# Fourier Transform Algorithms and Signal Processing

Jiayi Hu, Yi Jin, Taylor Tan, Lejun Xu

December 11, 2024

**Abstract**

A signal of length $N$ given by its values $(x_n)_{n=0}^{N-1}$ can be decomposed through the Discrete Fourier transform into its frequencies $(\omega_n)_{n=0}^{N-1}$. The uncertainty principle guarantees any nonzero signal can not be simultaneously well localized in both time and frequency and we demonstrate the application of this principle to recovery of binary signals assuming only quantitative band-frequency conditions.

## 1 Discrete Fourier Transform

The structure of this exposition is as follows: This first section recalls basic properties of the Fourier transform in the finite setting over general dimensions $d \geqslant 1$, however we will restrict the discussion to dimension $d = 1$ for later sections with the added remark that **most** arguments will generalize to higher dimensions. The second section describes the fast Fourier transform algorithm to calculate the Fourier transform of a length $N$ sequence in $O(N \log N)$ time. In the final two sections, we introduce an basic uncertainty principle and describe its application to signal processing and recovery.

Let $\mathbb{Z}_N$ denote the cyclic group modulo $N$. For a given signal $f : \mathbb{Z}_N^d \to \mathbb{C}$ of length N, we can define the discrete Fourier transform of our signal $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ with values

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

where $\chi(\cdot) = e^{\frac{2\pi i \cdot}{N}}$ denotes the standard characters on the dual group $Hom(\mathbb{Z}_N^d, S^1) \cong \mathbb{Z}_N^d$, and $x \cdot m$ denotes the usual scalar product on $\mathbb{Z}_N^d$. We call the values $\hat{f}(m)$ the Fourier coefficients of $f$. We are able to recover our signal $f$ given its Fourier coefficients through Fourier inversion:

**Proposition** (Fourier Inversion)**.** *For any signal* $f : Z_N^d \to \mathbb{C}$*,*

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

With the chosen normalization of Fourier transform, Plancharel's identity takes the form

**Theorem** (Plancharel)**.**

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

We outline another perspective that will be useful in later sections. For $d = 1$, we can view a signal as the length $N$ sequence generated by its values $(x_n)_{n=0}^{N-1}$ and likewise for its Fourier transform: $(\omega_n)_{n=0}^{N-1}$ where $x_n = f(n)$ and $\omega(n) = \hat{f}(n)$. Then Plancharel (4) takes the form

$$\sum_{n=0}^{N-1} |x_n|^2 = N \sum_{n=0}^{N-1} |\omega_n|^2.$$

In later sections, we will interchangeably use $f, \hat{f}$ or $(x_n), (\omega_n)$ to refer to signals and their Fourier transforms respectively.

---

# 2 Fast Fourier Transform Algorithms

The exposition in this section follows from [3]. Let $N$ be a positive integer. A complex number $z$ is an $N^{\text{th}}$ root of unity if $z^N = 1$. The set of $N^{\text{th}}$ roots of unity is precisely

$$\left\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, \dots, e^{2\pi i(N-1)/N}\right\}$$

and can be identified with the additive group $\mathbb{Z}(N)$. The fact that this set gives a uniform partition of the circle is clear from its definition. Note that the set $\mathbf{Z}(N)$ satisfies the following properties:

(i) If $z, w \in \mathbb{Z}(N)$, then $zw \in \mathbb{Z}(N)$ and $zw = wz$.

(ii) $1 \in \mathbb{Z}(N)$.

(iii) If $z \in \mathbb{Z}(N)$, then $z^{-1} = 1/z \in \mathbb{Z}(N)$ and of course $zz^{-1} = 1$.

If we define the $n^{\text{th}}$ Fourier coefficient of $F$ by

$$a_n = \frac{1}{N} \sum_{k=0}^{N-1} F(k) e^{-2\pi ikn/N}$$

the above observations give the following fundamental theorem which is the $\mathbb{Z}(N)$ version of the Fourier inversion and the Parseval-Plancherel formulas.

