


On Fourier Analysis of Sparse Boolean Functions over Certain Abelian Groups

Sourav Chakraborty ✉ 


Indian Statistical Institute Kolkata, India

Swarnalipa Datta ✉

Indian Statistical Institute Kolkata, India

Pranjal Dutta ✉ 

National University of Singapore, Singapore

Arijit Ghosh ✉ 

Indian Statistical Institute Kolkata, India

Swagato Sanyal ✉ 

Indian Institute of Technology Kharagpur, India

Abstract

Given an Abelian group \mathcal{G} , a Boolean-valued function $f : \mathcal{G} \rightarrow \{-1, +1\}$, is said to be s -sparse, if it has at most s -many non-zero Fourier coefficients over the domain \mathcal{G} . In a seminal paper, Gopalan et al. [15] proved “Granularity” for Fourier coefficients of Boolean valued functions over \mathbb{Z}_2^n , that have found many diverse applications in theoretical computer science and combinatorics. They also studied structural results for Boolean functions over \mathbb{Z}_2^n which are *approximately Fourier-sparse*. In this work, we obtain structural results for approximately Fourier-sparse Boolean valued functions over Abelian groups \mathcal{G} of the form, $\mathcal{G} := \mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_t}^{n_t}$, for distinct primes p_i . We also obtain a lower bound of the form $1/(m^2 s)^{\lceil \varphi(m)/2 \rceil}$, on the absolute value of the *smallest* non-zero Fourier coefficient of an s -sparse function, where $m = p_1 \cdots p_t$, and $\varphi(m) = (p_1 - 1) \cdots (p_t - 1)$. We carefully apply probabilistic techniques from [15], to obtain our structural results, and use some non-trivial results from algebraic number theory to get the lower bound.

We construct a family of at most s -sparse Boolean functions over \mathbb{Z}_p^n , where $p > 2$, for arbitrarily large enough s , where the minimum non-zero Fourier coefficient is $o(1/s)$. The “Granularity” result of Gopalan et al. implies that the absolute values of non-zero Fourier coefficients of any s -sparse Boolean valued function over \mathbb{Z}_2^n are $\Omega(1/s)$. So, our result shows that one *cannot* expect such a lower bound for general Abelian groups.

Using our new structural results on the Fourier coefficients of sparse functions, we design an efficient sparsity testing algorithm for Boolean function, which tests whether the given function is s -sparse, or ϵ -far from any sparse Boolean function, and it requires $\text{poly}((ms)^{\varphi(m)}, 1/\epsilon)$ -many queries. Further, we generalize the notion of *degree* of a Boolean function over an Abelian group \mathcal{G} . We use it to prove an $\Omega(\sqrt{s})$ lower bound on the query complexity of any adaptive sparsity testing algorithm.

2012 ACM Subject Classification Mathematics of computing; Theory of computation

Keywords and phrases Fourier coefficients, sparse, Abelian, granularity

Digital Object Identifier 10.4230/LIPIcs.MFCS.2024.40

Related Version *Full Version*: <https://arxiv.org/abs/2406.18700> [7]

Funding *Sourav Chakraborty*: Supported by the Science & Engineering Research Board of the DST, India, through the MATRICS grant MTR/2021/000318.

Pranjal Dutta: Supported by the project “Foundation of Lattice-based Cryptography”, funded by NUS-NCS Joint Laboratory for Cyber Security, Singapore.

Arijit Ghosh: Arijit Ghosh is partially supported by the Science & Engineering Research Board of the DST, India, through the MATRICS grant MTR/2023/001527.



© Sourav Chakraborty, Swarnalipa Datta, Pranjal Dutta, Arijit Ghosh, and Swagato Sanyal; licensed under Creative Commons License CC-BY 4.0

49th International Symposium on Mathematical Foundations of Computer Science (MFCS 2024).

Editors: Rastislav Kráľovič and Antonín Kučera; Article No. 40; pp. 40:1–40:16

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Boolean functions are fundamental objects of study in computer science. For a discrete domain \mathcal{D} , a Boolean function $f : \mathcal{D} \rightarrow \{+1, -1\}$ models a decision task where each member of \mathcal{D} is classified into one of two classes. Boolean functions play a vital role in the study of digital circuits and computer hardware. They are also significant in the study of algorithms and complexity, particularly in problems where the set \mathcal{D} of instances is endowed with an algebraic structure. Examples of such problems include matrix multiplication and polynomial evaluation.

The case of Boolean function complexity with $\mathcal{D} = \mathbb{Z}_2^n$ has been widely studied. These functions are often analyzed in connection with their Fourier transform (see Section 2) and a significant amount of research has focused on the structural properties of Fourier spectra of important classes of these functions. One such class that this work focuses on is that of Fourier-sparse functions. These are functions with only a few non-zero Fourier coefficients, formally defined in Definition 18. We will denote by s_f the Fourier sparsity of a Boolean function f . Fourier sparsity and Fourier-sparse functions have known connections with a variety of areas of Boolean function analysis and computational complexity like property testing [15], learning theory [20, 3], distance estimation [35] and communication complexity [23, 31, 19, 27, 22]. These connections provide enough motivation to comprehend the structure of Fourier coefficients for Fourier-sparse Boolean functions.

