Uncertainty Principles and Exact Signal Recovery for Linear Maps

Eli Seamans

April 21, 2024

Abstract

The Discrete Fourier Transform (DFT) has many applications to signal processing. One application leverages the uncertainty principle associated with the DFT, allowing a message to be reconstructed exactly from incomplete data. We generalize this uncertainty principle to an arbitrary invertible linear transformation, and show that the DFT is in some sense the optimal transform for this purpose. Stronger recovery properties are possible for sparse signals via the DFT, and we will give an overview of this theory, and provide examples of non-DFT transforms that satisfy this stronger recovery property.

1 Introduction

1.1 The discrete Fourier transform and the classical uncertainty principle

First we establish some notation. Throughout we will let V denote the complex vector space of functions from $\mathbb{Z}_N^d$ to $\mathbb{C}$.

Definition 1.1. *Given a function $f : \mathbb{Z}_N^d \to \mathbb{C}$, we define its Fourier transform $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ by*

$$\hat{f}(m) = N^{-d} \sum_{x \in \mathbb{Z}_N^d} \chi(-m \cdot x) f(x),$$

where $m \in \mathbb{Z}_N^d$, $m \cdot x$ is the dot product, and $\chi(y) = e^{\frac{2\pi i y}{N}}$. We will also use $\mathcal{F} : V \to V$ to refer to the Fourier transform.

Proposition 1.1. *Properties of the Fourier transform:*

a. $\mathcal{F}$ is linear.

b. $\mathcal{F}$ is invertible, with inverse given by

$$f(x) = \sum_{m \in \mathbb{Z}_N^d} \chi(m \cdot x) \hat{f}(m).$$

c. $\mathcal{F}$ satisfies the Plancherel identity:

$$\sum_{x\in\mathbb{Z}_N^d} |f(x)|^2 = N^d \sum_{m\in\mathbb{Z}_N^d} |\hat{f}(m)|^2.$$

In order to prove this, we will need the following lemma:

Lemma 1.1. *Let $a \in \mathbb{Z}_N$. Then*

$$\sum_{y\in\mathbb{Z}_N} \chi(ay) = \begin{cases} N \text{ if } a = 0 \\ 0 \text{ if } a \neq 0 \end{cases}$$

Proof. Linearity follows immediately from the linearity of finite sums. Before we prove (b) and (c), we will prove the lemma.

If $a = 0$ then $\chi(ay) \equiv 1$ and so the sum equals N, since $|\mathbb{Z}_N| = N$. If $a \neq 0$, then

$$\sum_{y\in\mathbb{Z}_N} \chi(ay) = \sum_{y=1}^{N} \chi(a)^y = \frac{1-\chi(a)^N}{1-\chi(a)} = 0,$$

where the second equality follows since

$$\chi(a)^N = \chi(aN) = e^{2\pi i} = 1,$$

and the third equality follows by interpreting the second as a geometric sum. This proves the lemma.

Next we prove (b). With the lemma, this can be verified by direct computation:

$$\sum_{m\in\mathbb{Z}_N^d} \chi(m\cdot x)\hat{f}(m) = N^{-d} \sum_{m\in\mathbb{Z}_N^d} \sum_{y\in\mathbb{Z}_N^d} \chi(m\cdot(x-y))f(y) = (*).$$

We can expand the sum over $m = (m_1, ..., m_d)$ to sums over each coordinate. Given that

$$\chi(m\cdot(x-y)) = \prod_{i=1}^{d} \chi(m_i(x_i - y_i)),$$

these sums will decouple, and so we have that

$$(*) = N^{-d} \sum_{y\in\mathbb{Z}_N^d} f(y) \left(\prod_{i=1}^{d} \left(\sum_{m_i\in\mathbb{Z}_N} \chi(m_i(x_i - y_i)) \right) \right).$$

To deal with the innermost sum, we apply the lemma with $a = x_i - y_i$ to conclude that the only terms that contribute to $(*)$ are the ones where $x_i = y_i$, so we can conclude that

$$(*) = N^{-d} f(x) \prod_{i=1}^{d} N = f(x),$$

verifying the inverse formula.

To prove (c), we first expand the left hand side with the inversion formula:

$$\begin{aligned}\sum_{x\in\mathbb{Z}_N^d}|f(x)|^2 &= \sum_{x\in\mathbb{Z}_{\mathbb{N}}}\left|\sum_{m\in\mathbb{Z}_N^d}\chi(m\cdot x)\hat{f}(m)\right|^2 \\ &= \sum_{x\in\mathbb{Z}_{\mathbb{N}}}\left(\sum_{m\in\mathbb{Z}_N^d}\chi(m\cdot x)\hat{f}(m)\right)\overline{\left(\sum_{m'\in\mathbb{Z}_N^d}\chi(m'\cdot x)\hat{f}(m')\right)} \\ &= \sum_{x\in\mathbb{Z}_N^d}\sum_{m\in\mathbb{Z}_N^d}\sum_{m'\in\mathbb{Z}_N^d}\chi((m-m')\cdot x)\hat{f}(m)\overline{\hat{f}(m')} \\ &= N^d\sum_{m\in\mathbb{Z}_N^d}\hat{f}(m)\overline{\hat{f}(m')} = N^d\sum_{m\in\mathbb{Z}_N^d}|\hat{f}(m)|^2.\end{aligned}$$

The fourth line follows from applying the lemma while summing over each coordinate x_i in x.

□

These properties can be used to prove the following result, which is central to this paper:

Theorem 1.1. *(Classical uncertainty principle) Let $f:\mathbb{Z}_N^d\to\mathbb{C}$ be a function that is not identically zero. Suppose that supp$(f)=E$ and supp$(\hat{f})=S$. Then*

$$|E|\cdot|S|\geq N^d.$$

This result essentially says that both f and $\hat{f}$ cannot each be highly localized. For example, if $E=\{y\}$ (i.e. f is supported on exactly one point), then

$$\hat{f}(m)=\sum_{x\in\mathbb{Z}_N^d}\chi(-m\cdot x)f(x)\equiv\chi(-m\cdot y)f(y)\neq 0,$$

so $\hat{f}$ is supported on all of $\mathbb{Z}_N^d$. Note also that this shows the uncertainty principle is sharp in general.