**Theorem 1.** *If $F$ is a function on $\mathbb{Z}(N)$, then*

$$F(k) = \sum_{n=0}^{N-1} a_n e^{2\pi ink/N}$$

*Moreover,*

$$\sum_{n=0}^{N-1} |a_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2$$

After introducing the necessary preliminary results and required theorems,we begin with a naive approach to the problem. Fix $N$, and suppose that we are given $F(0), \dots, F(N-1)$ and $\omega_N = e^{-2\pi i/N}$. If we denote by $a_k^N(F)$ the $k^{\text{th}}$ Fourier coefficient of $F$ on $\mathbb{Z}(N)$, then by definition

$$a_k^N(F) = \frac{1}{N} \sum_{r=0}^{N-1} F(r) \omega_N^{kr}$$

and crude estimates show that the number of operations needed to calculate all Fourier coefficients is $\leqslant 2N^2 + N$. Indeed, it takes at most $N-2$ multiplications to determine $\omega_N^2, \dots, \omega_N^{N-1}$, and each coefficient $a_k^N$ requires $N+1$ multiplications and $N-1$ additions.

We now present the fast Fourier transform, an algorithm that improves the bound $O\left(N^2\right)$ obtained above.

**Theorem 2.** *Given $\omega_N = e^{-2\pi i/N}$ with $N = 2^n$, it is possible to calculate the Fourier coefficients of a function on $\mathbb{Z}(N)$ with at most*

$$4 \cdot 2^n \cdot n = 4N \log_2(N) = O(N \log N)$$

*operations.*

Let $\#(M)$ denote the minimum number of operations needed to calculate all the Fourier coefficients of any function on $\mathbb{Z}(M)$. The key to the proof of the theorem is contained in the following recursion step.

**Lemma 1** If we are given $\omega_{2M} = e^{-2\pi i/(2M)}$, then

$$\#(2M) \leqslant 2\#(M) + 8M.$$

# 3 Uncertainty Principles

The goal of this section is to quantify the relationship between a signal $(x_n)$ and $(\omega_n)$. First, we define the support of a signal

**Definition 1.** *For any given signal $f : \mathbb{Z}_N \to \mathbb{C}$, define the set*

$$supp f = \{x \in \mathbb{Z}_N \mid f(x) \neq 0\},$$

*or equivalently*

$$supp(x_n) = \{0 \leqslant n \leqslant N-1 \mid x_n \neq 0\}.$$

so notably for any signal we have $|supp f| \leqslant n^d$. We can easily see any length $N$ signal has $|supp(x_n)| \leqslant N$ by definition. The classical uncertainty principle guarantees a signal can not be both time and band limited – that is, a signal and its Fourier transform can not simultaneously have small supports.

**Theorem** (Classical Uncertainty Principle)**.** *For a nonzero signal $(x_n)_{n=0}^{N-1}$ and its frequencies $(\omega_n)_{n=0}^{N-1}$, let $N_t := |supp(x_n)|$ and $N_\omega := |supp(\omega_n)|$. Then*

$$N_t N_\omega > N.$$

The sharpness of the inequality can be shown through taking the constant 1 signal $f(n) = 1$, so $|N_t| = N$ and $\{\hat{f}_n\}$ will be supported only at the frequency at $n = 0$, and we have $|N_\omega||N_t| = N$. We add as a remark that in higher dimensions $\mathbb{Z}_N^d$, the extremizers for the uncertainty principle occur only when our signal is the the characteristic function of a $k$-dimension subspace of $\mathbb{Z}_N^d$. Notably this tells us that a generic signal will often have a better estimate $|N_\omega||N_t| > N$.

In the context of signal processing, the inequality in 4 gives an lower bound to the time-bandwidth product of the signal which is dependent on the length of the signal and the dimension $(d = 1)$. Notably, the estimate does not make any distinction for where the zeros of the signal or its frequencies lie. The uncertainty principle immediately tells us that a **sparse** signal (one with many zero entries) must almost all its frequencies being nonzero. On the other one can check that a constant signal vanishes on all but one frequency.