In this work, we extend the study of Fourier-sparse Boolean functions to the domains \mathcal{D} , which are Abelian groups of the form $\mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_t}^{n_t}$, where p_1, \dots, p_t are distinct prime numbers. Boolean functions over general Abelian groups have been studied in both mathematics and computer science. A celebrated result regarding such functions is Chang’s Lemma [10]. Chang’s lemma over \mathbb{Z}_2^n has found numerous applications in complexity theory and algorithms [5, 9], analysis of Boolean functions [16, 31], communication complexity [31, 21], extremal combinatorics [13], and many more. Recently, [8] improved Chang’s lemma over \mathbb{Z}_2^n for some special settings of parameters, where Fourier sparsity played a crucial role. One motivation to study Fourier sparsity over a broader class of Abelian groups is to investigate possible generalizations of their bounds to those groups.

Fourier analysis over finite Abelian groups in cryptography. For the past three decades, the field of cryptography has been utilizing concepts derived from Fourier analysis, specifically over finite Abelian groups. Akavia, Goldwasser, and Safra [2] have combined some of these concepts to develop a comprehensive algorithm that can detect “large” Fourier coefficients of any concentrated function on finite Abelian groups, and compute a *sparse approximation* for the same. This algorithm has gained significant attention within the cryptography community, especially regarding the notion of “bit security” of the *discrete logarithm problem* (DLP), RSA, and learning with errors (LWE) problems; see [25, 14, 1]. In particular, the “nice” structural results on the Fourier coefficients of a Boolean-valued function over the general Abelian group are of utmost importance and interest from a crypto-theoretic point of view.

Interestingly, there are strong relationships between learning, sparsity, and sampling, in the context of Fourier-sparse Boolean functions. They have been rigorously studied in [28, 29, 30]. In [28], the authors asked the following:

► **Question 1.1.** *What can be said about the structure of the Fourier coefficients of a Boolean function f over an Abelian group $\mathcal{G} = \mathbb{Z}_p^n$, where the support is significantly smaller compared to \mathcal{G} ?*

Gopalan et al. [15] proved that any non-zero Fourier coefficient of a Boolean function over \mathbb{Z}_2^n with Fourier sparsity at most s_f , is *at least* $\frac{1}{s_f}$ in its absolute value. This gave a satisfactory answer of Question 1.1 over \mathbb{Z}_2^n . Furthermore, they proved *robust versions* of their result for functions which are *approximately Fourier-sparse*. Finally, their structural results were used to design a sample-efficient algorithm to test whether a function is Fourier-sparse.

In our work, we undertake the same task for Boolean functions over Abelian groups of the form \mathbb{Z}_p^n , for a prime $p \geq 3$. We prove lower bounds on the absolute value of any non-zero coefficient in terms of s_f and p . We also prove a tightness result that complements our lower bounds. In particular, our bound implies that a lower bound of $\frac{1}{\Theta(s_f)}$ that [15] showed *does not* hold anymore for \mathbb{Z}_p^n . Finally, we use our bounds to design a testing algorithm for Fourier-sparse Boolean functions over $\mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_t}^{n_t}$. This is probably the first time, we have advanced on understanding some structure on the Fourier-sparse coefficients over a general Abelian group, and shed some light on Question 1.1.

It is well-known that any Abelian group is isomorphic to a group of the form $\mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_t}^{n_t}$ where p_1, \dots, p_t are prime numbers and n_1, \dots, n_t are positive integers. Unfortunately, our techniques fall short of handling even a simpler case of \mathbb{Z}_{p^2} , fundamentally because of the *absence of a linear structure* on the solution space of systems of equations over \mathbb{Z}_{p^2} . Therefore, we are leaving the task of investigating the existence of similar bounds and algorithmic results when the domain of the function is a general Abelian group to future research.

Why care about Fourier-sparse Boolean functions over Abelian groups?

There has been a considerable amount of interest in studying the complexity of reconstructing or learning functions of the form $f : \mathcal{D} \rightarrow \mathbb{C}$, where \mathcal{D} is a known domain (more general than a hypercube, such as a general finite Abelian group), and f is Fourier-sparse; see [30, 26, 24, 11, 34]. Fourier-sparse functions over various finite Abelian groups have gained much interest with the advancement in sparse Fourier transform algorithms [17, 18, 4]. These algorithms improve the efficiency of the standard Fast Fourier Transform algorithms by taking advantage of the sparsity itself. To reliably use sparse Fourier transform algorithms, it is beneficial to have a way to *test* if a function is s -sparse or, more generally, to *estimate* the distance of a function to the closest s -sparse function. In this work, we consider the problem of non-tolerant sparsity-testing of Boolean functions over finite Abelian groups.

Finally, apart from mathematical curiosity and potential cryptographic applications (as mentioned previously), structural results on Fourier-sparse functions $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, for some $N \in \mathbb{N}$, have also found algorithmic applications in SOS-optimization and control theory. These applications have further implications in certifying maximum satisfiability (MAX-SAT) and maximum k -colorable subgraph (MkCS) problems; see [12, 33, 32].

1.1 Our results

Throughout the article, we will be working with the Abelian group $\mathcal{G} := \mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_t}^{n_t}$ where p_i are primes. Let $f : \mathcal{G} \rightarrow \{-1, +1\}$, and $f(x) = \sum_{\chi \in \hat{\mathcal{G}}} \hat{f}(\chi) \chi(x)$ be the Fourier transform of f , where $\hat{\mathcal{G}}$ is the set of characters of the Abelian group \mathcal{G} .

We say a Boolean function is s -sparse, if it has at most s non-zero Fourier coefficients. [15] proved that for any s -sparse Boolean functions over \mathbb{Z}_2^n , the magnitude of the Fourier coefficients are k -granular where $k = \lceil \log_2 s \rceil + 1$. A real number is k -granular if it is an integer multiple of $1/2^k$. One wonders whether such a phenomenon still holds over a more general group \mathcal{G} .