Proof. First we write f with the inversion formula, then estimate $|f(x)|^2$ with the Cauchy Schwarz inequality to see that

$$\begin{aligned}|f(x)|^2\leq\left(\sum_{m\in S}1\right)\left(\sum_{m\in S}\left|\chi(m\cdot x)\hat{f}(m)\right|^2\right) &= |S|\sum_{m\in S}|\hat{f}(m)|^2 \\ &= N^{-d}|S|\sum_{x\in E}|f(x)|^2,\end{aligned}$$

with the second line obtained by applying Plancherel. Summing both the left and right sides over E, and cancelling the $\sum_{x\in E}|f(x)|^2$ factor (which is nonzero by the assumption that f is not the zero function), we obtain that

$$1\leq N^{-d}|E|\cdot|S|,$$

and we are done.

□

This inequality has a well documented application to signal recovery. We will consider the function f as encoding some message to be transmitted (e.g. if $f : \mathbb{Z}_N^1 \to \{0, 1\}$, then f represents a binary string of length N). Then if we transmit f via its Fourier transform, it may be that some of the Fourier values are lost, that is, only

$$\{\hat{f}(m)\}_{m \notin S}$$

is received, for some $S \subset \mathbb{Z}_N^d$.

If we cannot recover f from this data uniquely, then there is another function $g : \mathbb{Z}_N^d \to \mathbb{C}$ supported on a set F such that $|E| = |F|$, and satisfying

$$\hat{g}|_{S^c} = \hat{f}|_{S^c}.$$

Then $h = f - g$ is supported on a subset of $E \cup F$, which has size at most $2|E|$. Since the Fourier transform is linear, and $\hat{f}$ and $\hat{g}$ agree outside S, $\hat{h}$ is supported on S. By assumption h is not identically zero, so we may apply the classical uncertainty principle to h, yielding that

$$|E| \cdot |S| \geq N^d/2.$$

This gives us the following result:

Theorem 1.2. *Let $f : \mathbb{Z}_N^d \to \mathbb{C}$ be a functionn supported in E, and $\hat{h} : \mathbb{Z}_N^d \to \mathbb{C}$ be a function such that*

$$\hat{h}(m) = \begin{cases} \hat{f}(m) \text{ if } m \notin S \\ 0 \text{ if } m \in S \end{cases}$$

for some $S \subset \mathbb{Z}_N^d$. Then provided

$$|E| \cdot |S| < N^d/2,$$

f can be recovered exactly from $\hat{h}$.

We will show that this result also holds for an entire class of linear operators $T : V \to V$.

1.2 Stronger uncertainty principles

Given that Theorem 1.2 holds for any function $f \in V$, it is bound to have some limitations. For instance, if f encodes a binary message that contains an equal number of ones and zeros, then $|E| = N^d/2$, and so the set S of missing data must satisfy $|S| < 1$ in order to guarantee recovery. But since $|S|$ is a nonnegative integer, this means $|S| = 0$ and so for a general signal of this profile, complete recovery is only possible with complete knowledge of its Fourier transform.

However, it turns out that if we impose additional assumptions on the support E of the signal, stronger results can be obtained. If instead of applying Cauchy-Schwarz when we proved the uncertainty principle, we applied Holder's inequality, with $1 \leq p < q \leq \infty$, we would have that

$$|f(x)| \leq |S|^{1/p} \left(\sum_{m \in S} |\hat{f}(m)|^q \right)^{1/q} = |S| \left(\frac{1}{|S|} \sum_{m \in S} |\hat{f}(m)|^q \right)^{1/q}$$

(the equality follows from the fact that $\frac{1}{p} + \frac{1}{q} = 1$). The following definition gives a condition for the set S that allows us to utlilize this idea.

Definition 1.2. *Let $S \subset \mathbb{Z}_N^d$. Then S satisfies the (p, q) restriction bound (for $1 \leq p < q \leq \infty$) if there is a constant $C_{p,q}$ independent of N and S such that for any function $f : \mathbb{Z}_N^d \to \mathbb{C}$,*

$$\left(\frac{1}{|S|} \sum_{m \in S} |\hat{f}(m)|^q \right)^{1/q} \leq C_{p,q} \cdot N^{-d} \left(\sum_{x \in \mathbb{Z}_N^d} |f(x)|^p \right)^{1/p}.$$

If $q = \infty$, we take the left hand side to be $\|f\|_\infty$.

If we suppose that S satisfies the (p, q) restriction bound (and again assuming f is supported on a nonempty set E), then we have

$$|f(x)| \leq |S| \left(\frac{1}{|S|} \sum_{m \in S} |\hat{f}(m)|^q \right)^{1/q} \leq C_{p,q} |S| N^{-d} \left(\sum_{y \in E} |f(y)|^p \right)^{1/p}.$$

Raising each side to the pth power, summing over $x \in E$, taking the pth root, then cancelling the common $\left(\sum_{y \in E} |f(y)|^p \right)^{1/p}$ factor from each side implies that

$$\frac{N^d}{C_{p,q}} \leq |E|^{\frac{1}{p}} |S|,$$

which is stronger than the classical uncertainty principle if $p > 1$. Iosevich and Mayeli were able to show that certain sets satisfy a $(4/3, 2)$ restriction estimate. We build the theory for this condition below.

Definition 1.3. *Let $E \subset \mathbb{Z}_N^d$ be a set. Then the additive energy $\mathcal{E}(E)$ is defined by*

$$\mathcal{E}(E) := |\{(x, x', y, y') \in E^4 : x + y = x' + y'\}|.$$

Observe that trivially every quadruple (x, x, y, y) for any $x, y \in E$ is counted in the above definition, so

$$|E|^2 \leq \mathcal{E}(E).$$

Moreover, any triple (x, y, x') uniquely determines $y' = x + y - x'$, and so we also have that

$$\mathcal{E}(E) \leq |E|^3.$$

We say that a set is a *Salem set* if $\mathcal{E}(E) = C|E|^2$ for some absolute constant C.