In practice, one wishes to transfer information through decomposing signals into frequencies. Section two provided an efficient algorithm to do this through **FFT**, but one can expect certain frequencies are dropped when transferring information due to noise or interference. As a result suppose we only receive information coming from certain frequencies. A natural question is it possible to **uniquely** recover the original signal from only frequencies we observe? Consider the following cases:

1. If we have received every frequency $(\omega_n)_{n=0}^{N-1}$, then we can completely reconstruct the signal by Fourier inversion 4.

2. If we have lost every frequency, there is no way to uniquely recover a signal $f$.
3. If the signal is sparse, then there must have **significant** amounts of nonzero frequencies due to the uncertainty principal 4.

Sparse signals should be less complex and ideally these are the signals we can hope to recover even with some frequencies unobserved.

# 4 Exact Recovery

The setup on the problem is as follows

**Question:** Suppose we are given the length of a signal, say $N$, and we only know the signal has $|N_t|$ nonzero entries. The signal is decomposed into frequencies and transferred over, but some subset $W$ with $|W| = N_\omega$ frequencies are unobserved due to interference. When can we recovery the original signal uniquely?

The following result due to [1] shows that **unique recovery** is possible if the signal $f$ is **sparse** and there are not too many unobserved frequencies.

**Theorem** (Donoho Stark Uncertainty Principle)**.** *Let $(x_k)_{k=0}^{N-1}$ be a signal with $N_t$ nonzero entries. Suppose the frequencies $(\omega_k)_{k=0}^{N-1}$ are unobserved on $N_\omega$ frequencies. Then the signal $(x_k)_{k=0}^{N-1}$ can be **uniquely recovered** from the observed frequencies if*

$$N_t N_\omega < \frac{N}{2}.$$

Specifically we see that no more than half the frequencies can be lost to have recovery, and **DSUP** 4 gives the following heuristic – the more frequencies are unobserved, the sparser our original signal must be to have recovery.

First, let us specify the **uniqueness** of recovery under the conditions of the theorem.

**Proposition** (Unique Recovery)**.** *Let a nonzero signal of length $N$, $f : \mathbb{Z}_N \to \mathbb{C}$ satisfy*

1. *$f$ has $N_t$ nonzero entries.*
2. *$N_\omega$ frequencies remain unobserved.*
3. *$N_t N_\omega < \frac{N}{2}$.*

*Then we call $g : \mathbb{Z}_n \to \mathbb{C}$ a recovered signal of $f$ if*

4. *$\hat{g} = \hat{f}$ on the observed frequencies.*
5. *$g$ has $N_t$ nonzero entries.*

*Given the conditions* 1, 2, 3*, any two recovered signals $g, \tilde{g}$ will satisfy $g = \tilde{g}$.*

*Proof.* Let $W$ denote the set of unobserved frequencies $\{\hat{f}_w\}_{w \in W}$. Suppose $g, \tilde{g}$ recover $f$, so $\hat{g}(m) = \hat{\tilde{g}}(m)$ on the observed frequencies $m \notin W$. We have $\hat{g}(m) - \hat{\tilde{g}}(m) = 0$ on $\mathbb{Z}_N \backslash W$ so the difference $\hat{h} := \hat{g} - \hat{\tilde{g}}$ is supported on a subset of $W$ which implies $|supp\hat{h}| \leqslant |W| = N_\omega$. Note we have $h = g - \tilde{g}$ and by condition 5, $|supph| < 2N_t$. We have have by condition 3,

$$|supph| \cdot |supp\hat{h}| < 2N_t N_\omega < N$$

which contradicts the classical uncertainty principle 4. Therefore we have $\hat{h} = 0$, which implies $\tilde{g} = g$ and we have uniqueness. ∎

For the remainder of this section, we focus on the specific case of recovery of binary signals, which take only the values 0 or 1, coming from Donoho-Stark [1] through a rounding algorithm. Such binary signals on $\mathbb{Z}_N$ can be realized as characteristic functions on subset of $E \subset \mathbb{Z}_N$.

