UNCERTAINTY PRINCIPLES, RESTRICTION, BOURGAIN'S Λ_q THEOREM, AND SIGNAL RECOVERY

A. IOSEVICH AND A. MAYELI

Abstract. Let G be a finite abelian group. Let $f : G \to \mathbb{C}$ be a signal (i.e. function). The classical uncertainty principle asserts that the product of the size of the support of f and its Fourier transform $\hat{f}$, $\text{supp}(f)$ and $\text{supp}(\hat{f})$ respectively, must satisfy the condition:

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

In the first part of this paper, we improve the uncertainty principle for signals with Fourier transform supported on generic sets. This improvement is achieved by employing *the restriction theory*, including Bourgain celebrate result on Λ_q-sets, and the *the Salem set* mechanism from harmonic analysis. Then we investigate some applications of uncertainty principles that were developed in the first part of this paper, to the problem of unique recovery of finite sparse signals in the absence of some frequencies.

Donoho and Stark ([11]) showed that a signal of length N can be recovered exactly, even if some of the frequencies are unobserved, provided that the product of the size of the number of non-zero entries of the signal and the number of missing frequencies is not too large, leveraging the classical uncertainty principle for vectors. Our results broaden the scope for a natural class of signals in higher-dimensional spaces. In the case when the signal is binary, we provide a very simple exact recovery mechanism through the DRA algorithm.

Contents

1. Introduction

The purpose of this paper is to examine some basic questions in the realm of signal recovery from incomplete data in signal processing, from the point of view of Fourier uncertainty principles obtained using the restriction theory for the Fourier transform. The questions are motivated by the seminal paper by Donoho and Stark ([11]) where the uncertainty principle

Date: May 25, 2024.

A.I. was supported in part by the National Science Foundation under grant no. HDR TRIPODS - 1934962 and by the NSF DMS - 2154232. A.M. was supported in part by AMS-Simons Research Enhancement Grant and the PSC-CUNY research grants.

was used in a fundamental way to affect the exact recovery of a sequence encoded in terms of its Discrete Fourier Transform (DFT).

The main thrust of this work is to investigate how classical restriction theory which has played such an important role in modern harmonic analysis comes into play in exact signal recovery via suitable uncertainty principle estimates. We also develop conditions under which exact signal recovery can be accomplished very simply and efficiently. Finally, we develop a simple procedure that allows us to both discretize a signal and perform an efficient recovery procedure.

This article is organized as follows. In Section 2.1 we describe the Donoho-Stark approach to exact signal recovery via the classical uncertainty principle. Section 3 is dedicated to the exposition of a variety of uncertainty principles, using restriction theory, Bourgain's Λ_q theorem, randomness, and decay properties of the Fourier transform. The interaction between the parameters associated with these quantities is discussed as well. In Section 4, we describe the application of the uncertainty principles in Section 3 to exact signal recovery. We also describe how these ideas combine with an elementary approach to exact signal recovery we call DRA (see Definition 4.4 below), the direct rounding algorithm. In Section 5, we discuss the exact recovery problem in a general setting, with a particular focus on the celebrated Euclidean restriction conjecture. Finally, the remaining proofs are given in Section 6.

1.1. **Acknowledgements.** The authors wish to thank Mark Rudelson, Terry Tao, and Roman Vershynin for helpful remarks on the initial arXiv version of this paper. In particular, they wish to thank Terry Tao for pointing out Meshulam's paper on the generalization of Tao's uncertainty principle for prime fields.

2. Preliminaries

2.1. **Donoho-Stark's uncertainty principle.** In order to introduce our viewpoint, we need to establish some notation regarding the discrete Fourier transform on finite abelian groups. For clarity, we narrow our attention to the finite groups over cyclic groups, i.e., $G = \mathbb{Z}_N^d$, where $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ is the cyclic group (mod) N. For a given signal (i.e. function) $f : \mathbb{Z}_N^d \to \mathbb{C}$, we denote by $\hat{f}$ the Fourier transform of f, which is a function $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ defined by

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

where χ is a character function defined by $\chi(t) = e^{\frac{2\pi i t}{N}}$, $t \in \mathbb{Z}_N$. Here m is the element of the dual group $\widehat{\mathbb{Z}_N^d}$, that is identified with $\mathbb{Z}_N^d$ itself, and $x \cdot y$ is the dot product in $\mathbb{Z}_N^d$. The Fourier inversion formula is given by

$$f(x) = \sum_{m \in \mathbb{Z}_N^d} \chi(x \cdot m) \widehat{f}(m). \tag{2.1}$$

The Plancherel identify is given by

$$\sum_{x \in \mathbb{Z}_N^d} |f(x)|^2 = N^d \sum_{m \in \mathbb{Z}_N^d} |\hat{f}(m)|^2 \tag{2.2}$$

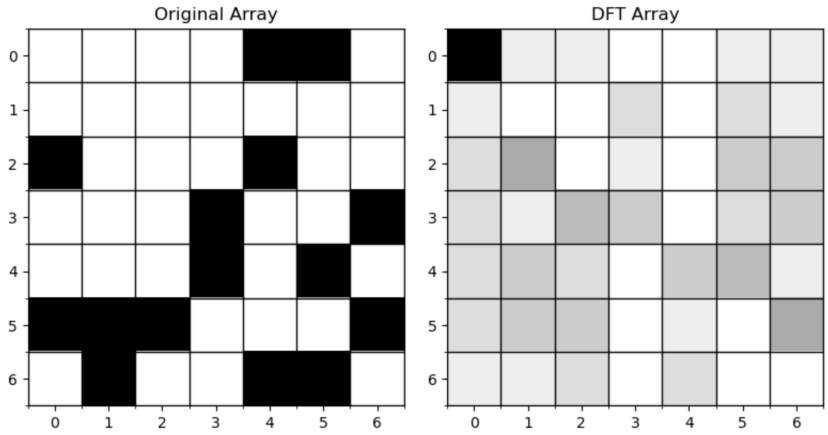

FIGURE 1. (left) A sparse 7×7 array of 1's and 0's in $\mathbb{Z}_7^2$, and (right) the array of its discrete Fourier transform on $\mathbb{Z}_7^2$ shaded according to the magnitude of the Fourier coefficients.

(For a description of the fundamentals of Fourier analysis on finite and infinite abelian groups, see e.g. [2, 31, 42].)

The *classical discrete-time uncertainty principle* for finite abelian groups is well-known. See, for example, [11, 38]. We shall outline the proof below (Proposition 3.1). For a sharper uncertainty principle result for $\mathbb{Z}_N$, N a prime, see Tao's result [41].

The principle for the group $G = \mathbb{Z}_N^d$ asserts that $f : \mathbb{Z}_N^d \to \mathbb{C}$ is a non-zero function with support $\text{supp}(f)$ and $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ denotes the Fourier transform with support $\text{supp}(\hat{f})$, then

$$|\text{supp}(f)| \cdot |\text{supp}(\hat{f})| \geq N^d. \tag{2.3}$$

This bounds the time-bandwidth product from below. This principle can be expressed in 1-dimensional case $\mathbb{Z}_N$ as follows: Let $(x_i)_{i=1}^{N-1}$ be a finite vector, and let the corresponding discrete Fourier transform $(\hat{x}_w)_{w=1}^{N-1}$ obtained through the DFT. If the original sequence has N_t non-zero entries and the transformed sequence has N_ξ non-zero entries, then

$$N_t \cdot N_\xi \geq N. \tag{2.4}$$

(For the proof, see Proposition 3.1.)

Another way to understand this inequality is that it implies the absence of any signal with a support size of $\sqrt{N/2}$ whose Fourier transform is non-zero only on a smaller region than $\sqrt{N/2}$ in size.

Using the uncertainty principle (2.4) in one dimension, Donoho and Stark established the following result for the recovery of finite one-dimensional signals in the presence of no noise.

Theorem 2.1 ([11]). *Let $f : \mathbb{Z}_N \to \mathbb{C}$ be a finite signal of length N in $\mathbb{Z}_N$ with N_t non-zero entries. Suppose that the set of unobserved frequencies $\{\hat{f}(m)\}_{m \in \mathbb{Z}_N}$ is of size N_w. Then the signal f can be 'recovered uniquely' from the observed frequencies if*

$$N_t \cdot N_w < \frac{N}{2}. \tag{2.5}$$

The result states that for successful unique recovery, the signal must exhibit some degree of sparsity, and a limited number of frequencies can be absent.

The recovery problem falls within the realm of inverse problems, and it has wide-ranging applications in computer vision, cryptography, data analysis, digital logic circuits, and many

other areas of computer science, data science, mathematics, and engineering. See, for example, [1, 3, 7, 8, 32, 33, 39, 36, 15, 6, 25] and the references contained therein.

2.1.1. *From uncertainty principle to exact recovery.* Donoho and Stark used an optimization and ℓ^2-minimization technique to recover the spare signal in the presence of missing frequencies, while they used the uncertainty principle to prove the uniqueness of the recovery. The proof of the uniqueness goes as follows: Let $f \neq 0$ with support $E = \text{supp}(f)$, and let $S \subset \mathbb{Z}_N$ be the set where the corresponding frequencies $\hat{f}(m)$, $m \in S$, are absent. Assume that r and g are two signals recovering f with $\hat{r}(m) = \hat{f}(m) = \hat{g}(m)$ for all $m \notin S$. Then $(\hat{r} - \hat{g})(m) = 0$ for all $m \notin S$. Define $h = r - g$. Thus, $\text{supp}(\hat{h}) \subset S$. On the other side, we have $\text{supp}(r) = \text{supp}(g) = \text{supp}(f)$. This implies that h is supported on a set of size at most $2|E|$, while $\widehat{h}$ is supported on S. By the uncertainty principle (2.4), no such h can exist if (2.5) holds, and the proof of the uniqueness is complete. The proof of uniqueness remains identical in higher dimensions.

Traditional approaches to establishing the uncertainty principle involve advanced techniques like Weyl's inequality or the use of prolate spheroidal wave functions. (For information on prolate spheroidal wave functions, see e.g. [37, 23].) These methods delve into complex concepts such as eigenfunctions of the Fourier transform (as demonstrated by Weyl in [44]) and eigenfunctions of compact operators, as introduced by Landau and Pollak in [26]. In the discrete setting, however, a much simpler approach can be employed, and this point of view is going to lead us to *an improved version* of the discrete-time uncertainty principle under some natural conditions.

For the remainder of the paper, we will omit mentioning discrete-time and simply refer to the uncertainty principle, provided it is clear from the context.

Remark 2.2. Several variants of the Donoho-Stark uncertainty principle have been explored in the literature, connecting to classical topics in mathematics. For instance, Tao's uncertainty principle [41] is a fundamental result with application in signal recovery and compressive sensing. Dyatlov's fractal uncertainty principle [10], on the other hand, is applied in ergodic theory and quantum chaos.

In this paper, we focus only on exploring the signal recovery problem in relation to the classical uncertainty principle of Donoho and Stark. However, we recognize the need to also explore recovery using different quantitative variants of the uncertainty principle.

3. Sharper uncertainty principles in $\mathbb{Z}_N^d$

3.1. **Via the restriction theory.** The goal of this section is to prove that the uncertainty principle can further *refined* using restriction theory. This result is stated in Theorem 3.6. For the sake of self-containment, we shall illustrate how the uncertainty principle in finite settings can be derived through the inverse Fourier transform.