One example of a Salem set is

$$P = \{(t, t^2) : t \in \mathbb{Z}_N\} \subset \mathbb{Z}_N^2$$

for $N > 2$. We can see this by observing that if

$$(t + s, t^2 + s^2) = (t' + s', (t')^2 + (s')^2),$$

then equating the first coordinates and squaring implies that

$$t^2 + 2st + s^2 = (t')^2 + 2s't' + (s')^2 \Rightarrow 2st = 2s't'.$$

Subtracting these from the equality in the second coefficients yields that

$$t^2 - 2st + s^2 = (t - s)^2 = (t' - s')^2 = (t')^2 - 2s't' + (s')^2,$$

so

$$t - s = \pm(t' - s').$$

Since $t + s = t' + s'$, this means there are three possible cases where each of these equalities can be satisfied:

1. $s = s'$ and $t = t'$
2. $s = t'$ and $t = s'$
3. $s = -t'$ and $t = -s'$

This means that for any choice of two points in P, there are at most three quadruples (x, x', y, y') satisfying $x + y = x' + y'$, so

$$\mathcal{E}(P) \leq 3|P|^2.$$

Iosevich and Mayeli's $(4/3, 2)$ restriction estimate holds exactly when the underlying set S is a Salem set. To give an idea of why additive energy is a natural object to consider, we look at the following computation. Let $E \subset \mathbb{Z}_N^d$ and let $E(x)$ denote its indicator function. Then

$$\begin{aligned}
\sum_{m \in \mathbb{Z}_N^d} |\hat{E}(m)|^4 &= \sum_{m \in \mathbb{Z}_N^d} \hat{E}^2(m)\overline{\hat{E}^2(m)} \\
&= \frac{1}{N^{4d}} \sum_{x,x',y,y' \in \mathbb{Z}_N^d} E(x)E(y)E(x')(E(y')\chi(-m \cdot (x + y - x' - y'))\cdot \\
&= N^{-3d}\mathcal{E}(E)
\end{aligned}$$

This relation between the fourth moment of the Fourier transform and the additive energy of a set allows for sharper estimates on $\|E\|_{L^4}$ necessary to prove their restriction estimate.

2 Uncertainty Principles for Invertible Linear Maps

2.1 Deriving the uncertainty principle

Let V be the complex vector space of functions $f : \mathbb{Z}_N^d \to \mathbb{C}$. Let $A = A(m, y)$ be an N^d by N^d matrix with complex entries. We will regard the entries in the matrix as being indexed by $\mathbb{Z}_N^d \times \mathbb{Z}_N^d$. The matrix A induces a linear transformation $T_A : V \to V$ by

$$T_A f(m) = \sum_{y \in \mathbb{Z}_N^d} A(m, y) f(y).$$

In the case when $A(y, m) = \chi(-m \cdot y)$, we have that

$$T_A f(m) = \sum_{y \in \mathbb{Z}_N^d} \chi(-m \cdot y) f(y) = N^d \hat{f}(m).$$

Our immediate goal is to derive an uncertainty principle for the transformation T_A akin to the one that exists for the Fourier transfrom. To do this, there are essentially two ingredients: an inversion formula, and an inequality of the form

$$\|T_A f\|_{L^2}^2 \leq C \|f\|_{L^2}^2,$$

where $C > 0$ is a constant depending on N and d (i.e. on the size of the space). In the case when the transform Af is induced by an orthogonal matrix T_A, this latter inequality is actually an equality. The Plancherel identity for the Fourier transform is an example of this phenomenon.

In order for the transform to be invertible, it is enough to impose that the matrix A be invertible. In this case, the inverse is given by

$$T_A^{-1} f(x) = \sum_{m \in \mathbb{Z}_N^d} A^{-1}(x, m) f(m),$$

as the definition of T_A implies

$$T_A^{-1} T_A f(x) = \sum_{m \in \mathbb{Z}_N^d} \sum_{y \in \mathbb{Z}_N^d} A^{-1}(x, m) A(m, y) f(y).$$

But

$$\sum_{m \in \mathbb{Z}_N^d} A^{-1}(x, m) A(m, y) = \begin{cases} 0 \text{ if } x \neq y \\ 1 \text{ if } x = y \end{cases},$$

so

$$\sum_{m \in \mathbb{Z}_N^d} \sum_{y \in \mathbb{Z}_N^d} A^{-1}(x, m) A(m, y) f(y) = f(x).$$

Suppose that f is supported on $E \neq \emptyset$ and $T_A f$ is supported on a set S. If we follow the same steps as in the case of the Fourier transform here, we can estimate $|f(x)|^2$ in the following way:

$$\begin{aligned} |f(x)|^2 &= \left| \sum_{m \in S} A^{-1}(x,m) T_A f(m) \right|^2 \\ &\leq \left(\sum_{m \in S} |A^{-1}(x,m)|^2 \right) \left(\sum_{m \in S} |T_A f(m)|^2 \right) \\ &\leq \sum_{m \in S} |A^{-1}(x,m)|^2 \cdot \|T_A\|_2^2 \cdot \|f\|_{L^2(E)}^2, \end{aligned}$$

where

$$\|T_A\|_2 = \sup_{\|f\|_{L^2}=1} \|T_A f\|_{L^2}$$

is the operator norm of T_A. Again summing over E and cancelling the $\|f\|_{L^2(E)}^2$ factors, we see that

$$\begin{aligned} 1 &\leq |E| \cdot \|T_A\|_2^2 \sum_{m \in S} |A^{-1}(x,m)|^2 \\ &\leq |E| \cdot |S| \cdot \|T_A\|_2^2 \cdot \|A^{-1}\|_\infty^2. \end{aligned}$$

If we want to recover the classical uncertainty principle, it is enough to have that

$$\|T_A\|_2^2 \cdot \|A^{-1}\|_\infty^2 \leq N^{-d}. \tag{1}$$

To compute $\|T_A\|_2$, we can compute $\|A\|_2$. This is because if we identify V with $\mathbb{C}^{N^d}$ by identifying a function $f \in V$ with the N^d-tuple $(f(x_1), ..., f(x_{N^d}))$, T_A is simply matrix-vector multiplication. We have the following way to compute $\|A\|_2$:

Proposition 2.1. *Let A be a matrix with complex entries. Then $\|A\|_2$ equals the square root of the largest eigenvalue of A^*A, where A^* is the conjugate transpose of A.*

Proof. We will prove this using the singular value decomposition of a matrix (cf. ch. 12 of [2]). There exist unitary matrices U and V such that

$$A = USV^T,$$

with S being a diagonal matrix whose entries along the diagonal are the square roots of eigenvalues of A^*A, sorted in decreasing order of absolute value. However, for a unitary matrix T, we have that

$$\langle Tx, Tx \rangle = \langle x, T^*Tx \rangle = \langle x, x \rangle,$$

so T is an isometry. This means that

$$\|Ax\| = \|Sx\|,$$

and so $\|A\|_2 = \|S\|_2$. But because of the structure of S, if s_i are the nonzero entries entries in the diagonal of S, and $\|x\| = 1$, then

$$\|Sx\|^2 = \sum_i |s_i x_i|^2 \leq \sum_i |s|^2 |x_i|^2 = |s|^2 \cdot \|x\|^2 = |s|^2,$$

where $s = s_1$ is the largest of the s_i. However, taking $y = (1, 0, ..., 0)$, we see that

$$\|Sy\| = |s|,$$

so this upper bound is achieved. This means that

$$\|A\|_2 = \|S\|_2 = |s|,$$

as claimed.