40:4 On Fourier Analysis of Sparse Boolean Functions over Certain Abelian Groups

This notion of granularity made sense over \mathbb{Z}_2^n , since in this case, all the Fourier coefficients are *rational* (and hence real) numbers. But when the domain of the function is a general group \mathcal{G} , the Fourier coefficients are necessarily complex numbers. So, we would like to suitably define granularity, and show that such a property still holds for s -sparse Boolean-valued functions over \mathcal{G} . Our first conceptual contribution in this paper is to generalize the notion of granularity appropriately.

► **Definition 1 (Granularity).** A complex number is said to be k -granular or has granularity k with respect to \mathbb{Z}_p if it is of the form $\frac{g(\omega_p)}{p^k}$, where $g(X) \in \mathbb{Z}[X]$ and ω_p is a primitive p^{th} root of unity.

More generally, a complex number is said to be (m_1, \dots, m_t) -granular with respect to $(\mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_t})$ if it is of the form $\frac{g(\omega_{p_1} \dots \omega_{p_t})}{p_1^{m_1} \dots p_t^{m_t}}$, where $g(X_1, \dots, X_t) \in \mathbb{Z}[X_1, \dots, X_t]$ and ω_{p_i} is a primitive p_i^{th} root of unity, $i \in [t]$.

Note that, this goes well with the definition of granularity in [15] for the case of \mathbb{Z}_2 as ω_2 is either $+1$ or -1 and hence $g(\omega_2)$ is an integer for any $g(X) \in \mathbb{Z}[X]$.

A function $f : \mathcal{G} \rightarrow \{-1, +1\}$ is said to be (m_1, \dots, m_t) -granular with respect to $(\mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_t})$ if each Fourier coefficient of f is (m_1, \dots, m_t) -granular.

We will also need a *robust* version of the definition of granularity of a complex number.

► **Definition 2 (μ -close to k -granular).** A complex number v is said to be μ -close to k -granular with respect to \mathbb{Z}_p if $|v - \frac{g(\omega_p)}{p^k}| \leq \mu$, for some non-zero polynomial $g(X) \in \mathbb{Z}[X]$.

Note that a similar notion can be defined for the case of μ -close to (m_1, \dots, m_t) -granular with respect to $(\mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_t})$.

Now, we are ready to formally state our two main structural results. All our results hold for Boolean-valued functions over the more general Abelian group \mathcal{G} . But for simplicity of presentation and ease of understanding, we first present the result for Boolean-valued functions over \mathbb{Z}_p^n . Later, we present more general versions of our results, see the archived version of the paper [7] for more details.

Our first theorem says that for any Boolean-valued function over \mathbb{Z}_p^n that is *close* to being sparse, all its large Fourier coefficients are close to being granular. This is a generalization of the structural theorem of [15, Theorem 3.3], which was proved over \mathbb{Z}_2^n .

► **Theorem 3 (Structure theorem 1).** Let $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ be a Boolean-valued function and let B be the set of characters corresponding to the set of s -largest Fourier coefficients of f (in terms of magnitude). If $\sum_{\chi \in B} |\hat{f}(\chi)|^2 \geq (1 - \mu)$ then for all $\chi \in B$, $\hat{f}(\chi)$ is $\frac{\mu}{\sqrt{s}}$ -close to $\lceil \log_p s \rceil + 1$ -granular.

For a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, $\sum_{\chi \in B} |\hat{f}(\chi)|^2 \geq (1 - \mu)$ (where B is the set of characters corresponding to the set of s largest coefficients of f) can also be stated as “there is an s -sparse function $g : \mathbb{Z}_p^n \rightarrow \mathbb{C}$ with the ℓ_2 -distance between f and g is at most $\sqrt{\mu}$ ”. But note that this *does not* guarantee that there is an s -sparse Boolean-valued function $g : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ with ℓ_2 -distance between f and g being at most $\sqrt{\mu}$. However, our second theorem proves that one can indeed find an s -sparse Boolean-valued function in a close enough vicinity, thus generalizing [15, Theorem 3.4].

► **Theorem 4 (Structure theorem 2).** Let $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ be a Boolean-valued function and let B be the set of characters corresponding to the set of s -largest Fourier coefficients of f (in terms of magnitude). If $\sum_{\chi \in B} |\hat{f}(\chi)|^2 \geq (1 - \mu)$, with $\mu \leq \frac{1}{8(p^2 s)^{p-1}}$ then there exists an s -sparse Boolean-valued function $F : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ with ℓ_2 distance between f and F is at most $\sqrt{2}\mu$.

Theorem 3 and Theorem 4 can be suitably generalized to functions from \mathcal{G} to $\{-1, +1\}$. But for the clarity of presentation, we state the generalized theorems and present their proofs in the archived version of the paper [7].

One important corollary of Theorem 3 is that for any s -sparse Boolean function $f : \mathbb{Z}_2^n \rightarrow \{-1, +1\}$ the non-zero Fourier coefficients has magnitude at least $1/2^k$, where $k = \lceil \log_2 s \rceil + 1$. Unfortunately, such a simple corollary cannot be claimed for s -sparse functions $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ if $p \neq 2$. The main reason is that the definition of granularity is for complex numbers, rather than real numbers and hence such a lower bound cannot be directly deduced. However, borrowing results from algebraic number theory, we can obtain a lower bound on the Fourier coefficients of Boolean-valued functions from \mathbb{Z}_p^n to $\{-1, +1\}$ for any arbitrary prime p .