Proposition 3.1. *Let $f : \mathbb{Z}_N^d \to \mathbb{C}$. Supposed that f is supported in $E \subset \mathbb{Z}_N^d$ and $\widehat{f}$ is supported in $\Sigma \subset \mathbb{Z}_N^d$. Then*

$$|E| \cdot |\Sigma| \geq N^d, \tag{3.1}$$

To prove this, note that by the Fourier Inversion Formula (2.1), we have

$$f(z) = \sum_{m \in \Sigma} \chi(z \cdot m) \widehat{f}(m), \quad \forall z \in E.$$

By applying the Cauchy-Schwarz inequality, we can derive the following: For any $z \in \mathbb{Z}_N^d$

$$|f(z)|^2 \leq |\Sigma| \cdot \sum_{m\in\Sigma} |\widehat{f}(m)|^2 = |\Sigma| \cdot \sum_{m\in\mathbb{Z}_N^d} |\widehat{f}(m)|^2$$

$$= |\Sigma| \cdot N^{-d} \cdot \sum_{x\in\mathbb{Z}_N^d} |f(x)|^2 \tag{3.2}$$

$$= |\Sigma| \cdot N^{-d} \cdot \sum_{x\in E} |f(x)|^2, \tag{3.3}$$

where in (3.2) we used the Plancherel identity (2.2), and in (3.3) we used the fact that f is supported in E. Summing both sides over $z \in E$ and dividing both sides by $\sum_{x\in E} |f(x)|^2$, we obtain (3.1), which recovers (2.4) in the case $d = 1$, and (2.3) in higher dimensions.

For a set A, we abuse notation by also denoting A as an indicator function, where $A(x)$ equals 1 if x belongs to A, and 0 otherwise.

Remark 3.2. It is important to note that the bound (3.1) is essentially sharp. For example, suppose that N is an integer, and E is a k-dimensional subspace of $\mathbb{Z}_N^d$. Then by a direct calculation, $\widehat{E}(m) = N^{-(d-k)}E^{\perp}(m)$, where $E^{\perp}$ is the orthogonal subspace to the space E, i.e., $e^{\frac{2\pi it\cdot n}{N}} = 1$ for all $t \in E$ and $n \in E^{\perp}$. When $m = \vec{0}$, this implies that $|E| \cdot |E^{\perp}| = N^d$. This indicates that if the frequencies in $E^{\perp}$ are missing or unobserved, it hinders the recovery of the original information. However, such examples are very rare. In fact, one can show that these are the only examples where the equality in (3.1) holds.

Remark 3.3. It is interesting to note that if N is prime, the problem takes on a variety of interesting additional features. For example, if $d = 1$, the classical uncertainty principle can be replaced by a stronger version proved by Tao ([41]). If $N = 2$, it is known ([24], [16]) that if $E \subset \mathbb{Z}_N^2$ and $\widehat{E}(m) = 0$ for some $m \in \mathbb{Z}_N^2$, then E has the same number of points on all lines perpendicular to m. This suggests a potentially interesting link between the exact recovery questions and tiling problems in vector spaces over finite fields. See, for example, [13], [14], and the references contained therein.

The key point we are going to exploit is that if Σ, the support of $\hat{f}$, is a typical set, then instead of using the support-driven identity

$$\sum_{m\in\Sigma} |\widehat{f}(m)|^2 = \sum_{m\in\mathbb{Z}_N^d} |\widehat{f}(m)|^2 \tag{3.4}$$

used in (3.2) above in the derivation of (3.1), followed by estimating the L^2 norm of f over its support, we can bound the left-hand side of (3.4) by a suitably scaled L^p-norm of f for some $p < 2$, resulting in *a generally better uncertainty principle*. This may seem counter-intuitive since (3.4) is an identity owing to the support assumption on $\widehat{f}$. The gain comes from comparing L^p norms, which leads to a lesser strain on the support of the signal f. To execute this idea, we bring in the following notion from classical restriction theory.

Definition 3.4. Let $S \subset \mathbb{Z}_N^d$. We say that a (p, q)-restriction estimation $(1 \leq p \leq q \leq \infty)$ holds for S if there exists a uniform constant $C_{p,q}$ (independent of N and S) such that for

any function $f : \mathbb{Z}_N^d \to \mathbb{C}$

$$\left(\frac{1}{|S|}\sum_{m\in S}|\widehat{f}(m)|^q\right)^{\frac{1}{q}} \leq C_{p,q}N^{-d}\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}}. \tag{3.5}$$

When p or q is infinity, we replace the norm by the supremum norm

$$\|\hat{f}\|_\infty = \max\{|\hat{f}(m)|\}_{m\in S}.$$

The definition indicates that when N is large, the frequency concentration of f on the set S is relatively low. This characteristic proves to be quite advantageous when it comes to signal recovery, especially in scenarios where frequencies outside of S are missing. See Corollary 4.1 below. The case $q = \infty$ immediately points to the relationship between the decay properties of the Fourier transform of S and the restriction phenomenon. We shall explore this phenomenon in more detail in Subsection 3.3.

Remark 3.5. Let us assume that S is a $(2, 2)$-restriction set, for which the inequality (3.5). Then for any $f \in L^2(\mathbb{Z}_N^d)$, one has

$$\sum_{m\in S}|\widehat{f}(m)|^2 \leq C_{2,2}^2|S|N^{-2d}\sum_{x\in\mathbb{Z}_N^d}|f(x)|^2. \tag{3.6}$$

Let B_S denote the frequency "cut-off" operator defined by $\widehat{B_S f} := \chi_S\hat{f}$. The preceding inequality indicates that

$$\|B_S f\|^2 \leq C_{2,2}^2|S|N^{-d}\|f\|^2. \tag{3.7}$$

Notice that B_S is a projection operator and it has maximum operator norm 1. The inequality above is sharp if $C_{2,2}^2|S|N^{-d} < 1$. Solving this for $|S|$, we obtain

$$|S| < CN^d.$$

Let $\Sigma \subset \mathbb{Z}_N^d$ be a non-trivial subset. Let P_Σ denote the spatio "cut-off" operator defined by $P_\Sigma(f) = \chi_\Sigma f$. The associated SSLO operator (matrix) with respect to the cut-off operators P_F and B_S is defined as $T_{S,F} = P_F B_S P_F$ (refer to, e.g., [23] and the references therein). It is know that the eigenvalues of the matrix $T_{S,F}$ constitute a non-increasing sequence of positive numbers upper bounded by 1:

$$1 > \lambda_1 \geq \cdots \lambda_k > 0,$$

and the largest eigenvalues λ_1 is given by

$$\lambda_1 = \max\left\{\frac{\|B_S f\|^2}{\|f\|^2} :\ P_\Sigma f = f\right\}.$$

Combining this with (3.7) gives us an upper bound for the top eigenvalue:

$$\lambda_1 \leq CN^{-d}|S|$$

Notice that upper bound is tight if $|S| << N^d$.

Looking at this from other point of view, one can assume that λ_1 is known. Then the smallest $C_{2,2}^2$ that one can expect is $|S|^{-1}N^d\lambda_1$; $C_{2,2} = |S|^{-1/2}N^{d/2}\lambda_1^{1/2}$ minimizes the constant in (3.5) for the case $p = q = 2$.

Next we do a similar analysis for the minimizer of $C_{p,q}$, when $(p, q) \neq (2, 2)$. For $1 \leq p \leq q \leq 2$, the question might be answered using some kind of interpolation technique,

A tremendous amount of work has been done on the restriction phenomenon in vector spaces over finite fields and modules over rings. See for example, [17, 19, 20, 21, 30] and the references contained therein. These results mostly deal with restriction to spheres, paraboloids, and other algebraic surfaces in finite settings. The Euclidean restriction theory is discussed briefly in Section 5 below. While these situations are interesting in the context of signal recovery, the most interesting case is where the restriction set S is random, and we are going to develop this theory later in this paper.

Our first result is the following.

Theorem 3.6 (An uncertainty Principle via Restriction Estimation I)**.** *Suppose that $f : \mathbb{Z}_N^d \to \mathbb{C}$ is supported in $E \subset \mathbb{Z}_N^d$, and $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ is supported in $\Sigma \subset \mathbb{Z}_N^d$. Suppose that the restriction estimation (3.5) holds for Σ for a pair (p, q), $1 \leq p \leq q < \infty$. Then*

$$|E|^{\frac{1}{p}} \cdot |\Sigma| \geq \frac{N^d}{C_{p,q}}. \tag{3.8}$$

Another version of the Restriction Theorem implies the Uncertainty Principle paradigm is the following.

Theorem 3.7 (An uncertainty Principle via Restriction Estimation II)**.** *Suppose that $f : \mathbb{Z}_N^d \to \mathbb{C}$ is supported in $E \subset \mathbb{Z}_N^d$, and $\hat{f} : \mathbb{Z}_N^d \to \mathbb{C}$ is supported in $\Sigma \subset \mathbb{Z}_N^d$. Suppose that the restriction estimation (3.5) holds for Σ for a pair (p, q), $1 \leq p \leq q$.*

i) If $q \geq 2$, then

$$|E|^{\frac{2-p}{p}} \cdot |\Sigma| \geq \frac{N^d}{C_{p,q}^2}. \tag{3.9}$$

ii) If $1 < q < 2$, then

$$|E|^{\frac{(q'-p)q}{q'p}} \cdot |\Sigma| \geq \frac{N^d}{C_{p,q}^q} \tag{3.10}$$

Remark 3.8. It is interesting to note that in either theorem mentioned above, when considering the pair (p, q) with $p = 1$, if the constraint estimation holds for any set Σ with a constant $C_{1,q} = 1$, it leads to the recovery of the classical uncertainty principle (3.1).

Remark 3.9. If the constant $C_{p,q}$ is small, Theorem 3.7 is strictly stronger than Theorem 3.6 since the exponents $\frac{p}{2-p}$ and $\frac{q'p}{(q-p)q}$ are both larger than p in the range $p > 1$. However, the fact that the constant $C_{p,q}$ is squared in the first part of Theorem 3.7 and raised to the power q in the second part means that Theorem 3.6 is stronger in different regimes.

Remark 3.10. Another reason Theorem 3.6 is valuable is that the underlying mechanism can be used in conjunction with the Direct Recovery Algorithm (DRA). This is convenient for many applications.

Remark 3.11. As an interested reader can easily check, the proof of Theorem 3.6 shows that (3.8) can be replaced by

$$\frac{\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}}}{\max_{x\in\mathbb{Z}_N^d}|f(x)|}\cdot|\Sigma|\geq\frac{N^d}{C_{p,q}}. \tag{3.11}$$

This is a better condition since the assumption that f is supported in E and straightforward domination imply that

$$\frac{\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}}}{\max_{x\in\mathbb{Z}_N^d}|f(x)|}\leq|E|^{\frac{1}{p}}.$$

Moreover, (3.11) is more stable than (3.8) since a small perturbation of f still satisfies the former, at a cost of a slight change in the constant. On the other hand, a small random perturbation of any function f results, with high probability, in a function that is non-zero on all of $\mathbb{Z}_N^d$. A concrete simple illustration of the relative strength of (3.11) is the following. Let E, F be disjoint subsets of $\mathbb{Z}_N^d$, and let $f(x)=E(x)+\delta F(x)$, where δ is a small parameter. Then the condition (3.8) takes the form

$$(|E|+|F|)^{\frac{1}{p}}\cdot|\Sigma|\geq\frac{N^d}{C_{p,q}},$$

whereas (3.11) translates to

$$(|E|+\delta|F|)^{\frac{1}{p}}\cdot|\Sigma|\geq\frac{N^d}{C_{p,q}},$$

which is much better if δ is small.