□

Proposition 2.2. *Let $A = A(i, j)$ be an invertible $n \times n$ matrix. Then*

$$\frac{1}{\sqrt{n}} \leq \|A\|_2 \cdot \|A\|_\infty.$$

Proof. Our strategy is two write

$$1 = \det I_n = |\det A| \cdot |\det A^{-1}|,$$

and then estimate each determinant on the right hand side separately. A result of Hadamard (cf. Appendix A for a proof) says that

$$|\det A^{-1}| \leq \|A^{-1}\|_\infty n^{n/2}.$$

For estimating $|\det A|$, we first observe that

$$\begin{aligned} |\det A| &= |\det(A^* A)|^{1/2} \\ &= \left| \prod_{i=1}^n \lambda_i \right|^{1/2} \\ &\leq \max_i |\lambda_i|^{n/2}, \end{aligned}$$

where $\{\lambda_i\}_{i=1}^n$ are the eigenvalues of $A^* A$ counted with multiplicity. By Proposition 2.1, this last quantity is equal to $\|A\|_2^n$. Combining these estimates yields that

$$1 \leq \|A\|_2^n \cdot \|A^{-1}\|_\infty n^{n/2},$$

which after dividing by $n^{n/2}$ and raising both sides to the power $1/n$ implies that

$$\frac{1}{\sqrt{n}} \leq \|A\|_2 \cdot \|A^{-1}\|_\infty,$$

as claimed.

□

Proposition 2.2 tells us that the only way a linear map $T_A : V \to V$ can satsify the classical uncertainty principle is when we have the equality

$$\|T_A\|_2^2 \cdot \|A^{-1}\|_\infty^2 = N^{-d},$$

i.e. it is impossible for inequality (1) to be strict. This means that in general, it is impossible for a linear transfromation to satisfy the classical uncertainty principle with a stronger constant than the Fourier transform. Propositions 2.1 and 2.2 let us characterize unitary matrices that satisfy the classical uncertainty principle, which will allow us to more systematically find new examples of such linear maps.

Theorem 2.1. *Let A be a unitary $N^d \times N^d$ matrix. Then A satisfies*

$$\|A\|_2^2 \cdot \|A^{-1}\|_\infty^2 = N^{-d}$$

(i.e. the operator T_A satisfies the classical uncertainty principle) if and only if every entry in A has absolute value $N^{-d/2}$.

Proof. First we observe that since A is unitary, $A^*A = I_{N^d}$. Since the identity matrix has only 1 as an eigenvalue, Proposition 2.1 implies $\|A\|_2 = 1$. If every entry in the matrix A has absolute value $N^{-d/2}$, then immediately we have that

$$N^{-d} = \|A\|_\infty^2 = \|A^*\|_\infty^2 = \|A^{-1}\|_\infty^2,$$

so we have that

$$\|A\|_2^2 \cdot \|A^{-1}\|_\infty^2 \leq N^{-d}.$$

Conversely, suppose that

$$\|A\|_2^2 \cdot \|A^{-1}\|_\infty^2 \leq N^{-d}.$$

Since A is unitary, $A^* = A^{-1}$, but entries of A^* have the same absolute values as entries in A, so

$$\|A\|_\infty^2 \leq N^{-d}.$$

If $(a_1, ..., a_{N^d})$ is a row in A, then the unitary property implies

$$|a| = |a_1|^2 + ... + |a_{N^d}|^2 = 1.$$

Suppose that $|a_i| < N^{-d}$ for some i. Then since every entry in A has absolute value at most N^{-d}, we have that

$$1 = |a_1|^2 + ... + |a_i|^2 + ... + |a_{N^d}|^2 < N^{-d} \cdot N^d = 1,$$

a contradiction. Thus since our choice of entry was arbitrary, we must have that every entry in A has absolute value equal to N^{-d}.

□

Note that when we proved the reverse direction, we did in fact obtain equality in the statement $\|A\|_2^2 \cdot \|A^{-1}\|_\infty^2 \leq N^{-d}$. This also means that the unitary matrices satisfying the uncertainty principle all behave somewhat like the Fourier transform, in that the entries in its matrix representation are uniformly distributed in absolute value.

In the next section, we will show that there exist linear transformations other than the Fourier transform that satisfy the classical uncertainty principle. We will also show that in some cases, these transfromations are similar enough to the Fourier transfrom that we can deduce the stronger restriction estimates for them.

2.2 The Hadamard transform

In the case when $d = 1$ and $N = 2^m$, there is a transform with enough similarity to the Fourier transform that we can apply the known (p, q) restriction bound.

Definition 2.1. *The Hadamard transform H_m is a $2^m \times 2^m$ matrix defined recursively, with H_0 the identity map and*

$$H_m = \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}.$$

Additionally, we can see that

$$H_0 H_0^T = I_1$$

and

$$H_1 H_1^T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix},$$

while

$$\begin{aligned} H_m H_m^T &= \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}^2 \\ &= \begin{pmatrix} H_{m-1}^2 + H_{m-1}^2 & 0 \\ 0 & H_{m-1}^2 + H_{m-1}^2 \end{pmatrix} \\ &= \begin{pmatrix} 2H_{m-1}H_{m-1}^T & 0 \\ 0 & 2H_{m-1}H_{m-1}^T \end{pmatrix}. \end{aligned}$$

The definition of H_m immediately implies $H_m = H_m^T$, from which the last equality follows. Inducting on m then implies that $H_{m-1}H_{m-1}^T = 2^m I_{2^m}$. The only eigenvalues of $2^m I_{2^m}$ is just 2^m, and so Proposition 2.1 implies

$$\|H_m\|_2 = 2^{m/2}.$$

We then claim the following:

Proposition 2.3. *The Hadamard transform H_m satisfies*

$$\|H_m\|_2^2 \cdot \|H_m^{-1}\|^2 = 2^{-m}.$$

As a consequence, the Hadamard transform obeys the classical uncertainty principle.

Proof. Our previous computation showed that H_m is invertible, so H_m^{-1} is well defined. In fact,

$$H_m^{-1} = 2^{-m} H_m^T.$$

Since H_m and consequently H_m^T only have entries ± 1, we immediately have that

$$\|H_m^{-1}\|_\infty^2 = 2^{-2m}.$$

Combining these results gives the claimed identity.

