a bijection.
- Therefore $\exists\, h$ supported on $T \cup S$ such that $\hat{h}|_\Omega \equiv 0$ but $\hat{h}(\omega_0) \neq 0$.
- In particular, h is not identically zero.
- $f := h|_T$, $g := -h|_S$

Application to Signal Recovery II

Example

- For signals of length N, where N is a prime number, this sparsity bound is far better than the one proposed based off the D-S uncertainty principle.
- Take $N = 101$ and assume we sample 91 of the 101 frequencies (i.e. $|\Omega| = 91$).
- D-S UP: $2|T||\Omega^c| < 101 \Longrightarrow 20|T| < 101 \Longrightarrow |T| \leq 5$
- UP for $\mathbb{Z}/p\mathbb{Z}$: $|T| \leq |\Omega|/2 = 91/2 \Longrightarrow |T| \leq 45$


Emmanuel Candes, Justin Romberg, and Terrence Tao.
Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information.
IEEE Transactions on Information Theory, 52(2):489–509, 2006.


David L. Donoho and Philip B. Stark.
Uncertainty principles and signal recovery.
Siam J. Appl. Math, 49(3):906–931, 1989.


P.E. Frenkel.
Simple proof of chebotarëv's theorem on roots of unity.
math.AC/0312398.


Roy Meshulam.
An uncertainty inequality for finite abelian groups.
math.CO/0312407.


K.T. Smith.

The uncertainty principle on groups.
SIAM J. Appl. Math, 50:876–882, 1990.


P. Stevenhagen and H.W. Lenstra Jr.
Chebotarëv and his density theorem.
Math. Intelligencer, 18(2):26–37, 1996.


Terrence Tao.
An uncertainty principle for cyclic groups of prime order.
Math. Res. Letters, 11:121–127, 2005.


A. Terras.
Fourier Analysis on Finite Groups and Applications, volume 43 of *London Mathematical Society Student Texts*.
Cambridge University Press, Cambridge, 1999.