► **Theorem 5** (Fourier coefficient lower bound). *Let $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, with Fourier sparsity s_f . Then, for any $\chi \in \text{supp}(f)$, we have $|\hat{f}(\chi)| \geq \frac{1}{(p^2 s_f)^{\lceil (p-1)/2 \rceil}}$.*

► **Remark.** One can also prove a weaker lower bound of the form $1/((s_f + 1)\sqrt{s_f})^{s_f}$, which is p -independent; for details, see the archived version of the paper [7].

Observe that the lower bound in Theorem 5 is much lower than $1/s_f$. One may wonder how tight our result is. It is known that $1/s$ is tight for the case when $p = 2$. For example, consider the function $AND : \mathbb{Z}_2^n \rightarrow \{-1, +1\}$. Its non-empty Fourier coefficients are either $\frac{1}{2^{n-1}}$ or $-\frac{1}{2^{n-1}}$, while the empty (constant) coefficient being $1 - \frac{1}{2^{n-1}}$.

To our pleasant surprise, we construct s -sparse Boolean-valued functions over \mathbb{Z}_p^n , for $p \geq 5$, such that they have nonzero Fourier coefficients with absolute value being $o(1/s)$.

► **Theorem 6** (Small Fourier coefficients). *For every prime $p \geq 5$, and large enough n , there exist a positive constant α_p that depends only on p and a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ with Fourier sparsity s_f satisfying the following property:*

$$\min_{\chi \in \text{supp}(f)} |\hat{f}(\chi)| \leq 1/s_f^{1+\alpha_p}.$$

We prove a generalized version of the lower bound result (Theorem 5) for Boolean-valued functions over \mathcal{G} . The above example (from Theorem 6) can also be easily extended to obtain Boolean-value functions over \mathcal{G} demonstrating similar bounds on the absolute value of the non-trivial Fourier coefficients.

Finally, we design efficient algorithms for testing whether a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ is s -sparse or “far” from s -sparse-Boolean. To state our results we need to define what we mean by a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ is ϵ -far from s -sparse.

► **Definition 7.** *A function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ is ϵ -far from s -sparse-Boolean if for every s -sparse function $g : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ the ℓ_2 -distance of f and g is at least $\sqrt{\epsilon}$.¹*

We say that an algorithm (property tester) \mathcal{A} ϵ -tests \mathcal{C} , for a class of functions $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, if given access to the truth table of a function f , whether $f \in \mathcal{C}$, or f is “ ϵ -far from \mathcal{C} ” can be tested using \mathcal{A} with success probability (called the *confidence*) $\geq 2/3$. The number of queries to the truth-table of f made by \mathcal{A} is called the query complexity of \mathcal{A} .

¹ In property testing usually the distance measure used is Hamming distance between two Boolean functions. But since we are using ℓ_2 distance in our other theorem, so for ease of presentation, we have defined the farness in terms of ℓ_2 instead of Hamming distance. Also, note that for a pair of Boolean-valued functions the square of the ℓ_2 distance and Hamming distance are the same up to a multiplicative factor of 4, see the archived version of the paper [7]

Using the structure theorems (Theorem 3 and Theorem 4), we prove the following theorem which tests sparsity of a Boolean-valued function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$.

► **Theorem 8** (Testing s -sparsity). *For a fixed prime p , there is a non-adaptive $\text{poly}(s, 1/\epsilon)$ query algorithm with confidence $2/3$, which tests whether a given function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, is s -sparse or ϵ -far from s -sparse-Boolean.*

We can also obtain a similar testing algorithm for sparsity, for a Boolean-valued function over \mathcal{G} . The generalized algorithm is discussed in the archived version of the paper [7].

We complement our result by showing a query-complexity lower bound for sparsity-testing algorithms. Gopalan et al. [15] gave a $\Omega(\sqrt{s})$ lower bound for s -sparsity testing algorithms over \mathbb{Z}_2^n . An important component of their proof was to cleverly use an alternative notion of *degree* (borrowed from [6]) of a Boolean function over \mathbb{Z}_2 . We also give a similar lower bound over \mathbb{Z}_p^n , by appropriately generalizing the useful notion of degree. For details on the definition of degree, see proof idea of Theorem 9 in Section 1.2 and in the archived version of the paper [7].

► **Theorem 9.** *For Boolean valued functions on \mathbb{Z}_p^n , to adaptively test s -sparsity, the query lower bound of any algorithm is $\Omega(\sqrt{s})$.*

Theorem 9 can be generalized for Boolean valued functions on \mathcal{G} , which will give us the same lower bound.

1.2 Proof ideas

In this section, we briefly outline the proof ideas of our main theorems. Although some of the proofs are indeed inspired by [15] (which worked over \mathbb{Z}_2), the proof techniques *does not* directly generalize over \mathbb{Z}_p . So, we will first discuss the proof ideas, and then clarify the differences between [15] and our techniques (see Section 1.2.1). While doing so, we will try to convey the hurdles for generalizing over \mathbb{Z}_p . Let us first sketch the proof of Theorem 3.

Proof idea of Theorem 3. Our goal is to show that if f is μ -close to some s -sparse complex-valued function in ℓ_2 , then there exists a non-zero polynomial $g(X) \in \mathbb{Z}[X]$ such that the following properties hold.