□

2.3 Generalized Hadamard transform

The Hadamard transfrom poses a somewhat strict restriction in the context of signal processing as it only works for signals of dyadic length. However, we can recast the definition of the transform via the more general Kronecker product. This, along with a simple way to construct matrices analogous to H_0 of varying lengths, will allow us to construct generalized Hadamard matrices of arbitrary dimensions. These transforms bear some resemblance to their domain's respective Fourier tranfsorms, though in general they are distinct.

Definition 2.2. *Let $A = A(i,j)$ and B be complex matrices of dimension $m \times n$ and $p \times q$, respectively. Then the Kronecker product $A \otimes B$ is the $mp \times nq$ matrix given in block form by*

$$A \otimes B = \begin{pmatrix} A(1,1)B & \cdots & A(1,n)B \\ \vdots & \ddots & \vdots \\ A(m,1)B & \cdots & A(m,n)B \end{pmatrix}.$$

Taking $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$ demonstrates that $A \otimes B \neq B \otimes A$ in general, as

$$(A \otimes B)(1,2) = -1 \neq 1 = (B \otimes A)(1,2).$$

We can also use this definition to write the recursive definition of the Hadamard transform more compactly:

$$H_m = H_1 \otimes H_{m-1}.$$

This is the viewpoint we will take to generalize the Hadamard transform. Given a positive integer n which can be factored into primes as $n = p_1 \cdot \ldots \cdot p_k$, we will construct a $p_i \times p_i$ orthogonal matrix for each i, and then take successive Kronecker products to obtain an appropriate $n \times n$ matrix. We begin by recording some properties of matrices associated with the Fourier transfrom.

Proposition 2.4. *Let F_N be an $N \times N$ matrix whose $jkth$ entry is given by*

$$F_N(j,k) = \frac{\chi(jk)}{\sqrt{N}}.$$

Then F_N is unitary.

Proof. First we observe that since $jk = kj$, $F_N(j,k) = F_N(k,j)$, so F_N is a symmetric matrix. The dot product of the jth column and kth column is

$$\sum_{l=1}^{N} F_N(l,j)\overline{F_N(l,k)} = \frac{1}{N}\sum_{l=1}^{N} \chi(l(j-k)) = \delta_{jk},$$

where δ_{jk} is the Kronecker delta. The last equality is an immediate consequence of Lemma 1.1.

□

F_N is just the matrix associated with the Fourier transform, having been rescaled so that it is unitary (instead of just having mutually orthogonal columns). These matrices will be our building blocks to construct a wide array of transformations obeying the classical uncertainty principle. In order to do this, we first need some information about how these matrices will combine via the Kronecker product.

Proposition 2.5. *Let U and V be unitary $n \times n$ and $m \times m$ matrices, respectively. Then $U \otimes V$ is a unitary $nm \times nm$ matrix.*

Proof. The lth column in $U \otimes V$ is given by

$$(U \otimes V)_l = (U(1,l)V_l^T, U(2,l)V_l^T, ..., U(n,l)V_l^T)^T,$$

where V_l is the lth column of V. Then

$$\begin{aligned}\langle (U \otimes V)_j, (U \otimes V)_k \rangle &= \sum_{i=1}^{n} U(i,j)\overline{U(i,k)}\langle V_j, V_k \rangle \\ &= \langle U_j, U_k \rangle \langle V_j, V_k \rangle \\ &= \delta_{jk}.\end{aligned}$$

Thus the columns of $U \otimes V$ form an orthonormal set, and so $U \otimes V$ is unitary.
□

Note by definition every entry in the Kronecker product $F_N \otimes F_M$ of two Fourier matrices is of the form $\frac{\chi(x)}{\sqrt{NM}}$ for some x. Proposition 2.4 allows us to conclude this matrix is also unitary. This means we can Theorem 2.1 to conclude that the linear transformation associated to $F_N \otimes F_M$ satisfies the classical uncertainty principle.

In the case when the length of a message is of the form N^d for some d, there is a much closer link between $\otimes_{i=1}^{d} F_N$ and the Fourier transform on $\mathbb{Z}_N^d$. It is worth observing that these two transformations are distinct for $d > 1$; the characters appearing in entries of $\otimes_{i=1}^{d} F_N$ are of the form

$$\exp(-2\pi i(k_1 + k_2 + ... + k_d)/N),$$

while those in F_{N^d} are of the form

$$\exp(-2\pi ik/N^d)$$

(where $1 \leq k \leq N^d$ and $1 \leq k_i \leq N$), meaning that when $d > 1$, the entries in each matrix will in general be distinct. However there is a connection between the $\mathbb{Z}_N^d$ Fourier transform and this Hadamard transform.

We can make the connection between generalized Hadamard transfroms for integer powers and the Fourier transform explicit. Let $f : \mathbb{Z}_{N^d} \to \mathbb{C}$. If we view the input x of $f(x)$ as an integer between 0 and $N^d - 1$, then it has a unique base N representation consisting of at most d digits. This representation is essentially an element of $\mathbb{Z}_N^d$, allowing us to regard f as a function from $\mathbb{Z}_N^d$ into $\mathbb{C}$ through this correspondance.

In view of this correspondence, we have the following result:

Theorem 2.2. *Let $f : \mathbb{Z}_{N^d} \to \mathbb{C}$ be a function, and let $H_{N,d} = N^{-d/2} \otimes_{i=1}^{d} F_N$. If we interpret $x \in \mathbb{Z}_N^d$ as an element in $\mathbb{Z}_N^d$ according to the above correspondence, then*

$$T_{H_{N,d}} f(m) = \hat{f}(m),$$

where $\hat{f}$ is the Fourier transfrom when viewing f as a function on $\mathbb{Z}_N^d$ under the same correspondence (associating 0 and N with each other).

Proof. By definition,

$$T_H f(m) = \sum_{x \in \mathbb{Z}_{N^d}} H_{N,d}(m, x) f(x).$$

By the recursive definition of H, we can locate an entry in the matrix by which character $N^{-1/2} \exp(-2\pi i k_j / N)$ was multiplied at the jth step in the construction (for $1 \leq j \leq d$). By the definition of F_N, the number $k_j = m_j l_j$ where m_j and l_j are between 1 and N. Here m_j represents the row position in $\otimes_{i=1}^{j} F_N$ and l_j represents the column position (when viewed as the $N \times N$ block matrix $N^{-j/2} F_N \otimes \left(\otimes_{i=1}^{j-1} F_N \right)$). This allows us to write

$$H_{N,d}(m, x) = N^{-d/2} \exp(-2\pi i (m_1 l_1 + ... + m_d l_d)).$$

It is enough now to show that under the previously described correspondance, $m \mapsto (m_1, ..., m_d)$. But this is immediate from the construction, as m_d tells us which of the N^{d-1} long sections (of which there are N) m lies in, while within this section m_{d-1} tells us the location of m among the N^{d-2} long sections within this first section, and so on, until we reach m_1.