Similarly, the conclusion of part i) of Theorem 3.7 can be replaced by

$$\frac{\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{2}{p}}}{\sum_{x\in\mathbb{Z}_N^d}|f(x)|^2}\cdot|\Sigma|\geq\frac{N^d}{C_{p,q}^2}, \tag{3.12}$$

and the conclusion of part ii) can be replaced with

$$\frac{\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{q}{p}}}{\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^{q'}\right)^{\frac{q}{q'}}}\cdot|\Sigma|\geq\frac{N^d}{C_{p,q}^q} \tag{3.13}$$

Using the same example as above, it is not difficult to see that these conditions are often less restrictive than those in the statement of the theorem.

Theorem 3.6 and Theorem 3.7 naturally lead us to ask, under which conditions a non-trivial restriction estimation can hold for a given $\Sigma\subset\mathbb{Z}_N^d$? A sample result in this direction is the following.

Theorem 3.12. *Let $\Sigma \subset \mathbb{Z}_N^d$ with the property that*

$$|\Sigma| = \Lambda_{size} N^{\frac{d}{2}}, \tag{3.14}$$

and

$$|\{(x,y,x',y') \in U^4 : \ x+y = x'+y'\}| \leq \Lambda_{energy} \cdot |U|^2 \tag{3.15}$$

for every $U \subset \Sigma$.

Then the restriction estimation holds for Σ for (p,q), where $p = 4/3$ and $q = 2$. Indeed, for any $f : \mathbb{Z}_N^d \to \mathbb{C}$,

$$\left(\frac{1}{|\Sigma|} \sum_{m \in \Sigma} |\widehat{f}(m)|^2 \right)^{\frac{1}{2}} \leq \Lambda_{size}^{-\frac{1}{2}} \cdot \Lambda_{energy}^{\frac{1}{4}} \cdot N^{-d} \left(\sum_{x \in \mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}} \right)^{\frac{3}{4}}. \tag{3.16}$$

Remark 3.13. It is interesting to note that the assumption (3.15) holds in a variety of natural deterministic situations. For example, if $d = 2$, N is an odd prime, and

$$\Sigma = \{x \in \mathbb{Z}_N^2 : x_1^2 + x_2^2 = 1\},$$

the unit circle, then (3.15) is satisfied with $\Lambda_{energy} = 3$ and Λ_{size} essentially equal to 1. The resulting restriction theorem was first established by the first listed author and Doowon Koh in [18]. See also [17] for a variety of restriction theorems over $\mathbb{Z}_N^d$.

Remark 3.14. (Additive energy of random sets) Let $\Sigma \subset \mathbb{Z}_N^d$ of size $|\Sigma| = \Lambda_{\text{size}} N^{\frac{d}{2}} > N^{\frac{d}{2}}$. Suppose that Σ is chosen randomly with respect to the uniform distribution. Then the expected value of

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

is bounded by

$$(5 + \Lambda_{\text{size}}^2)|\Sigma|^2. \tag{3.17}$$

The proof, which uses Chernoff's classical bound shows considerable concentration around the mean and shows that with very high probability, the desired energy inequality holds. The result follows easily from the calculations in [12]. If the size of Σ is restricted a bit, (3.17) estimate can be replaced by a stronger version where the same estimate holds for every $U \subset \Sigma$. This allows one to use this estimate in conjunction with Theorem 3.12. A systematic study will be conducted in the sequel.

Remark 3.15. (Higher order additive energy) We note that Theorem 3.12 is just one example of the relationship between additive energy and restriction. It is not difficult to show that if

$$|\{(x^1,\dots,x^k,y^1,\dots,y^k) \in U^{2k} : x^1 + x^2 + \cdots + x^k = y^1 + y^2 + \cdots + y^k\}| \leq \Lambda_{\text{energy}} |U|^k$$

for every $U \subset S$, then we obtain the restriction estimate with the exponents $\left(\frac{2k}{2k-1}, 2\right)$ with the uniform constant suitably dependent on Λ_{energy} and Λ_{size}. More work is required to obtain an appropriate variant of (3.17). This investigation will be conducted in the sequel.

Remark 3.16. (Concentration versus support) Throughout this paper we are going to stick to the pure support conditions, namely, the signal is supported in a set E, and its Fourier transform is supported in a set S. In practice, many of the arguments go through, up to a constant, if we assume that f is concentrated in E in a suitable sense. For example, we could assume that

$$\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}}\leq C_{p,E}\left(\sum_{x\in E}|f(x)|^p\right)^{\frac{1}{p}},$$

which would allow all of our results to go through at the cost of the constant $C_{p,E}$. We shall state a precise definition below and give a sample result in the context of our discussion of Bourgain's Λ_q theorem and its consequences for the uncertainty principle.

Remark 3.17. (Interpolation) The $(\frac{4}{3},2)$ restriction theorem in Theorem 3.12 extends, by interpolation, to a $(p,2)$ restriction theorem for any $1\leq p\leq\frac{4}{3}$, since the $(1,2)$ restriction theorem always holds as we noted above.

3.2. **Bourgain's Λ_q theorem, improved uncertainty principle and consequences for exact recovery.** Let G be a locally compact abelian group. Let Γ denote the dual group of G. For $q>2$, $\Lambda\subset\Gamma$ is said to be a Λ_q-set if $L^q_\Lambda(G)=L^2_\Lambda(G)$. Here and throughout, for a Λ, $L^q_\Lambda(G)$ denotes the closure in $L^q(G)$ of characters belonging to Λ interpreted as functions on G. A celebrated result due to Jean Bourgain ([4]) says the following.

Theorem 3.18. *Let $\Psi=(\psi_1,\ldots,\psi_n)$ denote a sequence of n mutually orthogonal functions, with $||\psi_i||_{L^\infty(G)}\leq 1$. There exists a subset S of $\{1,2,\ldots,n\}$, $|S|>n^{\frac{2}{q}}$ such that*

$$\left|\left|\sum_{i\in S}a_i\psi_i\right|\right|_{L^q(G)}\leq C(q)\left(\sum_{i\in S}|a_i|^2\right)^{\frac{1}{2}}.$$

The constant $C(q)$ depends only on q and the estimate above holds for a generic set of size $\lceil n^{\frac{2}{q}}\rceil$, where $\lceil x\rceil$ denotes the smallest integer greater than x.

The following consequence of Theorem 3.18 is particularly relevant to our investigation.

Corollary 3.19. *Given $f:\mathbb{Z}_N^d\to\mathbb{C}$, let*

$$\widehat{f}(m)=N^{-d}\sum_{x\in\mathbb{Z}_N^d}\chi(-x\cdot m)f(x),\ x\cdot m=x_1m_1+\cdots+x_dm_d,$$

where $\chi(t)=e^{\frac{2\pi it}{N}}$. Then for a generic subset Σ of $\mathbb{Z}_N^d$ of size $\lceil N^{\frac{2d}{q}}\rceil$, $q>2$, if $\widehat{f}$ is supported in Σ, we have

$$||f||_{L^q(\mu)}\leq C(q)||f||_{L^2(\mu)},\tag{3.18}$$

where $C(q)$ depends only on q, and here, and throughout,

$$||f||_{L^p(\mu)}=\left(\frac{1}{N^d}\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}}.\tag{3.19}$$

The following result provides a connection between Corollary 3.19 and the restriction theory results of the previous subsection. This connection follows from duality, but we make the statement and the argument explicit for the sake of simplicity and completeness.

Proposition 3.20. *Suppose that (3.18) holds for some $q > 2$ for Σ as in the statement of Corollary 3.18. Then*

$$\left(\frac{1}{|\Sigma|}\sum_{m\in\Sigma}|\widehat{f}(m)|^2\right)^{\frac{1}{2}} \leq C(q)\left(\frac{N^{\frac{2d}{q}}}{|\Sigma|}\right)^{\frac{1}{2}}\cdot N^{-d}\cdot\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^{q'}\right)^{\frac{1}{q'}}, \tag{3.20}$$

i.e the $(q', 2)$ restriction holds with the constant bound by

$$C(q)\cdot\left(\frac{N^{\frac{2d}{q}}}{|\Sigma|}\right)^{\frac{1}{2}}.$$

Since $|\Sigma| = [N^{\frac{2d}{q}}]$, the $(q', 2)$ holds with the constant $\leq C(q)$.

Before we state our first result, we need a definition that we foreshadowed in Remark 3.16 above.

Definition 3.21. We say that $f : \mathbb{Z}_N^d \to \mathbb{C}$ is L^p-concentrated on $E \subset \mathbb{Z}_N^d$ at level λ if

$$\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^p\right)^{\frac{1}{p}} \leq \lambda\left(\sum_{x\in E}|f(x)|^p\right)^{\frac{1}{p}}.$$

Our first result is the following.

Theorem 3.22. *[Uncertainty Principle in the presence of Randomness]. Let $\Sigma \subset \mathbb{Z}_N^d$ of size $\left[N^{\frac{2d}{q}}\right]$, chosen randomly with uniform probability. Suppose that $f : \mathbb{Z}_N^d \to \mathbb{C}$ is L^2-concentrated in $E \subset \mathbb{Z}_N^d$ at level $\lambda \geq 1$. Suppose $\widehat{f}$ is supported on Σ. Then with probability $1 - o_N(1)$,*

$$|E| \geq \frac{N^d}{(\lambda C(q))^{\frac{1}{\frac{1}{2}-\frac{1}{q}}}},$$

where $C(q)$ depends only on q.

Remark 3.23. Note that the numerology of Theorem 3.22 is the same as that of part i) of Theorem 3.7 in the case when $|S| \sim N^{\frac{2d}{q}}$, $q = p'$. This is because the two statements are dual up to normalization. The main point here is that the conclusion of Theorem 3.7 holds for a generic set S of size $\sim N^{\frac{2d}{q}}$. It would be interesting to quantify the statement that S is generic more precisely. This issue shall be addressed in the sequel.

Remark 3.24. Qualitatively, Theorem 3.22 says that if $\widehat{f}$ is supported on a random set S of size $\approx N^{d-\epsilon}$ for some $\epsilon > 0$, then the support of f is a positive proportion of $\mathbb{Z}_N^d$. On the other hand, if the support of $\widehat{f}$ is all of $\mathbb{Z}_N^d$, for instance, if $\widehat{f}$ is identically 1, then f is supported at the origin. It is natural to conjecture, qualitatively, that if $\widehat{f}$ is supported

on a random set of size $o(N^d)$, then the support of f is a positive proportion of $\mathbb{Z}_N^d$. This naturally leads to consider replacing the L^p, $p > 2$, space in Bourgain's inequality by a suitable function space close to L^2. A good starting point for this investigation is the Orlicz space version of Theorem 3.18 proved by Donggeun Ryou ([9]). Roughly speaking, in our context, he obtained a variant of Theorem 3.18 in the case when L^p spaces are replaced by Orlciz spaces defined by the Young function $\Phi(t) \sim t^p \log^{\alpha p}(t)$ for $p > 2$. The case we need, namely when $p = 2$, appears particularly difficult. We shall investigate this matter systematically in the sequel.

3.3. **Salem sets and Salem uncertainty principle.** We are now going to explore uncertainty principles based on the assumption that the underlying sets are Salem sets, named after Raphael Salem, the mathematician who first discovered them and studied their properties (see e.g. [35]). In the finite setting, the definition requires a bit of care.