**Definition 2.** *Let $E \subset \mathbb{Z}_N$ and take $E(x)$ to be the characteristic function of $E$;*

$$E(x) = \begin{cases} 1, & x \in E \\ 0, & x \notin E. \end{cases}$$

*Define the frequency projected signal of $E$ to $B \subset \mathbb{Z}_N$ as the signal given by*

$$\begin{aligned} P_B E(x) : &= \mathcal{F}^{-1}[B(\xi)\hat{E}(\xi)](x) \\ &= \sum_{m \in B} \hat{E}(m)\chi(m \cdot x). \end{aligned}$$

**Definition 3.** *Let $E \subset \mathbb{Z}_N$ be a binary signal and suppose $S \subset \mathbb{Z}_N$ give the missing frequencies of $\hat{E}$. The set of known frequencies is $B = \mathbb{Z}_N \backslash S$. We construct a binary signal $G$ as follows from rounding $P_B E$:*

$$G_B(x) := \begin{cases} 1, & |P_B E(x)| \geqslant \frac{1}{2} \\ 0, & |P_B E(x)| < \frac{1}{2}. \end{cases}$$

*We say that the binary signal $E$ can be recovered by rounding if $E(x) = G(x)$ for all $x \in \mathbb{Z}_N$.*

Donoho and Stark [1] are able to give a quantitative criterion in terms of uncertainty principles for when DRA is possible.

**Theorem 3.** *Let $E \subset \mathbb{Z}_N$ be a binary signal. Suppose $S \subset \mathbb{Z}_N$ are unobserved frequencies of $\hat{E}$. If*

$$|E||S| < \frac{N}{4},$$

*then $E$ can be recovered with a direct rounding algorithm.*

Other scenarios of signal recovery in different circumstances can be found in [2], which improved uncertainty principal estimates through discrete Fourier restriction estimates. However, such estimates come into play at higher dimensions $d > 1$ and invoke certain $L^p \to L^q$ restriction estimates for Holder conjugates $p, q$ rather than $L^2 \to L^2$ Cauchy Schwartz that is employed in this exposition. Notably [2] treated recovery of random signals.

# Appendix

## Proofs in Section 1 Discrete Fourier Transform

**Proposition** (Fourier Inversion)**.** *For any signal* $f : Z_N^d \to \mathbb{C}$,

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

*Proof.* Expand $\chi(x \cdot m)\chi(-y \cdot m) = e^{\frac{2\pi i x m}{N}} e^{\frac{-2\pi i y m}{N}} = e^{\frac{2\pi i (x-y) m}{N}} = \chi(x - y \cdot m)$. The inner sum $\sum_{m \in \mathbb{Z}_N^d} \chi((x - y) \cdot m)$ is key here. By the orthogonality property of characters over $\mathbb{Z}_N^d$:

- If $x = y$, then $\sum_{m \in \mathbb{Z}_N^d} \chi((x - y) \cdot m) = N^d$.
- If $x \neq y$, then $\sum_{m \in \mathbb{Z}_N^d} \chi((x - y) \cdot m) = 0$.

Therefore,

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

$$\begin{aligned}
\sum_{x \in \mathbb{Z}_N^d} \chi(x \cdot m)\hat{f}(m) &= \sum_{x \in \mathbb{Z}_N^d} \chi(x \cdot m)(N^{-d} \sum_{y \in \mathbb{Z}_N^d} \chi(-y \cdot m) f(y)) \\
&= \frac{1}{N^d} \sum_{x \in \mathbb{Z}_N^d} \chi(x \cdot m) \sum_{y \in \mathbb{Z}_N^d} \chi(-y \cdot m) f(y) \\
&= \frac{1}{N^d} \sum_{m \in \mathbb{Z}_N^d} \chi(x \cdot m) \sum_{y \in \mathbb{Z}_N^d} \chi(-y \cdot m) f(y) \\
&= \frac{1}{N^d} \sum_{y \in \mathbb{Z}_N^d} f(y) \sum_{m \in \mathbb{Z}_N^d} \chi((x - y) \cdot m) \\
&= \frac{1}{N^d} \sum_{y \in \mathbb{Z}_N^d} f(y) \cdot N^d \delta_{x,y} \\
&= f(x)
\end{aligned}$$