□

For the sake of clarity we will look in detail at an example of this phenomenon. In particular, we will compute explictly the equivalence between $T_{H_{3,2}}$ and the $\mathbb{Z}_3^2$ Fourier transfrom. Let $\omega = e^{2\pi i/3}$ be a primitive cube root or unity. In terms of ω, we have that

$$\frac{1}{\sqrt{3}} F_3 = \frac{1}{3} \begin{pmatrix} \omega & \omega^2 & 1 \\ \omega^2 & \omega & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Using this, we compute $H_{2,3}$:

$$H_3 = \frac{1}{\sqrt{3}}F_3 \otimes \frac{1}{\sqrt{3}}F_3$$
$$= \frac{1}{9}\begin{pmatrix} \omega\begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \omega^2\begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} \\ \omega^2\begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \omega\begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} \\ \begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} & \begin{pmatrix}\omega & \omega^2 & 1\\ \omega^2 & \omega & 1\\ 1 & 1 & 1\end{pmatrix} \end{pmatrix}.$$

Then we can view an index for either a row or a column by a tuple in $\mathbb{Z}_3^2$. For example, if we wanted to locate the (8,5) entry in the matrix, we can see that the 8th row is really the second row in the third row of blocks, so this corresponds to the (1,2) row by our correspondence. Similarly, the 5th column is really the $(1,1)$ column. These strings, when interpreted as base-3 numbers, equal 7 and 4, respectively. Because our labelling of the rows and columns starts at 0 and ends at N^{d-1} (8 in this case), this is consistent with what we expect from the correspondance.

This association means that any uncertainty principles for the Fourier transfrom will also hold for generalized Hadamard matrices on $\mathbb{Z}_{N^d}$. In particular, the stronger undertainty principles that follow from restriction estimates will hold for these transformations. We will now explore this association explicitly.

Let $I : \mathbb{Z}_{N^d} \to \mathbb{Z}_N^d$ represent the bijection described above, that is, to compute $I(x)$, we find the unique integer representative x' of x such that $0 \leq x' \leq N^d - 1$. Then $I(x)$ is defined to be the $d-$tuple of the digits of x' in its base$-N$ representation. This inverse of this map simply undoes this operation, i.e.

$$I^{-1}(a_1, ..., a_d) = a_1 + a_2N + ... + a_dN^{d-1}.$$

Let $f : \mathbb{Z}_{N^d} \to \mathbb{C}$ be a function. We have already shown that when interpreting the input of f as $I(x)$ instead of x, we have that $H_{N,d}f$ is essentially the $\mathbb{Z}_N^d$ Fourier transform. More precicely,

$$T_{H_{N,d}}f(m) = \mathcal{F}(f \circ I^{-1})(I(m)),$$

where $\mathcal{F}$ is the $\mathbb{Z}_N^d$ Fourier transform.

The only other assumptions for their $(4/3, 2)$ restiction estimate are that the set S is not too big ($|S| \leq N^{d/2}$) and that S is a Salem set. Our association map I is a bijection, so we can impose the same size restriction on a set $S \subset \mathbb{Z}_{N^d}$ without issue. In order for the restriction estimate to hold, then, we must have that for our prospective set S, $I(S)$ is a Salem set. The following proposition addresses this problem.

Proposition 2.6. *Let $S \subset \mathbb{Z}_{N^d}$. Then*

$$\mathcal{E}(I(S)) \leq \mathcal{E}(S).$$

Proof. Let $x, y, x', y' \in I(S)$ with $x = (x_1, ..., x_d)$, identifying x_i with an integer in $[0, N-1]$. Further suppose that $x + y = x' + y'$. Then

$$I^{-1}(x) + I^{-1}(y) = \sum_{i=1}^{d} (x_i + y_i) N^{i-1}$$

and

$$I^{-1}(x') + I^{-1}(y') = \sum_{i=1}^{d} (x'_i + y'_i) N^{i-1}.$$

But $x + y = x' + y'$ implies that $x_i + y_i = x'_i + y'_i$, and so

$$I^{-1}(x) + I^{-1}(y) = I^{-1}(x') + I^{-1}(y').$$

Hence if (x, y, x', y') is a quadruple counted in $\mathcal{E}(I(S))$, the quadruple

$$(I^{-1}(x), I^{-1}(y), I^{-1}(x'), I^{-1}(y'))$$

is counted in $\mathcal{E}(S)$, from which the desired inequality is immediate.

□

Note that the converse of what we proved in Proposition 2.6 does not hold in general. Take $N = 5$ and $d = 2$, and let $x = y = (3, 0)$, $x' = (1, 1)$, and $y' = (0, 0)$. Then $x + y \neq x' + y'$, yet

$$I^{-1}(x) + I^{-1}(y) = 6$$

and

$$I^{-1}(x') + I^{-1}(y') = 0 + 1 + 5 = 6.$$

This means that the inequality can in fact be strict. However, this is enough to prove the following:

Theorem 2.3. *Let $S \subset \mathbb{Z}_{N^d}$ be a set such that $|S| \leq N^{d/2}$ and $\mathcal{E}(S) \leq c|S|^2$ for some positive absolute constant c. Then S satisfies the $(4/3, 2)$ restriction bound with $H_{N,d}$ in place of the Fourier transfrom.*

Proof. Let $f : \mathbb{Z}_{N^d} \to \mathbb{C}$ be a function. Then

$$\left(\frac{1}{|S|} \sum_{m \in S} |T_{H_{N,d}} f(m)|^2 \right)^{1/2} = \left(\frac{1}{|S|} \sum_{m \in I(S)} |\mathcal{F}(f \circ I^{-1})(m)|^2 \right)^{1/2} = (*)$$

by Theorem 2.2 and the fact that $|S| = |I(S)|$. Since we are assuming S is Salem, the previous proposition implies that $I(S)$ is Salem, and so applying

the $(4/3, 2)$ restriction bound for the Fourier transfrom to the right hand side implies that

$$(*) \leq C_{4/3,2} \cdot N^{-d} \left(\sum_{x \in \mathbb{Z}_N^d} |f(x)|^{4/3} \right)^{4/3},$$

from which the restriction bound for $T_{H_{N,d}}$ is obtained.