Definition 3.25 (Salem sets)**.** A set $S \subset \mathbb{Z}_N^d$ is a Salem set at level Λ_{Salem} if

$$|\widehat{S}(z)| \leq \Lambda_{\text{Salem}} \cdot N^{-d} \cdot |S|^{\frac{1}{2}} \quad \forall\ z \neq 0. \tag{3.21}$$

Notice that every set is a Salem set with the constant $\Lambda_{\text{Salem}} = |S|^{\frac{1}{2}}$. This follows from the following simple argument: By the definition of the Fourier transform, the inequality

$$|\widehat{S}(z)| \leq N^{-d}|S|$$

always holds. Therefore, we can write

$$|\widehat{S}(z)| \leq |S|^{\frac{1}{2}} \cdot N^{-d}|S|^{\frac{1}{2}}.$$

In general, however, the estimate on Λ_{Salem} is much better, as we will show later in Proposition 3.29. Indeed, it shows that with probability $1 - N^{-d\epsilon}$, a randomly chosen set S satisfies the bound $|\widehat{S}(z)| \leq \Lambda_{\text{Salem}} N^{-d}|S|^{\frac{1}{2}}$, for $z \neq (0, \ldots, 0)$, with $\Lambda_{\text{Salem}} \leq \sqrt{(1+\epsilon)d\ln(n)}$.

Theorem 3.26. *(Salem Uncertainty Principle) Let $E, \Sigma \subset \mathbb{Z}_N^d$. Suppose that Σ is Salem at level Λ_{Salem}. Then if $f : \mathbb{Z}_N^d \to \mathbb{C}$ is supported in E and its Fourier transform $\hat{f}$ with support in Σ, we have*

$$|E| \cdot |\Sigma|^{\frac{3}{4}} \geq N^d \cdot \sqrt{\frac{1 - dens(\Sigma)}{\Lambda_{Salem}}}, \tag{3.22}$$

where $dens(\Sigma) = N^{-d}|\Sigma|$ is the density of the set Σ.

Remark 3.27. It is not difficult to see that the roles of E and Σ in Theorem 3.26 can be switched if E is assumed to be a Salem set.

Remark 3.28. The interested reader can check that the proof of Theorem 3.26 given below also yields a restriction theorem. In the course of proving Theorem 3.26, we show that

$$\left(\frac{1}{|\Sigma|}\sum_{m\in\Sigma}|\widehat{f}(m)|^2\right)^{\frac{1}{2}} \leq \frac{N^{-d}\cdot|\Sigma|^{-\frac{1}{4}}\cdot\Lambda_{\text{Salem}}^{\frac{1}{2}}\cdot\sum_x|f(x)|}{\sqrt{1-dens(S)}}. \tag{3.23}$$

We can also check using Plancherel that

$$\left(\frac{1}{|\Sigma|}\sum_{m\in\Sigma}\left|\widehat{f}(m)\right|^2\right)^{\frac{1}{2}} \leq |\Sigma|^{-\frac{1}{2}}N^{-\frac{d}{2}}\cdot\left(\sum_x |f(x)|^2\right)^{\frac{1}{2}} \tag{3.24}$$

$$= N^{-d}\cdot\left(\frac{N^d}{|\Sigma|}\right)^{\frac{1}{2}}\left(\sum_x |f(x)|^2\right)^{\frac{1}{2}}.$$

Interpolating (3.23) and (3.24), we see that

$$\left(\frac{1}{|\Sigma|}\sum_{m\in\Sigma}\left|\widehat{f}(m)\right|^2\right)^{\frac{1}{2}} \leq \left(\Lambda_{\text{Salem}}^{\frac{1}{2}}\cdot|\Sigma|^{-\frac{1}{4}}\right)^{1-\frac{2}{p'}}\cdot\left(\frac{N^d}{|\Sigma|}\right)^{\frac{1}{p'}}\cdot N^{-d}\left(\sum_x |f(x)|^p\right)^{\frac{1}{p}} \tag{3.25}$$

$$= \Lambda_{\text{Salem}}^{\frac{1}{2}-\frac{1}{p'}}|\Sigma|^{-\frac{1}{4}-\frac{1}{2p'}}N^{\frac{d}{p'}}\cdot N^{-d}\cdot\left(\sum_x |f(x)|^p\right)^{\frac{1}{p}}$$

for $1\leq p\leq 2$.

In particular, if $|\Sigma|\approx N^\alpha$ and $0<\alpha<d$, then under the assumptions of Theorem 3.26, we obtain a $(p,2)$ restriction theorem for $p'\geq\frac{2(2d-\alpha)}{\alpha}$. See, for example, [30] for analogous results.

Theorem 3.26 leads to the natural question of which sets S are Salem at level Λ_{Salem}, and this leads us to consider the following. Given $A\subset\mathbb{Z}_N^d$, define

$$\Phi(A)=\max\left\{|\widehat{A}(m)| : m\in\mathbb{Z}_N^d;\ m\neq\vec{0}\right\}.$$

Given that $|A|\leq\frac{N^d}{2}$, the quantity $\Phi(A)$ is bounded from below and above as

$$N^{-d}\sqrt{\frac{|A|}{2}}\leq\Phi(A)\leq N^{-d}|A|,$$

where the upper bound follows from direct domination and the lower bound follows from Plancherel theorem and the assumption on the size of A. (For a detailed proof, we refer to Proposition 2.6 in [2].) The following result addresses the question we raised above about when we can expect a Salem type estimate to hold.

Proposition 3.29 ([2], Proposition 5.14)**.** *Let $\epsilon>0$. For all but $O(N^{-d\epsilon})$ subsets A of $\mathbb{Z}_N^d$ of size $|A|\leq\frac{N^d}{2}$*

$$\Phi(A)<N^{-d}\sqrt{2(1+\epsilon)|A|\cdot d\cdot\ln(N)}, \tag{3.26}$$

where $\ln(N)$ is the natural logarithm of N.

Remark 3.30. The proof of Proposition 3.29 shows that if A of a given size $\leq\frac{N^d}{2}$ is chosen randomly, with respect to the uniform probability distribution on $\mathbb{Z}_N^d$, then for any $\epsilon>0$, (3.26) holds with probability $1-N^{-d\epsilon}$.

Also, observe that the random subset S is significantly smaller than the total size of $\mathbb{Z}_N^d$, specifically less than half of it, chosen uniformly at random.

3.3.1. *Comparison with Meshulam's uncertainty principle.* Roy Meshulam ([28]) proved the following extension of Tao's uncertainty principle ([41]). Suppose that G is an abelian group of size N, and d_1, d_2 are two consecutive divisors of N with $d_1 < d_2$. Suppose that $f : G \to \mathbb{C}$ such that f is supported in E and $\widehat{f}$ is supported in S. If $d_1 \leq |E| \leq d_2$, then

$$|S| \geq \frac{N}{d_1 d_2} \left(d_1 + d_2 - |E|\right). \tag{3.27}$$

To give an example of a comparison between this estimate and the results of this paper, let's consider the case when $N = a^2$, a large prime. Let $d_1 = 1, d_2 = a$, and let $|E| = a-k$, for some $0 \leq k \leq a-1$, with the exact value of k to be determined later. Then by Meshulam's result, if $f : \mathbb{Z}_N \to \mathbb{C}$ supported in E, with $\widehat{f}$ supported in S, then

$$|S| \geq \frac{a^2}{a}(1 + a - |E|) = a + a^2 - a(a-k) = a(k+1). \tag{3.28}$$

On the other hand, if we use Theorem 3.26 and Proposition 3.29, we see that if S is chosen randomly with uniform probability distribution, then with probability $a^{-2\epsilon}$,

$$|E| \cdot |S|^{\frac{3}{4}} \geq a^2 \cdot \sqrt{\frac{1 - dens(S)}{\Lambda_{\text{Salem}}}},$$

with

$$\Lambda_{\text{Salem}} \leq \sqrt{(1+\epsilon)\ln(a)}.$$

It follows that

$$|S|^{\frac{3}{4}} \geq \frac{a}{k+1}\sqrt{\frac{1 - dens(S)}{\Lambda_{\text{Salem}}}},$$

which implies that

$$|S| \geq \left(\frac{a}{k+1}\sqrt{\frac{1 - dens(S)}{\Lambda_{\text{Salem}}}}\right)^{\frac{4}{3}}.$$

This is more restrictive than (3.28) if k is small. On the other hand, if $k = \frac{a}{2}$, then Meshulam's bound is better. It is also interesting to note that by the classical uncertainty principle,

$$|S| \geq \frac{a^2}{|E|} = \frac{a^2}{a-k},$$

which is slightly weaker than Meshulam bound (3.28).

It would be interesting to work out a unified approach combining restriction and Meshulam's approach. This investigation will be conducted in the sequel.

Remark 3.31. One can use Meshulam's uncertainty principle to achieve a unique signal recovery result analogous to Donoho-Stark's as follows. Let $f : \mathbb{Z}_N \to \mathbb{C}$ be a signal with support E and a set of missing frequencies S. Assume that $d_1 \leq 2|E| \leq d_2$ and

$$|S| \leq N(d_1 d_2)^{-1}(d_1 + d_2 - 2|E|).$$

Then, f can be uniquely recovered. In the case where N is prime, the conditions for the recovery problem change to $|E| \leq \frac{N}{2}$ and the size of unobserved frequencies must be

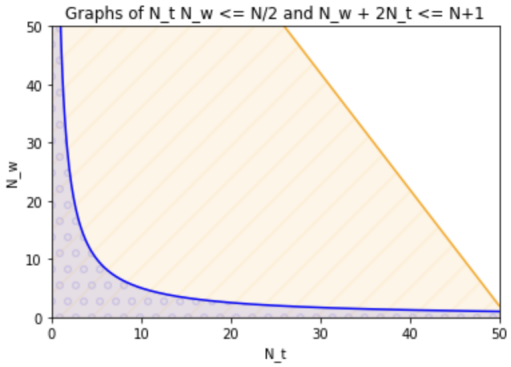

FIGURE 2. The blue dotted area represents the allowed range of missing frequencies and signal sparsity when Donoho and Stark's Uncertainty Principle (UP) is considered. Meanwhile, the striped beige area indicates the permitted range when Meshulam's as well as Tao's UP (for prime N) is taken into account.

$|S| + 2|E| \leq N + 1$. See Fig. 2 for a comparison of the allowed range for the size of sparsity and the size of absent frequencies for an exact recovery using Donoho-Stark's vs. Meshulam's uncertainty principles.