1. The sum of the absolute values of its coefficients is *at most* p^k , where $k := \lceil \log_p s \rceil + 1$.
2. The *distance* between the absolute value of each non-zero Fourier coefficient of f and $|g(\omega_p)|/p^k$ is at most μ/\sqrt{s} .

To show the above, we first utilize a probabilistic method to prove that for each character $\chi_i \in B$ in the Fourier support of f , there exists a matrix $A \in \mathbb{Z}_p^{k \times n}$, and a column vector $b \in \mathbb{Z}_p^{n \times 1}$, such that – (1) χ_i is a solution of the linear system $A\chi = b$, and (2) *no other* character in the Fourier support of f is a solution of $A\chi = b$, where B be the set of s -largest Fourier coefficients of f . After establishing the existence of such A and b , we consider the Fourier transform of the projection operator for the solution space of $A\chi = b$ (see the archived version of the paper [7]). The projection operator, as the name suggests, is an operator that projects \mathbb{Z}_p^n onto a linear subspace which yields a partition of the Fourier spectrum of f . Then we show that the ℓ_2 Fourier weight of $S \cap H$, i.e., $\sum_{\chi \in S \cap H} |\hat{f}(\chi)|^2$ is upper bounded by μ/\sqrt{s} , where $S = \overline{B}$, and H is a coset of A^\perp that are solutions to the system of linear equations $A\chi = b$. For details, see the archived version of the paper [7].

Proof idea of Theorem 5. If we put $\mu = 0$ in Theorem 3, we get that there exists a $g \in \mathbb{Z}[X]$, with the sum of the absolute values of its coefficients is *at most* p^k , such that $|\widehat{f}(\chi)| \geq |g(\omega_p)/p^k|$, where $k = \lceil \log_p s_f \rceil + 1$, s_f being the sparsity of the Boolean valued function f . The remaining part of the proof is to show that for any polynomial g with the aforementioned properties, $|g(\omega_p)|/p^k \geq 1/(p^2 s_f)^{\lceil (p-1)/2 \rceil}$.

As stated earlier, we use a non-trivial result from algebraic number theory (Theorem 25), which states that if $f \in \mathbb{Z}[x]$, such that $f(\omega_n) \neq 0$, where ω_n be a primitive root of unity, then, $|\prod_{i \in \mathbb{Z}_n^*} f(\omega_n^i)| \geq 1$. We also use the fact that the sum of the absolute values of the coefficients of g is at most p^k , to get an upper bound on the quantities $|g(\omega_p^i)|$, for any $i \in [p-1]$. Combining these two facts, we obtain our lower bound; for details see the archived version of the paper [7].

Proof idea of Theorem 4. We first show that the given function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, that is μ -close to some s -sparse complex-valued function in ℓ_2 , can be written as the sum of two functions F and G , where the Fourier coefficients of F are $\lceil \log_p s \rceil + 1$ -granular and the absolute value of the Fourier coefficients of G are upper bounded by μ/\sqrt{s} , where p is an odd prime. This follows from Theorem 3. Then we show that the range of F is $\{-1, +1\}$, which uses the following facts:

1. $(F + G)^2 = f^2 = 1$ and
2. F^2 is $2\lceil \log_p s \rceil + 1$ -granular.

We compute $\mathbb{E}[G(x)^2]$ in order to find an upper bound on the Fourier coefficients of $H := G(2f - G)$, which helps us to conclude that $\widehat{F^2}(\chi) = 0$ for all $\chi \neq \chi_0$, and $\widehat{F^2}(\chi_0) = 1$, where χ_0 is the character which takes the value 1 at all points in \mathbb{Z}_p^n . Then we complete the proof by showing that the $\Pr_x[x \in \mathbb{Z}_p^n | f(x) \neq g(x)] \leq \mu^2/2$, which implies that F is $\sqrt{2}\mu$ close to f in ℓ_2 (see Lemma 22). This idea has also been employed in [15]. We have also extended this proof to a more general Abelian group \mathcal{G} , (see the archived version of the paper [7]).

Proof idea of Theorem 6. The example that we construct to prove Theorem 6 is a simple one. The crucial observation in this regard is that there are functions from \mathbb{Z}_p to $\{-1, +1\}$, whose Fourier coefficients are smaller than $1/p$. In this work, we work with one such function $\mathbb{I}_{\geq \frac{p+1}{2}} : \mathbb{Z}_p \rightarrow \{-1, +1\}$. We claim that the composition function $AND_n \circ \mathbb{I}_{\geq \frac{p+1}{2}}$ is one such desired function from \mathbb{Z}_p^n to $\{-1, +1\}$, such that its minimum Fourier coefficient is less than $1/p^n$. Here, we assume a trivial bound of p^n on the Fourier sparsity of the function $AND_n \circ \mathbb{I}_{\geq \frac{p+1}{2}}$.

Proof idea of Theorem 8. We sketch the algorithmic idea over \mathbb{Z}_p^n , where p is an odd prime; this idea can be canonically extended to more general Abelian groups \mathcal{G} . The main idea of the algorithm is to partition the set of characters into buckets and estimate the *weights* of the individual buckets (that is the sum of the squares of the absolute values of the Fourier coefficients corresponding to the characters in the buckets). We know from Theorem 5 that all the coefficients of an s -sparse function are at least as large as $1/(p^2 s)^{\lceil (p-1)/2 \rceil}$. So, we are certain that if the weights of the buckets can be approximated within an additive error of $\tau/3$, where $\tau \geq 1/(p^2 s)^{p-1}$, then in the case the function is s -sparse, not more than s of the buckets can have weight more than $\tau/2$. On the other hand, we will show that if the function f is ϵ -far from any s -sparse Boolean function then with a high probability at least $(s+1)$ buckets will have weight more than τ , making the estimated weight at least $2\tau/3$; see the archived version of the paper for more details [7].