□

3 The Radon transform

We have seen that Fourier transfrom is essentially a weighted average of a given function. In the stronger uncertainty principle proven by Iosevich and Mayeli, a necessary assumption is that the set a function is supported on is not too large. This case effectively restricts the Fourier transform to be a weighted average over a subset of the function's domain, rather than over the entire domain. In light of this fact, we will investigate uncertainty principles for the discrete Radon transform.

Definition 3.1. *Let $f : \mathbb{Z}_p^2 \to \mathbb{C}$ be a function and p a prime. Then the discrete Radon transfrom of f, Rf, is defined as*

$$Rf(m,t) = \frac{1}{p} \sum_{m \cdot y = t} f(y).$$

The input $t \in \mathbb{Z}_p$, while $m \in V$, where V is the quotient of $\mathbb{Z}_p^2$ under the equivalence relation

$$a \sim b \iff a = \lambda b$$

for some $\lambda \neq 0$.

The reason for the involved definition of the m-coordinate of Rf is to avoid redundancy, as the line $\ell_{m,t} := \{y \in \mathbb{Z}_p^2 : m \cdot y = t\}$ is the same for any l in the same equivalence class as m. Throughout this section we will conflate m and the equivalence class of m. This transform arises naturally in x-ray imaging. If f represents (an approximation of) the density of a cross section of an object, then x-rays, which eminate in straight lines, can be used to compute values of Rf along particular lines. The Radon transform is invertible, which we develop below.

Proposition 3.1. *Let $\mathcal{F}_2 Rf$ denote the partial Fourier transform of Rf in the second coordinate. Then*

$$f(x) = \sum_{m \in \mathbb{Z}_p^2} \mathcal{F}_2 Rf(m,r) \chi(rx \cdot m)$$

for any $r \neq 0$.

Proof. With the orthogonality condition from Lemma 1.1, we can write Rf in the following way:

$$\begin{aligned} Rf(m,t) &= p^{-1} \sum_{m \cdot y = t} f(y) \\ &= p^{-2} \sum_{s \in \mathbb{Z}_p} \sum_{y \in \mathbb{Z}_p^2} \chi(s(m \cdot y - t)) f(y). \end{aligned}$$

This implies that

$$\begin{aligned} \mathcal{F}_2 Rf(m,r) &= p^{-1} \sum_t Rf(m,t) \chi(-rt) \\ &= p^{-3} \sum_{t,s,y} \chi(-s(m \cdot y - t)) \chi(-rt) f(y). \end{aligned}$$

This can be combined with the previous equality to obtain that

$$\begin{aligned} \mathcal{F}_2 Rf(m,r) &= p^{-3} \sum_{t,s,y} \chi(t(s-r)) \chi(-sm \cdot y) f(y) \\ &= p^{-2} \sum_y \chi(-rm \cdot y) f(y) \\ &= \hat{f}(rm), \end{aligned}$$

where the second to last equality comes from interpreting the sum over t as a Gauss sum, which equals zero unless $s = r$, where it equals p.

By Fourier inversion, we have for $r \neq 0$ that

$$\begin{aligned} f(x) &= \sum_{m \in M} \hat{f}(m) \chi(x \cdot m) \\ &= \sum_m \hat{f}(rm) \chi(rx \cdot m), \end{aligned}$$

where the second equality holds because if $r \neq 0$ then the assignment $m \mapsto rm$ is a bijection. Note that this is enough to prove the claim, since we may substitute $\mathcal{F}_2 Rf(m,r)$ for $\hat{f}(rm)$ in our modified Fourier inversion formula:

$$\begin{aligned} f(x) &= \sum_{m \in \mathbb{Z}_p^2} \hat{f}(rm) \chi(rx \cdot m) \\ &= \sum_{m \in \mathbb{Z}_p^2} \mathcal{F}_2 Rf(m,r) \chi(rx \cdot m) \end{aligned}$$

□

Like before, our goal is to leverage the inversion formula to derive an uncertainty principle for Rf and f to find situations in which f can be reconstructed from incomplete Rf data.

To do this, we will assume $\mathcal{F}_2 Rf(\cdot, r)$ is supported on a set $M_r \subset \mathbb{Z}_p^2$ (here we are regarding $M_r \subset \mathbb{Z}_p^2$ instead of as a subset of V so that the first coordinate of Rf is compatible with our discrete Fourier transform). We can estimate $|f(x)|^2$ with Cauchy-Schwarz:

$$\begin{aligned}
|f(x)|^2 &= \left| \sum_{m \in M_r} \mathcal{F}_2 Rf(m,r) \chi(rx \cdot m) \right|^2 \\
&\leq \left| \sum_{m \in M_r} 1 \right| \cdot \sum_{m \in M_r} |\mathcal{F}_2 Rf(m,r) \chi(rx \cdot m)|^2 \\
&= |M_r| \cdot \sum_{m \in M_r} |\mathcal{F}_2 Rf(m,r) \chi(rx \cdot m)|^2.
\end{aligned}$$

In our proof of the inversion formula for the Radon transform, we showed that $\mathcal{F}_2 Rf(m,r) = \hat{f}(rm)$. We can use this fact to see that

$$\begin{aligned}
\sum_{m \in M_r} |\mathcal{F}_2 Rf(m,r) \chi(rx \cdot m)|^2 &= \sum_{m \in V} |\hat{f}(rm)|^2 \\
&= \sum_{m \in \mathbb{Z}_p^2} |\hat{f}(m)|^2 \\
&= p^{-2} \sum_{y} |f(y)|^2,
\end{aligned}$$

where the third equality follows from Plancherel's identity. Combining this with out estimate for $|f(x)|^2$ yields that

$$|f(x)|^2 \leq |M_r| \cdot p^{-2} \sum_{y \in E} |f(y)|^2,$$

where E is the support of f. Summing over all $x \in E$ and cancelling $\sum_{y \in E} |f(y)|^2$ from each side (provided f is not the zero function) then implies

$$p^2 \leq |M_r| \cdot |E|.$$

We have just proven the following result:

Theorem 3.1. *(Uncertainty Principle for the Radon Transform). Let $f : \mathbb{Z}_p^2 \to \mathbb{C}$ be a function that is not identically zero, and let $r \neq 0$. If $supp(f) \subset E$ and $supp(\mathcal{F}_2 Rf(\cdot, r)) \subset M_r$, then*

$$p^2 \leq |M_r| \cdot |E|.$$

Because of the similarity between $\mathcal{F}_2 Rf$ and the discrete Fourier transform, this result is not terribly surprising. We can view $\mathcal{F}_2 Rf(\cdot, r)$ as differing from the discrete Fourier transform by a linear change in variables (we showed it equals the Fourier transform precomposed with the map $m \mapsto rm$), and so this can be viewed as an instance of our uncertainty principle for general linear transformations.