3.4. **The relationships between the parameters Λ_{size}, Λ_{Salem} and Λ_{energy}.** We are now going to exhibit some interesting relationships between the parameters we have been repeatedly using.

i) (Λ_{Salem} bound) As we noted above, the inequality

$$|\widehat{S}(z)| \leq \Lambda_{\text{Salem}} N^{-d} |S|^{\frac{1}{2}}$$

always holds for any set S with $\Lambda_{\text{Salem}} = |S|^{\frac{1}{2}}$.

ii) (Λ_{energy} bound) The inequality

$$|\{(x, y, x', y') \in S^4 : x + y = x' + y'\}| \leq \Lambda_{\text{energy}} |S|^2$$

always holds with $\Lambda_{\text{energy}} = |S|$, since we can fix x, y, x' and solve for y'.

iii) (Random Λ_{Salem} bound) It is also important to note that Proposition 3.29 implies that if S is chosen randomly and $|S| < \frac{N^d}{2}$, then with probability $1 - N^{-d\epsilon}$ we may take $\Lambda_{\text{Salem}} \leq \sqrt{(1+\epsilon)\ln(N)}$.

iv) (Λ_{Salem} versus Λ_{energy}) By a simple calculation, we have

$$\begin{aligned}\sum_z |\widehat{S}(z)|^4 &= N^{4d} \sum_{x,y,x',y'} \chi(z \cdot (x + y - x' - y')) S(x) S(y) S(x') S(y') \\ &= N^{-3d} |\{(x, y, x', y') \in S^4 : x + y = x' + y'\}|,\end{aligned}$$

i.e.,

$$|\{(x, y, x', y') \in S^4 : x + y = x' + y'\}| = N^{3d} \sum_z |\widehat{S}(z)|^4. \tag{3.29}$$

Suppose that S satisfies $|\widehat{S}(z)| \leq \Lambda_{\text{Salem}} N^{-d} \cdot |S|^{\frac{1}{2}}$ for $z \neq (0, \ldots, 0)$. By this assumption, the right-hand side of (3.29) is bounded by

$$N^{3d} \cdot \Lambda_{\text{Salem}}^2 \cdot N^{-2d} \cdot |S| \cdot \sum_z |\widehat{S}(m)|^2.$$

By Plancherel, this expression equals

$$\Lambda_{\text{Salem}}^2 \cdot |S|^2,$$

from which we conclude that

$$\Lambda_{\text{energy}} \leq \Lambda_{\text{Salem}}^2. \tag{3.30}$$

v) The calculation above shows that a good Fourier bound (small Λ_{Salem}) leads to a good energy bound (small Λ_{energy}). We are about to see that the converse is much more problematic.

Here is a sketch of an example in the prime setting, but similar examples can be constructed for any N. Let N be a large prime number, and let E denote the disjoint union of the parabola $\{x \in \mathbb{Z}_p^2 : x_2 = x_1^2\}$ and an arithmetic progression on a line of length $\approx p^\alpha$, with $0 < \alpha < \frac{2}{3}$. A direct calculation shows that

$$|\{(a, b, c, d) \in E^4 : a + b = c + d\}| \approx |E|^2$$

because rich additive properties of the arithmetic progression on a line do not interfere the poor additive properties of the parabola because the arithmetic progression is too small. Please note that this calculation requires the primality of N.

Now, $\widehat{E}(m) = \widehat{S}(m) + \widehat{L}(m)$, where S is the indicator function of the parabola, and L is the indicator function of a line. By classical Gauss sum estimates (see e.g. [22]),

$$|\widehat{S}(m)| \leq N^{-\frac{3}{2}},$$

and this estimate is exact for all m with $m_2 \neq 0$. On the other hand, it is not difficult to find m with $m_2 \neq 0$ such that $|\widehat{L}(m)| \approx |L| p^{-2} = p^{\alpha - 2}$. It follows that

$$|\widehat{E}(m)| \approx p^{-\frac{3}{2}} + p^{\alpha-2} \approx p^{\alpha-2} = p^{-\frac{3}{2}} \cdot p^{\alpha - \frac{1}{2}},$$

so

$$\Lambda_{\text{Salem}} = p^{\alpha - \frac{1}{2}}$$

as long as $\alpha > \frac{1}{2}$. On the other hand, $\Lambda_{\text{energy}} \approx 1$ in this case. This shows that the inequality (3.30) can be very far from equality.

vi) In view of Remark 3.14, in the case when S is chosen randomly, $\Lambda_{\text{energy}} \leq \Lambda_{\text{size}}^2$.

4. Signal recovery in $\mathbb{Z}_N^d$

4.1. **Exact recovery via restriction theory.** We begin with the exact recovery mechanism that follows from Theorem 3.6.

Corollary 4.1 (Exact Recovery via Restriction Estimation)**.** *Let $f : \mathbb{Z}_N^d \to \mathbb{C}$ be a signal supported in $E \subset \mathbb{Z}_N^d$. Let r be a frequency bandlimited signal such that*

$$\widehat{r}(m) = \begin{cases} \widehat{f}(m), & \text{for } m \notin S \\ 0, & \text{otherwise.} \end{cases} \tag{4.1}$$

Suppose that (3.5) holds for S, the set of unobserved frequencies of f. Then f can be reconstructed from r uniquely if

$$|E|^{\frac{1}{p}} \cdot |S| < \frac{N^d}{2^{\frac{1}{p}} C_{p,q}}. \tag{4.2}$$

This result follows from Theorem 3.6 using the Donoho-Stark mechanism described in subsection 2.1.1.

The following consequence of Theorem 3.22 is deduced using the Donoho-Stark approach described above.

Corollary 4.2 (Exact recovery in the presence of randomness)**.** *Let $f : \mathbb{Z}_N^d \to \mathbb{C}$ supported in $E \subset \mathbb{Z}_N^d$. Let r be a frequency bandlimited signal given by (4.1), where S is a subset of $\mathbb{Z}_N^d$ of size $\lceil N^{\frac{2d}{q}} \rceil$, for some $q > 2$, randomly chosen with uniform probability. Then there exists a constant $C(q)$ that depends only on q such that with probability $1 - o(1)$, if*

$$|E| < \frac{N^d}{2(C(q))^{\frac{1}{\frac{1}{2}-\frac{1}{q}}}}, \tag{4.3}$$

then f can be reconstructed from r uniquely.

Remark 4.3. The size assumption of Corollary 4.2 can easily be restated in the form $|S| = \lceil N^{d-\epsilon} \rceil$ for some $\epsilon > 0$. Then by writing $d - \epsilon = \frac{2d}{q}$, we obtain $\frac{1}{2} - \frac{1}{q} = \frac{\epsilon}{2d}$, which leads to the following variant equivalent of (4.3):

$$|E| < \frac{N^d}{(C(q))^{\frac{2d}{\epsilon}}}.$$

4.2. **DRA algorithm and recovery of 0-1 signals via restriction theory.** [1] Donoho and Stark [11] provide an algorithm for reconstructing the signal f, with a certain degree of complexity. Our observation is that in the case of $0-1$ signals, the recovery mechanism is very simple and via Direct Rounding Algorithm under more "sparsity" conditions, as we illustrate in the next theorem.

Definition 4.4 (DRA–Direct Rounding Algorithm)**.** Let $E, S \subset \mathbb{Z}_N^d$ and let $E(x)$ denote its indicator function. Suppose that the values of $\widehat{E}(m)$ are not known for $m \in S$. Let r be a frequency bandlimited signal obtained by a sharp frequency "cut-off" map $P_{\mathbb{Z}_N^d \setminus S}$:

$$r := P_{\mathbb{Z}_N^d \setminus S}(E),$$

[1] Note that there are many reasons why someone may want to transmit a higher dimensional signal. For example, a graph on N vertices can be specified via its adjacency matrix, which is an N by N matrix of 1s and 0s, which can be encoded as an indicator function of a subset of $\mathbb{Z}_N^2$ corresponding to the 1 entries in the matrix.

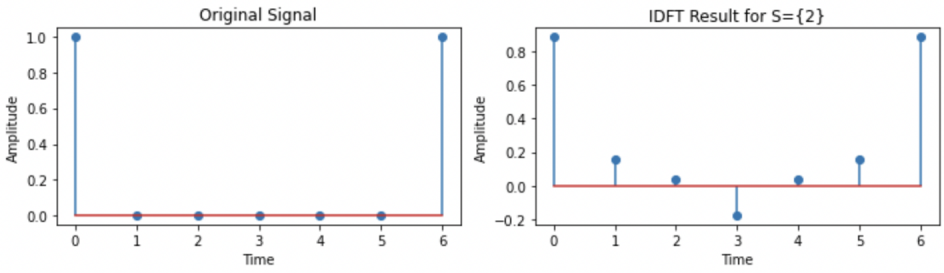

FIGURE 3. Left: Graph of original 1-bit signal. Right: Inverse discrete Fourier transform of the signal in the presence of a single missing Fourier measurement S. The recovery of original signal is obtained from DRA (or threshelding) of IDFT.

Then

$$r(x) = \sum_{m \in \mathbb{Z}_N^d \setminus S} \hat{E}(m)\chi(m \cdot x) \qquad \forall x \in \mathbb{Z}_N^d,$$

and $\widehat{r}(m) = \widehat{E}(m)$ for $m \notin S$, and 0 otherwise.

We define $G(x)$ as follows. If $|r(x)| \geq .5$, then $G(x) = 1$, otherwise $G(x) = 0$. We say that E can be recovered via the *Direct Rounding Algorithm* if $E(x) = G(x)$ for all $x \in \mathbb{Z}_N^d$.

In Figure 3, we illustrate an example of the recovery process facilitated by DRA.

The next results illustrate that the Direct Rounding Algorithm can be effectively applied for the recovery of binary signals under some specific size conditions for the sets E and S.

Theorem 4.5. *Let E be a binary signal in $\mathbb{Z}_N^d$.*

i) *Suppose that the frequencies in $S \subset \mathbb{Z}_N^d$ are unobserved. Then E can be recovered via DRA provided that*

$$|E| \cdot |S| < \frac{N^d}{4}, \tag{4.4}$$

holds.

ii) *Suppose that the frequencies in $S \subset \mathbb{Z}_N^d$ are unobserved and S satisfies the restriction estimate (3.5), then E can be recovered via DRA provided that*

$$|E|^{\frac{1}{p}} \cdot |S| < \frac{N^d}{2C_{p,q}}, \tag{4.5}$$

holds.

Proof. (i) Let $E \subset \mathbb{Z}_N^d$ and let $E(x)$ denote its indicator function, i.e., $E(x) = 1$ when $x \in E$ and $E(x) = 0$ otherwise. Suppose that $S \subset \mathbb{Z}_N^d$. We can write

$$\begin{aligned} E(x) &= \sum_{m \in \mathbb{Z}_N^d} \chi(x \cdot m)\widehat{E}(m) \\ &= \sum_{m \notin S} \chi(x \cdot m)\widehat{E}(m) + \sum_{m \in S} \chi(x \cdot m)\widehat{E}(m) = I(x) + II(x). \end{aligned} \tag{4.6}$$

Suppose that the frequencies in S are unobserved. Under the assumption (4.9), the signal E can be recovered directly via DRA. Indeed, by the Cauchy-Schwarz inequality, we estimate

the error term from above:

$$|II(x)| \leq |S|^{\frac{1}{2}} \cdot \left(\sum_{m \in S} |\widehat{E}(m)|^2 \right)^{\frac{1}{2}} \tag{4.7}$$

$$\leq |S|^{\frac{1}{2}} \cdot \left(\sum_{m \in \mathbb{Z}_N^d} |\widehat{E}(m)|^2 \right)^{\frac{1}{2}} = N^{-\frac{d}{2}} |S|^{\frac{1}{2}} \cdot |E|^{\frac{1}{2}}. \tag{4.8}$$

Notice that by the assumption (4.9) we have

$$|II(x)| < \frac{1}{2}. \tag{4.9}$$

Now, by applying DRA to $r(x) = E(x) - I(x)$, we can successfully recover the entire singal E.

We note that the DRA algorithm, described above, is executed as follows in this context. We take $I(x)$, compute its complex modulus, then round up to 1 if $|E(x) - I(x)| \geq 0.5$, and round it down to 0 otherwise. This is because $E(x)$ is equal to 1 or 0 and the error of $< \frac{1}{2}$ does not interfere with the rounding process.