The challenge is that estimating the weights of the buckets is not easy if the characters are randomly partitioned into buckets. Here we use the ideas from Gopalan et al [15] and appropriately modify them to handle the technicalities of working with \mathbb{Z}_p^n . We choose the buckets carefully. The buckets corresponds to the cosets of H^\perp in \mathbb{Z}_p^n , where H is a random subspace of \mathbb{Z}_p^n of dimension, $t = \Theta(s^2)$. For such kinds of buckets, we show that estimation of the weight can be done using a small number of samples. We also need to use the concept of “random shift”, see the archived version of the paper [7], to avoid the corner case of characters being put into the trivial bucket.

Unlike [15], it becomes a bit more challenging to prove that if f is ϵ -far from any s -sparse Boolean function over \mathbb{Z}_p^n , then with high probability at least $(s + 1)$ buckets will have weight more than τ . Since we partition the set of characters by cosets, the events whether two characters land in the same bucket (that is same coset) are *not independent* – since two characters (in the case $p \neq 2$) can be scalar multiple of each other; this is where some additional care is required (which was not the case in [15]). Under random shifts and case-by-case analysis, we can show that the two events are *not correlated*, i.e., the covariance of the corresponding indicator variables of the two events is 0; see the archived version of the paper [7]. Thus, we can use Chebyshev’s inequality and then Markov’s inequality to bound the number of buckets that can be of low weight, or in other words prove that the number of “heavy” weight buckets is more than $s + 1$. The proof of Theorem 8 is given in the archived version of the paper [7].

Proof idea of Theorem 9. In [15], Gopalan et al. proved a query lower bound over \mathbb{Z}_2^n , by using a natural notion of *degree* of a Boolean function, denoted deg_2 . They crucially used the fact that for a Boolean function f over \mathbb{Z}_2 , $2^{\dim(f)} \geq s_f \geq 2^{\text{deg}_2(f)}$; this was originally proved in [6]. To define the degree, let us consider all possible restrictions $f|_{V_{b,r_1,\dots,r_t}}$ of f , where V_{b,r_1,\dots,r_t} is a coset of V_{0,r_1,\dots,r_t} in \mathbb{Z}_p^n as defined as

$$V_{b,r_1,\dots,r_t} := \{x \in \mathbb{Z}_p^n : r_j \cdot x = b_j \pmod{p} \forall j \in [t]\}.$$

Then the degree over \mathbb{Z}_p of f , denoted by deg_p , is defined in the following way.

$$\text{deg}_p(f) = \max_{\ell} \{ \ell = \dim(V_{b,r_1,\dots,r_t}) : s_{f|_{V_{b,r_1,\dots,r_t}}} = p^{\dim(V_{b,r_1,\dots,r_t})} \},$$

where $s_{f|_{V_{b,r_1,\dots,r_t}}}$ is the Fourier sparsity of the function $f|_{V_{b,r_1,\dots,r_t}}$. [15] defined the degree over \mathbb{Z}_2^n via similar restrictions. However, [15] argued that this is a natural definition of the degree over \mathbb{Z}_2^n . To argue, observe that $\hat{f} = \frac{1}{2^n} H_n f$, where H_n is the $2^n \times 2^n$ Hadamard matrix, when $x_i \in \mathbb{Z}_2^n$ are seen in lexicographic order. Consider the restrictions $f|_{V_{b,r_1,\dots,r_t}}$ that takes the value 1 at those points such that each entry of $\hat{f}|_{V_{b,r_1,\dots,r_t}}$ is nonzero. Then deg_2 can be defined as the dimension of the coset V_{b,r_1,\dots,r_t} which is *largest* amongst them! In that case, all the Fourier coefficients of $f|_{V_{b,r_1,\dots,r_t}}$ are nonzero.

Interestingly, we can also show that the above definition of deg_p is natural, mainly because $\hat{f} = \frac{1}{p^n} V_n f$, where V_1 is a $p \times p$ *Vandermonde* matrix V_1 , whose (i, j) -th entry is $(V_1)_{i,j} := \omega_p^{(i-1)(j-1)}$, and V_n is defined by taking n many *Kronecker products* of V_1 , i.e., $V_n := V_1^{\otimes n} = V_1 \otimes \dots \otimes V_1$. Note that $H_n = V_n$, over \mathbb{Z}_2^n . Similar to [6], one can also show that $p^{\dim(f)} \geq s_f \geq p^{\text{deg}_p(f)}$ (see the archived version of the paper [7]). This plays a crucial role in the proof.

We first define two distributions \mathcal{D}_{Yes} and \mathcal{D}_{No} on the set of Boolean valued functions from \mathbb{Z}_p^n to $\{-1, +1\}$. Let us choose a *random* t -dimensional subspace H of \mathbb{Z}_p^{Ct} , for some parameter C (to be fixed later). Let \mathcal{C} be the set of all cosets of H . There are 2 main steps as follows.

1. We construct random functions f by making f a constant on each coset of \mathcal{C} . The constant is chosen randomly from $\{-1, +1\}$. We call this probability distribution \mathcal{D}_{yes} .
2. We choose a random function f randomly from \mathbb{Z}_p^{Ct} , conditioned on the fact that f is $2 - \tau$ far in ℓ_2 from any function which has $\deg_p = t$, where τ is as defined in Theorem 8. Let us call this distribution \mathcal{D}_{No} .