4 Future Work

4.1 The non-unitary case

We saw earlier that for a function F_A induced by an $N \times N$ matrix to satisfy the classical uncertainty principle, it must satisfy the identity

$$\|A^{-1}\|_\infty^2 \cdot \|A\|_2^2 = \frac{1}{n}. \tag{2}$$

In section 2, we dealt with the case when the matrix A is unitary. It would likely be worthwhile to investigate what happens when A is not unitary. Note that the left hand side of (2) is invariant when scaling A by a nonzero constant. Because all of our linear maps are on finite dimensional complex vector spaces, they are continuous, so $\|A\|_\infty$ is bounded. This means that if we let $c = \frac{1}{\|A\|_2}$, then the matrix cA satisfies

$$\|cA\|_2 = 1.$$

This means that without loss of generality, we could have assumed from the beginning that $\|A\|_2 = 1$.

4.2 Restriction estimates for the Radon transform

Our analyis of the Radon transfrom relied on using the orthogonality property from Lemma 1.1 to encode algebraically the fact that our transfrom restricted the sum to a subset of the ambient space. It would be worth investigating how this transfrom behaves when the sum defining it has weights introduced, or when we modify the set on which we are taking averages.

An alternative way to think about the parameters in the Radon transfrom is that they encode basic rigid motions applied to a fixed set. Instead of a line, if our initial set was one that satisfies the conditions of the restriction estimates of Iosevich and Mayeli, there could be interesting behavior present for a transformation built with these facts in mind.

4.3 A conjecture of Hadamard

It is known that Hadamard matrices must have dimension 1, 2, or a multiple of 4. It is however unknown whether there exists a Hadamard matrix with the corresponding size for every multiple of 4.

Our generalized Hadamard matrix construction allows us to build matrices of size a multiple of 4 having orthogonal rows and entries with constant absolute value 1. If there was a Hadamard matrix H_k of size $4k$ for every k, then we could find a unitary matrix U such that UH_k equals our generalized Hadamard matrix of the same size. One way to do this is to let the columns of our matrix (call it A) form a basis, do the same for the columns of H_k, and let U be the matrix representation of the map sending the latter basis to the former. The resulting transformation is an isometry, and hence unitary.

Conversely, if there is such a matrix, then $U^{-1}A$ is a Hadamard matrix and the conjecture is resolved. Thus Hadamard's conjecture is equivalent to finding a unitary matrix that multiplies onto our generalized Hadamard matrix such that the resulting matrix has entries only ± 1.

5 Acknowledgements

I would first like to thank my advisor, Alex Iosevich, for his support and guidance in this project. I would also like to thank Mira Chaskes, William Hagerstrom, and Nathan Skerrett for their support and input into the ideas appearing in this paper. Lastly, I would like to thank the other members of my committee, Professor Geba and Professor Pakianathan, for their academic support throughout my undergraduate career.

A Hadamard Determinant Estimate

In the proof of Proposition 2.2, we make use of the following estimate for an $n \times n$ matrix M. The following proof is from pp. 418 of [6].

Theorem A.1. *Let a_i be the ith column of A. Then*

$$|\det A| \leq \prod_{i=1}^{n} \|a_i\|.$$

Proof. First we observe that the result is immediate if $\det A = 0$. Thus we can assume that the a_i are linearly independent, in particular each a_i is nonzero. Let B be the matrix obtained by normalizing each columm in A, and let b_i be the ith column of B. Then

$$|\det A| = |\det B| \cdot \prod_{i=1}^{n} \|a_i\|,$$

and so it suffices to show that for a matrix B whose columns each have norm 1,

$$|\det B| \leq 1.$$

Consider the matrix $C = B^*B$, and let $\{\lambda_i\}_{i=1}^n$ be the eigenvalues of C (counted with multiplicity). We have that

$$C_{ii} = \|b_i\| = 1,$$

so the trace of C is n. Then, applying the AM-GM inequality, we have that

$$\det C = \prod_{i=1}^{n} \lambda_i \leq \left(\frac{1}{n} \sum_{i=1}^{n} \lambda_i \right)^n = \left(\frac{1}{n} tr(C) \right) = 1^n = 1.$$

Hence $|\det B| = |\det C|^{1/2} \leq 1$, and by our previous comments we are done. □

In the proof of Proposition 2.2, we use the following corollary of this inequality:

Corollary A.1. *For an $n \times n$ matrix A,*

$$|\det A| \leq n^{n/2} \|A\|_\infty.$$

Proof. If a_i is the ith row in A, then we have the trivial estimate

$$\|a_i\| = \left(\sum_{j=1}^{n} |a_{ji}|^2 \right)^{1/2} \leq \sqrt{n} \|A\|_\infty.$$

In sight of the previous result, we have that

$$|\det A| \leq \prod_{i=1}^{n} \|a_i\| \leq n^{n/2} \|A\|_\infty,$$

as desired.

□

References

[1] Banerjee, Sudipto; Roy, Anindya. (2014), *Linear Algebra and Matrix Analysis for Statistics*. Texts in Statistical Science (1st ed.), Chapman and Hall/CRC.

[2] Hadamard, Jacques. (1893), *Résolution d'une question relative aux déterminants*. Bulletin des Sciences Mathématiques, 17, pp. 240–246.

[3] Horn, Roger; Johnson, Charles. *Matrix Analysis* (2nd ed.), Cambridge University Press, 1994.

[4] Hoffman, Kenneth; Kunze, Ray. (1971), *Linear Algebra*. Pretence-Hall International, Englewood Cliffs, New Jersey.

[5] Iosevich, Alex; Mayeli, Azita. (2023), *Uncertainty Principles on Finite Abelian Groups, Restriction Theory, and Applications to Sparse Signal Recovery*. Digital preprint, https://arxiv.org/abs/2311.04331.

[6] Mirsky, Leon. (1963) *An Introduction to Linear Algebra*. Oxford University Press, London.