□

**Theorem** (Plancharel)**.**

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

*Proof:*

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

Therefore,

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

## Proofs in Section 2 Fast Fourier Transform Algorithm

**Theorem 4.** *Given $\omega_N = e^{-2\pi i/N}$ with $N = 2^n$, it is possible to calculate the Fourier coefficients of a function on $\mathbb{Z}(N)$ with at most*

$$4 \cdot 2^n \cdot n = 4N \log_2(N) = O(N \log N)$$

*operations.*

The proof of the theorem consists of using the calculations for $M$ division points, to obtain the Fourier coefficients for $2M$ division points. Since we choose $N = 2^n$, we obtain the desired formula as a consequence of a recurrence which involves $n = O(\log N)$ steps.This step uses symmetry and periodicity properties inherent in the Fourier transform, allowing us to efficiently handle the larger set by focusing on two smaller subsets. $\square$

Let $\#(M)$ denote the minimum number of operations needed to calculate all the Fourier coefficients of any function on $\mathbb{Z}(M)$. The key to the proof of the theorem is contained in the following recursion step.

**Lemma 1** If we are given $\omega_{2M} = e^{-2\pi i/(2M)}$, then

$$\#(2M) \leqslant 2\#(M) + 8M.$$

Proof. The calculation of $\omega_{2M}, \ldots, \omega_{2M}^{2M}$ requires no more than $2M$ operations. Note that in particular we get $\omega_M = e^{-2\pi i/M} = \omega_{2M}^2$. The main idea is that for any given function $F$ on $\mathbf{Z}(2M)$, we consider two functions $F_0$ and $F_1$ on $Z(M)$ defined by

$$F_0(r) = F(2r) \quad \text{and} \quad F_1(r) = F(2r+1).$$

We assume that it is possible to calculate the Fourier coefficients of $F_0$ and $F_1$ in no more than $\#(M)$ operations each. If we denote the Fourier coefficients corresponding to the groups $\mathbb{Z}(2M)$ and $\mathbb{Z}(M)$ by $a_k^{2M}$ and $a_k^{M}$, respectively, then we have

$$a_k^{2M}(F) = \frac{1}{2}\left(a_k^M\left(F_0\right) + a_k^M\left(F_1\right)\omega_{2M}^k\right)$$

To prove this, we sum over odd and even integers in the definition of the Fourier coefficient $a_k^{2M}(F)$, and find

$$\begin{aligned}
a_k^{2M}(F) &= \frac{1}{2M}\sum_{r=0}^{2M-1} F(r)\omega_{2M}^{kr} \\
&= \frac{1}{2}\left(\frac{1}{M}\sum_{\ell=0}^{M-1} F(2\ell)\omega_{2M}^{k(2\ell)} + \frac{1}{M}\sum_{m=0}^{M-1} F(2m+1)\omega_{2M}^{k(2m+1)}\right) \\
&= \frac{1}{2}\left(\frac{1}{M}\sum_{\ell=0}^{M-1} F_0(\ell)\omega_M^{k\ell} + \frac{1}{M}\sum_{m=0}^{M-1} F_1(m)\omega_M^{km}\omega_{2M}^k\right)
\end{aligned}$$

which establishes our assertion. As a result, knowing $a_k^M\left(F_0\right), a_k^M\left(F_1\right)$, and $\omega_{2M}^k$, we see that each $a_k^{2M}(F)$ can be computed using no more than three operations (one addition and two multiplications). So

$$\#(2M) \leqslant 2M + 2\#(M) + 3 \times 2M = 2\#(M) + 8M,$$

and the proof of the lemma is complete. An induction on $n$, where $N = 2^n$, will conclude the proof of the theorem. The initial step $n = 1$ is easy, since $N = 2$ and the two Fourier coefficients are

$$a_0^N(F) = \frac{1}{2}(F(1) + F(-1)) \quad \text{and} \quad a_1^N(F) = \frac{1}{2}(F(1) + (-1)F(-1)).$$