We show that if an adaptive query algorithm makes less than $q < \Omega(p^{t/2})$ queries, then the total variation distance $\|\mathcal{D}_{Yes} - \mathcal{D}_{No}\|_{TV}$ between the two distributions \mathcal{D}_{Yes} and \mathcal{D}_{No} is $\leq \frac{1}{3}$. This proves that any adaptive query algorithm which distinguishes between \mathcal{D}_{Yes} and \mathcal{D}_{No} , i.e., where $\|\mathcal{D}_{Yes} - \mathcal{D}_{No}\|_{TV} > \frac{1}{3}$, must make at least $\Omega(p^{t/2})$ queries. This essentially proves Theorem 9.

1.2.1 Comparison with Gopalan et al. [15]

In this section, we discuss the main differences and points between our proof and the one by Gopalan et al. [15]. Our proofs (and the analysis of the testing algorithm) are more elaborate, subtle, case-dependent, and complicated than [15].

Linear dependence is bad. [15] used the similar idea as in Theorem 3, see the archived version of the paper for more details [7]. However, their proof took advantage of the fact that any two distinct non-zero vectors in \mathbb{Z}_2^n are *linearly independent*. This is *not true* for \mathbb{Z}_p^n , as distinct vectors can be scalar multiples of each other; e.g., $(1, \dots, 1)$ and $(2, \dots, 2)$ in \mathbb{Z}_p^n , for any $p \geq 3$. Thus, our proof technique is capable of handling and overcoming these difficulties effectively. This is also why our analysis of the structure theorems and algorithms are very much case-dependent.

Different granularity. In case of \mathbb{Z}_2^n , [15] defined a function $f : \mathbb{Z}_2^n \rightarrow \{-1, +1\}$ to be k -granular, where k is a positive integer, if all of its nonzero Fourier coefficients are an *integer multiple* of $\frac{1}{2^k}$. In the case of \mathbb{Z}_p^n , since the Fourier coefficients are truly complex numbers, we define a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ to be k -granular if all of its nonzero Fourier coefficients are of the form $\frac{g(\omega_p)}{p^k}$ (see Definition 1), where $g \in \mathbb{Z}[X]$ and ω_p is a primitive p^{th} root of unity.

Algebraic integer lower bounds are harder. While proving a lower bound on the absolute value of the Fourier coefficients, in the case of \mathbb{Z}_2^n , proving a lower bound on the magnitude of a Fourier coefficient [15] translates to proving a lower bound on $|g(-1)|/2^k$ (since $\omega_2 = -1$). Note that $|g(-1)| \geq 1$, because $g(-1) \in \mathbb{Z} \setminus \{0\}$; hence the lower bound follows. However, for a general prime p , ω_p is *truly* a complex number, and hence, $g(\omega_p)$ is *no longer* an integer (and therefore, there is no way to conclude that $|g(\omega_p)| \geq 1$). We use a non-trivial result from algebraic number theory (Theorem 25) to tackle this problem, in the proof of Theorem 5. We also crucially use the fact that the sum of the absolute values of the coefficients of g is at most p^k , to get an upper bound on the quantities $|g(\omega_p^i)|$, for any $i \in [p-1]$. Clearly, this part requires much more non-triviality than [15].

Do not expect a tight linear lower bound. For $p = 2$, it follows from [15] that the lower bound on the absolute value of the Fourier coefficients is equal to $\frac{1}{s_f}$. We show in Theorem 6 that there exists a family of Boolean valued functions on \mathbb{Z}_p^n , $p > 3$ such that $\min_{\chi \in \text{supp}(f)} |\widehat{f}(\chi)| \leq 1/s_f^{1+\alpha_p}$, hence proving that the lower bound on the absolute value of the Fourier coefficients is not linear in $\frac{1}{s_f}$ in case of $p > 3$.

Generalizing the notion of degree. For functions from \mathbb{Z}_2^n to $\{-1, +1\}$, it is known that $\widehat{f} = \frac{1}{p^n} H_n f$, where H_n denotes the Hadamard matrices (see [6]). Then, the degree \deg_2 is defined naturally in the case of \mathbb{Z}_2^n . The definition of \deg_p becomes slightly challenging, since the relation $\widehat{f} = \frac{1}{p^n} H_n f$ is simply *false* over \mathbb{Z}_p^n . To define \deg_p for Boolean valued functions on \mathbb{Z}_p^n (see the archived version of the paper [7]), where p is an odd prime, we have defined the matrix V_1 using Vandermonde matrix, and have inductively defined the matrices V_n , where n is a positive integer, via Kronecker product. Then we have shown that $\widehat{f} = \frac{1}{p^n} V_n f$, which helps us to define $\deg_p(f)$. We claim that this is an appropriate generalization of degree, since $H_n = V_n$, over \mathbb{Z}_2^n .

Finally, we remark that because of the *absence of a linear structure* on the solution space of systems of equations over arbitrary Abelian groups (e.g. \mathbb{Z}_{p^2}), we could not generalize this to arbitrary Abelian groups.