(ii) With the assumption that the restriction estimation (3.5) holds for S, we proceed to adapt our previous argument as follows. We have

$$|II(x)| \leq |S|^{\frac{1}{q'}} \cdot \left(\sum_{m \in S} |\widehat{E}(m)|^q \right)^{\frac{1}{q}} = |S| \cdot \left(\frac{1}{|S|} \sum_{m \in S} |\widehat{E}(m)|^q \right)^{\frac{1}{q}}$$

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

We conclude that exact recovery via DRA is possible for $0-1$ signals under the assumption (3.5), provided that

$$|E|^{\frac{1}{p}} \cdot |S| < \frac{N^d}{2C_{p,q}}, \tag{4.10}$$

a slightly more stringent condition than the one in Corollary 4.1. □

Remark 4.6. In Theorem 4.5 (i), we achieve a very simple exact recovery process. The price that we pay for this simple algorithm is that (4.9) is more restrictive, by a factor of $\frac{1}{2}$, compared to the condition $|E| \cdot |S| < \frac{N^d}{2}$ that arises when we prove the exact recovery directly using the uncertainty principle in (3.1). The same argument holds true for (ii).

Remark 4.7. It is interesting to note that if $f : \mathbb{Z}_N^d$ has a bounded range and takes only a finite number of values, then the DRA mechanism can be applied, much like above, except that we need to bound $|II(x)|$ by $\frac{1}{2k}$ instead of $\frac{1}{2}$.

4.3. **Signal recovery via the Salem uncertainty principle.** We are now going to explore the exact recovery consequences of the Salem Uncertainty Principle (Theorem 3.26). Our main result in this direction is the following.

Theorem 4.8. *Let $f : \mathbb{Z}_N^d \to \mathbb{C}$ be a signal supported in $E \subset \mathbb{Z}_N^d$. Let r be a frequency bandlimited signal obtained by a sharp frequency "cut-off" map P_B:*

$$r := P_B(f),$$

where $P_B = \mathcal{F}^{-1}\chi_B\mathcal{F}$ and $B = \mathbb{Z}_N^d \setminus S$. Then $\widehat{r}(m) = \widehat{f}(m)$ for $m \notin S$, and 0 otherwise. Suppose that S is Salem at level Λ_{Salem}. Then f can be reconstructed from r uniquely if

$$|E| \cdot |S|^{\frac{3}{4}} < \frac{1}{2} \cdot N^d \cdot \sqrt{\frac{1 - dens(S)}{\Lambda_{Salem}}}. \tag{4.11}$$

This result follows from Theorem 3.26 using the Donoho-Stark mechanism described in Subsection 2.1.1.

Remark 4.9. In view of Proposition 3.29, we can replace the assumption on S in Theorem 4.8 by the assumption that S is chosen randomly with respect to uniform probability. Then the conclusion that f can be reconstructed from r uniquely if (4.11) holds with $\Lambda_{\text{Salem}} = \ln((1+\epsilon) \cdot d \cdot N)$ is valid with probability $1 - N^{-d\epsilon}$.

In the realm of $0-1$ signals, we can use Theorem 3.26 and run the DRA mechanism from Subsection 4.2 to obtain the following result.

Theorem 4.10. *Let $E \subset \mathbb{Z}_N^d$ and identify E with its indicator function. Let r be a frequency bandlimited signal obtained by a sharp frequency "cut-off" map P_B:*

$$r := P_B(E),$$

where $P_B = \mathcal{F}^{-1}\chi_B\mathcal{F}$ and $B = \mathbb{Z}_N^d \setminus S$. Then $\widehat{r}(m) = \widehat{E}(m)$ for $m \notin S$, and 0 otherwise. Suppose that S is Salem at level Λ_{Salem}. Then E can be reconstructed from r uniquely via the DRA if

$$|E| \cdot |S|^{\frac{3}{4}} < \frac{1}{2} \cdot N^d \cdot \sqrt{\frac{1 - dens(S)}{\Lambda_{Salem}}}.$$

5. Signal recovery in $\mathbb{R}^d$

The signal recovery problem can be set up in a very general setting, such as manifolds, hyperbolic domains, fractals, and Lie groups. We shall address this issue in the sequel, but in the meantime, we are going to provide a simple illustration of how the concepts of this paper play out in the context of the celebrated restriction conjecture in $\mathbb{R}^d$, $d \geq 2$.

In Euclidean spaces, we may consider the following version of the exact recovery problem. Let A be a subset of the unit cube, say, of positive Lebesgue measure, and let $1_A(x)$ denote its indicator function. By the inverse Fourier transform,

$$1_A(x) = \int e^{2\pi i x\cdot\xi}\ \widehat{1}_A(\xi) d\xi, \quad \forall\ x \in \mathbb{R}^d.$$

Suppose that the values of $\widehat{1}_A(\xi)$ for $\xi \in S^\delta$ are missing, where S^δ is the δ-neighborhood of $S \subset \mathbb{R}^d$.

As before, we have

$$1_A(x) = \int_{\xi \notin S^\delta} e^{2\pi i x\cdot\xi}\, \widehat{1}_A(\xi) d\xi + \int_{S^\delta} e^{2\pi i x\cdot\xi}\, \widehat{1}_A(\xi) d\xi = I + II,$$

where for some $r \in [1, \infty)$

$$|II| \leq |S^\delta| \cdot \left(\frac{1}{|S^\delta|} \int_{S^\delta} |\widehat{1}_A(\xi)|^r d\xi \right)^{\frac{1}{r}}. \tag{5.1}$$

Definition 5.1. (Restriction in $\mathbb{R}^d$) Given a compact set $S \subset \mathbb{R}^d$, and a measure σ_S supported on S, we say that a (p, r) restriction theorem holds for S if there is a constant $C_{p,r}$, depending only on p and r, such that for any function f

$$\left(\frac{1}{|S^\delta|} \int_{S^\delta} |\widehat{f}(\xi)|^r d\xi \right)^{\frac{1}{r}} \leq C_{p,r} \left(\int_{\mathbb{R}^d} |f(x)|^p dx \right)^{\frac{1}{p}} \tag{5.2}$$

with constants independent of $\delta > 0$, where $C_{p,r}$ is a uniform constant and S^δ is the δ-neighborhood of S.

Remark 5.2. Suppose that S is a compact surface and S^δ is defined as above. Note that

$$\sigma_S := \lim_{\delta \to 0^+} \frac{1}{|S^\delta|} 1_{S^\delta} \tag{5.3}$$

is the usual surface measure on S.

Moving right along, if a (p, r)- restriction theorem is valid for S^δ, with constants independent of δ (if δ is sufficiently small), the expression on the right of (5.1) above is bounded by

$$C_{p,r} |S^\delta| \cdot |A|^{\frac{1}{p}}.$$

Suppose, for example, S has the upper Minkowski dimension α. Then we conclude that

$$|II| \leq C_{p,r} \cdot \delta^{d-\alpha} \cdot |A|^{\frac{1}{p}}. \tag{5.4}$$

The restriction theorem always holds with $p = 1$, so we have

$$|II| \lesssim \delta^{d-\alpha} |A|, \tag{5.5}$$

and exact recovery is possible if $\delta^{d-\alpha}|A|$ is smaller than a sufficiently small constant. If S is a compact piece of a hyperplane, for example, it is not difficult to see that we can never obtain a (p, r) restriction estimate with $p > 1$. However, we can say much more in some specific cases, like the cases of a sphere or a paraboloid due to their curvature properties. See, for example, the discussion of restriction theory in [40]. See also [29] for the discussion of restriction for sets of fractional dimension.

Conjecture 5.3. *(Restriction conjecture) The restriction conjecture says that if S is the unit sphere, (see e.g. [40]; for a thorough description of the problem, and [43] for some recent developments) then* (5.2) *holds whenever*

$$p < \frac{2d}{d+1}, \ r \leq \frac{d-1}{d+1} p',$$

where p' is the conjugate exponent to p.

Theorem 5.4. *Suppose that the Restriction conjecture 5.3 holds. Suppose that the same estimate holds if σ_S is replaced by $\frac{1}{|S^\delta|}1_{S^\delta}$ with δ sufficiently small. Let A be a measurable subset of $\mathbb{R}^d$ and the Fourier transform of $\widehat{1}_A(\xi)$ is known, except for the δ-neighborhood of the unit sphere. Then there exists $C < \infty$, independent of δ, such that exact recovery of A is possible, up to a set of measure 0, if*

$$|A| \leq C\delta^{-p} \text{ for any } p < \frac{2d}{d+1}.$$

The proof of Theorem 5.4 follows by taking $\alpha = d-1$ and p from the Restriction conjecture in 5.3 above.

6. Proof of Theorems

Proof of Theorem 3.6. Suppose that f is supported in a set E, and $\widehat{f}$ is supported in a set Σ. Then by the Fourier Inversion Formula and the support condition,

$$f(y) = \sum_{m \in \mathbb{Z}_N^d} \chi(y \cdot m)\widehat{f}(m) = \sum_{m \in \Sigma} \chi(y \cdot m)\widehat{f}(m)$$

By Hölder's inequality,

$$|f(y)| \leq |\Sigma| \cdot \left(\frac{1}{|\Sigma|} \sum_{m \in \Sigma} |\widehat{f}(m)|^q \right)^{\frac{1}{q}}.$$

By restriction bound assumption (3.5), this expression is bounded by

$$|\Sigma| \cdot C_{p,q} \cdot N^{-d} \cdot \left(\sum_{x \in \mathbb{Z}_N^d} |f(x)|^p \right)^{\frac{1}{p}},$$

and by the support assumption, this quantity is equal to

$$|\Sigma| \cdot C_{p,q} \cdot N^{-d} \cdot \left(\sum_{x \in E} |f(x)|^p \right)^{\frac{1}{p}}.$$

Putting everything together, we see that

$$|f(y)| \leq |\Sigma| \cdot C_{p,q} \cdot N^{-d} \cdot \left(\sum_{x \in E} |f(x)|^p \right)^{\frac{1}{p}} \quad \forall\ y \in E.$$

Raising both sides to the power of p, summing over E, and dividing both sides of the resulting inequality by $\sum_{x \in E} |f(x)|^p$, we obtain

$$|\Sigma|^p \cdot |E| \cdot C_{p,q}^p \geq N^{dp},$$

or, equivalently,

$$|E|^{\frac{1}{p}} \cdot |\Sigma| \geq \frac{N^d}{C_{p,q}},$$

as desired.

□

Proof of Theorem 3.7. To simplify the presentation, we introduce the following notation. Given $f : \mathbb{Z}_N^d \to \mathbb{C}$ and a set $A \subset \mathbb{Z}_N^d$, define

$$||f||_{L^p(A)} = \left(\sum_{x \in A} |f(x)|^p \right)^{\frac{1}{p}}, \tag{6.1}$$

and

$$||f||_{L^p(\mu_A)} = \left(\frac{1}{|A|} \sum_{x \in A} |f(x)|^p \right)^{\frac{1}{p}}. \tag{6.2}$$

Note that (6.2) is defined in (3.19) in the case $A = \mathbb{Z}_N^d$.

Observe that if $1 \leq a \leq b$, then by Hölder's inequality,

$$||f||_{L^a(\mu_A)} \leq ||f||_{L^b(\mu_A)}. \tag{6.3}$$

Similarly, if $1 \leq a \leq b$,

$$||f||_{L^a(A)} = |A|^{\frac{1}{a}} ||f||_{L^a(\mu_A)} \leq |A|^{\frac{1}{a}} ||f||_{L^b(\mu_A)} = |A|^{\frac{1}{a}-\frac{1}{b}} ||f||_{L^b(A)}. \tag{6.4}$$

In this notation, (p, q) restriction theorem can be rephrased in the form

$$||\widehat{f}||_{L^q(\mu_S)} \leq C_{p,q} N^{-d} ||f||_{L^p(\mathbb{Z}_N^d)}. \tag{6.5}$$

Suppose that f is supported in E and $\widehat{f}$ is supported in S. Also, suppose that (6.5) holds. There are two cases.