Calculating these Fourier coefficients requires no more than five operations, which is less than $4 \times 2 = 8$. Suppose the theorem is true up to $N = 2^{n-1}$ so that $\#(N) \leqslant 4 \cdot 2^{n-1}(n-1)$. By the lemma we must have

$$\#(2N) \leqslant 2 \cdot 4 \cdot 2^{n-1}(n-1) + 8 \cdot 2^{n-1} = 4 \cdot 2^n n,$$

which concludes the inductive step and the proof of the theorem. □

## Proofs in Section 3 Uncertainty Principles

**Theorem** (Classical Uncertainty Principle)**.** *For a nonzero signal* $(x_n)_{n=0}^{N-1}$ *and its frequencies* $(\omega_n)_{n=0}^{N-1}$*, let* $N_t := |supp(x_n)|$ *and* $N_\omega := |supp(\omega_n)|$*. Then*

$$N_t N_\omega > N.$$

*Proof.* Let $f : \mathbb{Z}_n \to \mathbb{C}$ be a signal supported on $E$ of size $|E| = N_t$. Suppose $\hat{f} : \mathbb{Z}_n \to \mathbb{C}$ is frequency supported on $W$ of size $|W| = N_\omega$. Fourier inversion gives

$$f(x) = N^{-1}\sum_{m \in W}\chi(x \cdot m)\hat{f}(m)$$

and applying Cauchy Schwartz we see for any $x \in \mathbb{Z}_n$

$$
\begin{aligned}
|f(x)|^2 &\leqslant N^{-1}|N_\omega| \sum_{m \in \mathbb{Z}_n} |\hat{f}(m)|^2 \\
&\leqslant N^{-1}|N_\omega| \sum_{n \in E} |f(n)|^2. && \text{(Plancharel)} \\
\sum_{x \in E} |f(x)|^2 &\leqslant N^{-1}|N_\omega||N_t| \sum_{n \in E} |f(n)|^2.
\end{aligned}
$$

and we recover $|N_\omega||N_t| \geqslant N$. □

## Proofs in Section 4 Exact Recovery

**Theorem 5.** *Let $E \subset \mathbb{Z}_N$ be a binary signal. Suppose $S \subset \mathbb{Z}_N$ are unobserved frequencies of $\hat{E}$. If*

$$|E||S| < \frac{N}{4},$$

*then $E$ can be recovered with a direct rounding algorithm.*

*Proof.* We write by Fourier inversion

$$
\begin{aligned}
E(x) &= \sum_{m \in S} \chi(x \cdot m)\hat{E}(m) + \sum_{m \notin S} \chi(x \cdot m)\hat{E}(m) \\
&= P_S E(x) + P_B E(x).
\end{aligned}
$$

where $B = \mathbb{Z}_N \backslash S$. Applying Cauchy Schwartz on $P_S E$ directly gives

$$
\begin{aligned}
|P_S E(x)|^2 &\leqslant |S| \big( \sum_{m \in S} |\hat{E}(m)|^2 \big) \\
&\leqslant |S| \big( \sum_{m \in \mathbb{Z}_n} |\hat{E}(m)|^2 \big) \\
&= N^{-1}|S||E| < \frac{1}{4},
\end{aligned}
$$

where the last inequality follows from the assumption, and taking square roots we get $|P_S E(x)| < \frac{1}{2}$ for each $x$. We have

$$P_B E(x) = E(x) - P_S E(x).$$

so by the triangle inequality

$$|P_B E(x)| < |E(x)| + \frac{1}{2}.$$

Using the DRA, the construct the binary signal

$$G_B(x) = \begin{cases} 1, & x \in E \\ 0, & x \notin E. \end{cases}$$

hence $G_B = E$ and the signal $E$ is recovered by DRA. □

## References


[1] David L. Donoho and P. B. Stark. Uncertainty principles and signal recovery. *SIAM Journal on Applied Mathematics*, 49:906–930, 1989.

[2] Alex Iosevich and Azita Mayeli. Uncertainty principles on finite abelian groups, restriction theory, and applications to sparse signal recovery. *2311.04331*, 2023.

[3] E. M. Stein and R. Shakarchi. *Fourier Analysis: An Introduction*. Princeton University Press, 2003.