Case 1: $q \geq 2$. By (6.3)

$$||\widehat{f}||_{L^2(\mu_S)} \leq ||\widehat{f}||_{L^q(\mu_S)}, \tag{6.6}$$

which implies that if (6.5) holds with exponents (p, q) and constant $C_{p,q}$, it also holds with exponents $(p, 2)$ and constant $C_{p,q}$.

Since $\widehat{f}$ is supported in S and f is supported in E,

$$||\widehat{f}||_{L^2(\mu_S)} = |S|^{-\frac{1}{2}} ||\widehat{f}||_{L^2(S)} = |S|^{-\frac{1}{2}} ||\widehat{f}||_{L^2(\mathbb{Z}_N^d)} = |S|^{-\frac{1}{2}} N^{-\frac{d}{2}} ||f||_{L^2(\mathbb{Z}_N^d)} = |S|^{-\frac{1}{2}} N^{-\frac{d}{2}} ||f||_{L^2(E)}.$$

By (6.6) and (6.5),

$$|S|^{-\frac{1}{2}} N^{-\frac{d}{2}} ||f||_{L^p(E)} \leq C_{p,q} N^{-d} ||f||_{L^p(E)} \leq C_{p,q} N^{-d} |E|^{\frac{1}{p}-\frac{1}{2}} ||f||_{L^2(E)}$$

by (6.3) and (6.4). It follows that

$$|S|^{-\frac{1}{2}} N^{-\frac{d}{2}} ||f||_{L^2(E)} \leq C_{p,q} N^{-d} |E|^{\frac{1}{p}-\frac{1}{2}} ||f||_{L^2(E)}.$$

Cancelling $||f||_{L^2(E)}$ on both sides and rearranging, we obtain part i) of Theorem 3.7.

Case 2: $q \leq 2$. We shall need the Hausdorff-Young inequality (see e.g. [34] in the generality of locally compact abelian groups), i.e if $1 \leq p \leq 2$,

$$||\widehat{f}||_{L^{p'}(\mathbb{Z}_N^d)} \leq N^{-\frac{d}{p}}||f||_{L^p(\mathbb{Z}_N^d)}. \tag{6.7}$$

As usual, the case $p = 1$ follows by the triangle inequality, the case $p = 2$ is Plancherel, and the rest is a consequence of the Riesz-Thorin interpolation inequality (see e.g. [40], [5]).

Note that if $g = \widehat{f}$, then $\widehat{g}(x) = N^{-d}f(-x)$. It follows that the left-hand side of (6.5) is bounded from below by

$$|S|^{-\frac{1}{q}}N^{\frac{d}{q}}N^{-d}\left(\sum_{x\in\mathbb{Z}_N^d}|f(-x)|^{q'}\right)^{\frac{1}{q'}} = |S|^{-\frac{1}{q}}N^{-\frac{d}{q'}}||f||_{L^{q'}(E)},$$

where the last step follows by a change of variables $x \to -x$ and the assumption that f is supported in E.

Putting everything together and using (6.3) and (6.4) once again, we see that

$$|S|^{-\frac{1}{q}}N^{-\frac{d}{q'}}||f||_{L^{q'}(E)} \leq C_{p,q}N^{-d}||f||_{L^p(E)} \leq C_{p,q}|E|^{\frac{1}{p}-\frac{1}{q'}}N^{-d}||f||_{L^{q'}(E)}.$$

Cancelling $||f||_{L^{q'}(E)}$ and rearranging, we obtain part ii) of Theorem 3.7. This completes the proof.

□

Proof of Theorem 3.12. We have

$$\sum_{m\in\Sigma}|\widehat{f}(m)|^2 = \sum_{m\in\mathbb{Z}_N^d}|\widehat{f}(m)|^2\Sigma(m) \tag{6.8}$$

$$= \sum_{m\in\mathbb{Z}_N^d}\widehat{f}(m)\Sigma(m)g(m), \tag{6.9}$$

where

$$g(m) = \overline{\widehat{f}(m)}\Sigma(m).$$

By definition of the Fourier transform, the right-hand side of (6.9) is equal to

$$N^{-d}\sum_m\sum_x\chi(-x\cdot m)f(x)\Sigma(m)g(m)$$

$$= \sum_x f(x)\widehat{g\Sigma}(x). \tag{6.10}$$

By Hölder's inequality, the quantity in (6.10) is bounded by

$$\left(\sum_{x\in\mathbb{Z}_N^d}|f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}}\cdot\left(\sum_{x\in\mathbb{Z}_N^d}|\widehat{g\Sigma}(x)|^4\right)^{\frac{1}{4}}. \tag{6.11}$$

Continuing, we have

$$\sum_{x\in\mathbb{Z}_N^d} |\widehat{g\Sigma}(x)|^4 =$$
$$= N^{-4d} \sum_x \sum_{m_1,m_2,m_3,m_4\in\Sigma} \chi(x\cdot(m_1+m_2-m_3-m_4)) g(m_1)g(m_2)g(m_3)g(m_4)$$
$$= N^{-3d} \sum_{m_1+m_2=m_3+m_4;\ m_j\in\Sigma} g(m_1)g(m_2)g(m_3)g(m_4).$$

The modulus of this expression is bounded by

$$\Lambda_{\text{energy}} \cdot N^{-3d} \cdot \left(\sum_m |g(m)|^2\right)^2.$$

To see this, we use a similar idea in [27], page 11: we take g to be a linear combination of indicator functions of sets, then apply the Cauchy-Schwartz and the assumption (3.15).

Going back, we see that the expression is bounded by

$$\left(\sum_{x\in\mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}} \cdot \Lambda_{\text{energy}}^{\frac{1}{4}} \cdot N^{-\frac{3d}{4}} \cdot \left(\sum_m |g(m)|^2\right)^{\frac{1}{2}}.$$

If we go back to (6.8), and unravel the definitions, we see that

$$\sum_m |g(m)|^2 \le \left(\sum_{x\in\mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}} \cdot \Lambda_{\text{energy}}^{\frac{1}{4}} \cdot N^{-\frac{3d}{4}} \cdot \left(\sum_m |g(m)|^2\right)^{\frac{1}{2}},$$

hence

$$\left(\frac{1}{|\Sigma|}\sum_{m\in\Sigma} |\widehat{f}(m)|^2\right)^{\frac{1}{2}} \le \left(\sum_{x\in\mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}} \cdot \frac{1}{|\Sigma|^{\frac{1}{2}}} \cdot \Lambda_{\text{energy}}^{\frac{1}{4}} \cdot N^{-\frac{3d}{4}}$$
$$= \Lambda_{\text{energy}}^{\frac{1}{4}} \cdot N^{-d} \cdot \left(\sum_{x\in\mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}} \cdot \frac{N^{\frac{d}{4}}}{|\Sigma|^{\frac{1}{2}}}$$
$$= \Lambda_{\text{size}}^{-\frac{1}{2}} \cdot \Lambda_{\text{energy}}^{\frac{1}{4}} \cdot N^{-d} \cdot \left(\sum_{x\in\mathbb{Z}_N^d} |f(x)|^{\frac{4}{3}}\right)^{\frac{3}{4}},$$

as claimed. □

Proof of Proposition 3.20. We have

$$|\Sigma|^{-1} \sum_{m\in S} |\widehat{f}(m)|^2 = \sum_m \widehat{f}(m)\Sigma(m)g(m)\Sigma(m),$$

where $g(m) = \overline{\widehat{f}(m)}$. We shall use definitions (6.1), (6.2), and (3.19) throughout.

This expression equals

$$\sum_x f(x)\widehat{g\Sigma}(x),$$

and the modulus of this expression is bounded by

$$\begin{aligned}
&||f||_{L^{q'}(\mathbb{Z}_N^d)} \cdot ||\widehat{g\Sigma}||_{L^q(\mathbb{Z}_N^d)} \cdot |\Sigma|^{-1} \\
&= N^{\frac{d}{q'}} \cdot ||f||_{L^{q'}(\mu)} \cdot N^{\frac{d}{q}} \cdot ||\widehat{g\Sigma}||_{L^q(\mu)} \cdot |\Sigma|^{-1} \\
&\leq N^d \cdot ||f||_{L^{q'}(\mu)} \cdot C(q) \cdot ||\widehat{g\Sigma}||_{L^2(\mu)} \cdot |\Sigma|^{-1} \\
&N^d \cdot ||f||_{L^{q'}(\mu)} \cdot C(q) \cdot ||\widehat{g\Sigma}||_{L^2(\mathbb{Z}_N^d)} \cdot N^{-\frac{d}{2}} \cdot |\Sigma|^{-1} \\
&= ||f||_{L^{q'}(\mu)} \cdot C(q) \cdot ||g\Sigma||_{L^2(\mathbb{Z}_N^d)} \cdot |\Sigma|^{-1} \\
&= ||f||_{L^{q'}(\mu)} \cdot C(q) \cdot \left(\frac{1}{|\Sigma|} \sum_{m \in \Sigma} |\widehat{f}(m)|^2 \right)^{\frac{1}{2}} \cdot |\Sigma|^{-\frac{1}{2}} \\
&= N^{-\frac{d}{q'}} \cdot ||f||_{L^{q'}(\mathbb{Z}_N^d)} \cdot C(q) \cdot \left(\frac{1}{|\Sigma|} \sum_{m \in \Sigma} |\widehat{f}(m)|^2 \right)^{\frac{1}{2}} \cdot |\Sigma|^{-\frac{1}{2}} \\
&= C(q) \left(\frac{N^{\frac{2d}{q}}}{|\Sigma|} \right)^{\frac{1}{2}} N^{-d} ||f||_{L^{q'}(\mathbb{Z}_N^d)},
\end{aligned}$$

which completes the proof.

□

Proof of Theorem 3.22. It is not difficult to see that we may write $f(x)$ in the form

$$\sum_{i=1}^n c_i 1_{E_i}(x),$$

where $\{E_i\}$ is a disjoint collection of subsets of $\mathbb{Z}_N^d$. Note that

$$E \equiv \cup_{i=1}^n E_i$$

is the support of f.

A direct calculation shows that

$$||f||_{L^p(\mu)} = N^{-\frac{d}{q}} \cdot \left(\sum_{i=1}^n |c_i|^q |E_i| \right)^{\frac{1}{q}}. \tag{6.12}$$

By Theorem 3.18, the estimate (3.18) holds. Plugging in (6.12) yields

$$N^{-\frac{d}{q}} \cdot \left(\sum_{i=1}^n |c_i|^q |E_i| \right)^{\frac{1}{q}} \leq \lambda \cdot C(q) N^{-\frac{d}{2}} \cdot \left(\sum_{i=1}^n |c_i|^2 |E_i| \right)^{\frac{1}{2}}. \tag{6.13}$$

Let $w_i = \frac{|E_i|}{|E|}$. Observe that

$$\sum_{i=1}^n w_i = 1.$$

We may rewrite inequality (6.13) in the form

$$|E|^{\frac{1}{2}-\frac{1}{q}} \cdot \frac{\left(\sum_{i=1}^n |c_i|^2 w_i\right)^{\frac{1}{2}}}{\left(\sum_{i=1}^n |c_i|^q w_i\right)^{\frac{1}{q}}} \cdot \lambda \cdot C(q) \geq (N^d)^{\frac{1}{2}-\frac{1}{q}}.$$

By Holder's inequality, the left-hand side is bounded above by $|E|^{\frac{1}{2}-\frac{1}{p}} C(p)$, and we see that

$$|E|^{\frac{1}{2}-\frac{1}{q}} \lambda \cdot C(q) \geq (N^d)^{\frac{1}{2}-\frac{1}{q}}.$$

Taking the roots of both sides yields the conclusion of the theorem.

□

Proof of Theorem 3.26. By Fourier Inversion,

$$f(x) = \sum_{m \in S} \chi(x \cdot m) \widehat{f}(m).$$

It follows that

$$|f(x)| \leq |S| \cdot \left(\frac{1}{|S|} \sum_{m \in S} |\widehat{f}(m)|^2 \right)^{\frac{1}{2}}.$$

We have

$$\sum_{m \in S} |\widehat{f}(m)|^2 = \sum_{m \in S} |\widehat{f}(m)|^2 S_0(m) + \frac{|S|}{N^d} \sum_{m \in S} |\widehat{f}(m)|^2,$$

where $S_0(m) = S(m) - \frac{|S|}{N^d}$.

It follows that

(6.14)

$$(1 - dens(S)) \sum_{m \in S} |\widehat{f}(m)|^2 = \sum_m |\widehat{f}(m)|^2 S_0(m)$$

$$= N^{-d} \sum_{x,y} \bar{f}(x) f(y) \widehat{S}_0(x-y) \leq N^{-d} \cdot \Lambda_{\text{Salem}} \cdot \frac{|S|^{\frac{1}{2}}}{N^d} \cdot \left(\sum_x |f(x)| \right)^2.$$

We deduce that

$$\left(\frac{1}{|S|} \sum_{m \in S} |\widehat{f}(m)|^2 \right)^{\frac{1}{2}} \leq \frac{N^{-d} \cdot |S|^{-\frac{1}{4}} \cdot \Lambda_{\text{Salem}}^{\frac{1}{2}} \cdot \sum_x |f(x)|}{\sqrt{1 - dens(S)}}.$$

Putting everything together, we see that

$$|f(x)| \leq \frac{1}{N^d} \cdot |S|^{\frac{3}{4}} \cdot \Lambda_{\text{Salem}}^{\frac{1}{2}} \cdot \sum_x |f(x)| \cdot \frac{1}{\sqrt{1 - dens(S)}}.$$

Summing both sides over $x \in E$, using the assumption that f is supported in E, and dividing both sides by $\sum_{x \in E} |f(x)|$, we obtain the conclusion of the theorem. This completes the proof. □

Proof of Theorem 4.10. We have

$$E(x) = \sum_m \chi(x \cdot m)\widehat{E}(m) \tag{6.15}$$
$$= \sum_{m \notin S} \chi(x \cdot m)\widehat{E}(m) + \sum_{m \in S} \chi(x \cdot m)\widehat{E}(m)$$
$$= I(x) + II(x).$$

By Cauchy-Schwarz,

$$|II(x)| \leq |S| \cdot \left(\frac{1}{|S|} \sum_{m \in S} |\widehat{E}(m)|^2 \right)^{\frac{1}{2}}.$$

By the proof of Theorem 3.26 above,

$$|S| \cdot \left(\frac{1}{|S|} \sum_{m \in S} |\widehat{E}(m)|^2 \right)^{\frac{1}{2}}$$
$$\leq \frac{1}{N^d} \cdot |S|^{\frac{3}{4}} \cdot \Lambda_{\text{Salem}}^{\frac{1}{2}} \cdot |E| \cdot \frac{1}{\sqrt{1 - dens(S)}}.$$

We need this quantity to be $< \frac{1}{2}$ and the desired conclusion follows using the reasoning laid out in Subsection 4.2.

□

References

[1] N. Alon, Y. Matias, and M. Szegedy, *The Space Complexity of Approximating the Frequency Moments*, J. Comput. System Sci., **58** (1):137-147, (1999). 4

[2] L. Babai, *The Fourier transform and equations over abelian groups*, Lecture Notes, University of Chicago, (2002). 3, 13

[3] R. Berinde, A. Gilbert, P. Indyk, H. Karloff, and M. Strauss, *Combining geometry and combinatorics: a unified approach to sparse signal recovery*, Allerton, (2008). 4

[4] J. Bourgain, *Bounded orthogonal systems and the $\Lambda(p)$-set problem*, Acta Math. **162** (1989), no. 3-4, 227–245. 10

[5] C. Bennett and R. Sharpley, *Interpolation of operators*, **129**, Pure and Applied Mathematics, Academic Press, Inc., Boston, MA, (1988). 24

[6] Ciletti, Michael D., and M. Morris Mano, *Digital design*. Hoboken: Prentice-Hall, 2007. 4

[7] E. J. Candes and J. Romberg, *Recovery of Sparse Signals via Convex Programming*, (2005). Available at: http://www.acm.caltech.edu/l1magic. 4

[8] E. J. Candes, J. Romberg, and T. Tao, *Stable signal recovery from incomplete and inaccurate measurements*, Comm. Pure Appl. Math., 59(8):1208–1223, (2006). 4

[9] D. Ryou, *A variant of the $\Lambda(p)$ -set problem in Orlicz spaces*, Math. Z. **302** (2022), no. 4, 2545-2566. 12

[10] S. Dyatlov, *An introduction to fractal uncertainty principle.* Journal of Mathematical Physics 60.8 (2019). 4

[11] D. Donoho and P. Stark, *Uncertainty principle and signal processing*, SIAM Journal of Applied Math., (1989), Society for Industrial and Applied Mathematics, volume 49, No. 3, pp. 906-931. 1, 3, 17

[12] A. Dubickas, T. Schoen, M. Silva, and P. Sarka, *Finding large co-Sidon subsets in sets with a given additive energy*, (English summary) European J. Combin. **34** (2013), no.7, 1144-1157. 9

[13] T. Fallon, G. Kiss, and G. Somlai, *Spectral sets and tiles in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$*, J. Funct. Anal. 282 (2022), no. 12, Paper No. 109472, 16 pp. 5

[14] T. Fallon, A. Mayeli, and D. Villano, *The Fuglede Conjecture holds in $\mathbb{Z}_p^3$ for $p = 5, 7$*, (2019), arXiv:1902.02936. 5

[15] Gonzalez, Rafael C., and Richard E. Woods, *Digital Image Processing, Hoboken.* NJ: Pearson (2018). 4

[16] C. Haessig, A. Iosevich, J. Pakianathan, S. Robins, and L. Vaicunas, *Tiling, circle packing and exponential sums over finite fields*, Anal. Math. **44** (2018), no. 4, 433–449. 5

[17] J. Hickman and J. Wright, *The Fourier Restriction and Kakeya Problems over Rings of Integers Modulo N*, Discrete Analysis, (2018), 54 pages. 7, 9

[18] A. Iosevich and D. Koh, *Extension theorems for the Fourier transform associated with nondegenerate quadratic surfaces in vector spaces over finite fields*, *Illinois J. Math.* **52** (2008), no. 2, 611–628. MR2524655. 9

[19] A. Iosevich and D. Koh, *Extension theorems for paraboloids in the finite field setting*, *Math. Z.* **266** (2010), no. 2, 471–487. MR2678639. 7

[20] A. Iosevich and D. Koh, *Extension theorems for spheres in the finite field setting*, *Forum Math.* **22** (2010), no. 3, 457–483. MR2652707. 7

[21] A. Iosevich, D. Koh, and Mark Lewko, *Finite field restriction estimates for the paraboloid in high even dimensions*, Preprint: arXiv:1712.05549. MR3771037. 7

[22] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. **359** (2007), no. 12, 6127–6142. 16

[23] A. Israel and A. Mayeli, *On the eigenvalue distribution of spatio-spectral limiting operators in higher dimensions*, Applied and Computational Harmonic Analysis 70 (2024): 101620 4, 6

[24] A. Iosevich, A. Mayeli, and J. Pakianathan, *The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$*, Anal. PDE 10 (2017), no. 4, 757–764. 5

[25] Janert, Philipp K, *Data analysis with open source tools: a hands-on guide for programmers and data scientists.* O'Reilly Media, Inc., 2010. 4

[26] H.J. Landau and H.O. Pollak, *Prolate spheroidal wave functions, Fourier analysis, and uncertainty – II*, Bell Systems Tech. J., vol. 40, no. 1, pp. 65–84, 1961. 4

[27] D. Koh and T. Pham, *A spherical extension theorem and applications in positive characteristic*, (2022), (arXiv:2008.08279). 25

[28] R. Meshulam, *An uncertainty inequality for finite abelian groups*, European J. Combin. **27** (2006), no. 1, 63-67. 14
[29] G. Mockenhaupt, *Salem sets and restriction properties of Fourier transforms*, Geom. Funct. Anal. 10 (2000), no. 6, 1579-1587. 21
[30] G. Mockenhaupt and T. Tao, *Restriction and Kakeya phenomena for finite fields*, *Duke Math. J.* **121** (2004), no. 1, 35–74. MR2031165. 7, 13
[31] W. Rudin, *Fourier analysis on groups*, Wiley Classics Library, (1962). 3
[32] M. Rudelson and R. Veshynin, *Sparse reconstruction by convex relaxation: Fourier and Gaussian measurements*, In Proc. 40th Ann. Conf. Information Sciences and Systems, Princeton, Mar. (2006). 4
[33] M. Rudelson and R. Vershynin, *On sparse reconstruction from Fourier and Gaussian measurements*, Comm. Pure Appl. Math. 61 (2008), no. 8, 1025-1045. 4
[34] W. Rudin, *Fourier analysis on groups*, Interscience Tracts in Pure and Applied Mathematics, No. 12. Interscience Publishers (a division of John Wiley & Sons, Inc.), New York-London, (1962). 24
[35] R. Salem, *On singular monotonic functions whose spectrum has a given Hausdorff dimension*, Ark. Mat. **1** (1950), 353—365. 12
[36] Schneier, Bruce, *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, (2007). 4
[37] D. Slepian and H.O. Pollak, *Prolate spheroidal wave functions, Fourier analysis, and uncertainty – I*, Bell Systems Tech. J., Volume: 40, Issue: 1, pages: 43–64, January 1961. 4
[38] K.T. Smith, *The uncertainty principle on groups*, SIAM J. Apl. Math. 50 (1990), 876–882. 3
[39] W. Stallings, *Cryptography and network security*, 4/E. Pearson Education India, 2006. 4
[40] E. M. Stein, *Harmonic Analysis*, Princeton University Press, (1993). 21, 24
[41] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Mathematical Research Letters, Volume 12 (2005), Number 1, pages 121-127. 3, 4, 5, 14
[42] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Mathematical Society Student Texts. Cambridge: Cambridge University Press, 1999. 3
[43] H. Wang, *A restriction estimate in* $\mathbb{R}^3$ *using brooms*, Duke Math. J. **171** (2022), no. 8, 1749-1822. 21
[44] H. Weyl, *Gruppentheorie und Quantenmechanik*, Hirzel-Verlag, Leipzig, 1928. 4

Department of Mathematics, University of Rochester, Rochester, NY
Email address: iosevich@gmail.com

Department of Mathematics, CUNY Graduate Center, New York, NY
Email address: amayeli@gc.cuny.edu