2 Preliminaries

2.1 Fourier Analysis over $\mathbb{Z}_{p_1}^{n_1} \times \dots \times \mathbb{Z}_{p_t}^{n_t}$

$\mathbb{Z}_{p_1}^{n_1} \times \dots \times \mathbb{Z}_{p_t}^{n_t}$ forms a finite Abelian group under addition whose order is $p_1^{n_1} \dots p_t^{n_t}$, where p_1, \dots, p_t are distinct primes. Its individual components form a vector space, that is, $\mathbb{Z}_{p_i}^{n_i}$ is a vector space over the field \mathbb{Z}_{p_i} for all $i \in \{1, 2, \dots, t\}$ whenever p_i 's are primes. Throughout this paper we will denote $\mathbb{Z}_{p_1}^{n_1} \times \dots \times \mathbb{Z}_{p_t}^{n_t}$ by \mathcal{G} . So \mathcal{G} is a finite Abelian group with $|\mathcal{G}| = p_1^{n_1} \dots p_t^{n_t}$, where $|\cdot|$ denotes the order of \mathcal{G} .

We will denote this root of unity by ω_p a p^{th} primitive root of unity, that is $e^{2\pi i/p}$.

Let us begin by defining the characters of \mathcal{G} .

► **Definition 10** (Character). *A character of \mathcal{G} is a homomorphism $\chi : \mathcal{G} \rightarrow \mathbb{C}^\times$ of \mathcal{G} , that is, χ satisfies the following:*

$$\chi(x + y) = \chi(x)\chi(y), \quad x, y \in \mathcal{G}.$$

Equivalently, a character χ of \mathcal{G} can be defined by

$$\chi(x_1, \dots, x_t) = \chi_{r_1}(x_1) \dots \chi_{r_t}(x_t) = \omega_{p_1}^{r_1 \cdot x_1} \dots \omega_{p_t}^{r_t \cdot x_t},$$

where χ_{r_i} is a character of $\mathbb{Z}_{p_i}^{n_i}$ for each i and is defined by $\chi_{r_i}(x_i) = \omega_{p_i}^{r_i \cdot x_i}$, $x_i, r_i \in \mathbb{Z}_{p_i}^{n_i}$ for all i , $r_i \cdot x_i = \sum_{j=1}^{n_i} r_{i(j)} x_{i(j)}$, $r_{i(j)}$ and $x_{i(j)}$ being the j^{th} component of r_i and x_i respectively (It follows from the fact that any character χ of \mathcal{G} can be written as the product of characters of $\mathbb{Z}_{p_1}^{n_1}, \dots, \mathbb{Z}_{p_t}^{n_t}$). Let us denote this character by χ_{r_1, \dots, r_t} .

Now let us look at some properties of characters.

► **Lemma 11.** *Let χ be a character of \mathcal{G} . Then,*

1. $\chi_0(x) = 1$ for all $x \in \mathcal{G}$.
2. $\chi(-x) = \chi(x)^{-1} = \overline{\chi(x)}$ for all $x \in \mathcal{G}$.
3. For any character χ of \mathcal{G} , where $\chi \neq \chi_0$, $\sum_{x \in \mathcal{G}} \chi(x) = 0$.
4. $|\chi_0(x)| = 1$ for all $x \in \mathcal{G}$.

Now let us define the dual group of \mathcal{G} .

► **Definition 12** (Dual group). *The set of characters of \mathcal{G} forms a group under the operation $(\chi\psi)(x) = \chi(x)\psi(x)$ and is denoted by $\widehat{\mathcal{G}}$, where χ and ψ are characters of \mathcal{G} . $\widehat{\mathcal{G}}$ is called the dual group of \mathcal{G} .*

The following theorem states that \mathcal{G} is isomorphic to its dual group.

► **Theorem 13.** $\widehat{\mathcal{G}} \cong \mathcal{G}$.

Let us look at the definition of Fourier transform for functions on \mathcal{G} .

► **Definition 14** (Fourier transform). *For any function $f : \mathcal{G} \rightarrow \mathbb{C}$, the Fourier transform $\widehat{f} : \widehat{\mathcal{G}} \rightarrow \mathbb{C}$ is defined by*

$$\widehat{f}(\chi_{r_1, \dots, r_t}) = \frac{1}{|\mathcal{G}|} \sum_{x \in \mathcal{G}} f(x) \omega_{p_1}^{-r_1 \cdot x_1} \dots \omega_{p_t}^{-r_t \cdot x_t},$$

where $x_i, r_i \in \mathbb{Z}_{p_i}^{n_i}$ for all i , and $r_i \cdot x_i = \sum_{j=1}^{n_i} r_{i(j)} x_{i(j)}$, $r_{i(j)}$ and $x_{i(j)}$ being the j^{th} component of r_i and x_i respectively.

► **Remark 15.** The Fourier transform of a function $f : \mathcal{G} \rightarrow \mathbb{C}$ is defined by

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

where $\overline{\chi(x)}$ is the conjugate of $\chi(x)$. The Definition 14 follows from this, as $\chi = \chi_{r_1, \dots, r_t}$ for some $r_i \in \mathbb{Z}_{p_i}^{n_i}$, $i \in \{1, \dots, t\}$.

The following theorem states that any function from \mathcal{G} to \mathbb{C} can be written as a linear combination of characters of \mathcal{G} .

► **Theorem 16** (Fourier inversion formula). *Any function $f : \mathcal{G} \rightarrow \mathbb{C}$ can be uniquely written as a linear combination of characters of \mathcal{G} , that is,*

$$f(x) = \sum_{\chi_{r_1, \dots, r_t} \in \widehat{\mathcal{G}}} \widehat{f}(\chi_{r_1, \dots, r_t}) \omega_{p_1}^{r_1 \cdot x_1} \dots \omega_{p_t}^{r_t \cdot x_t},$$

where $x_i, r_i \in \mathbb{Z}_{p_i}^{n_i}$ for all i , $r_i \cdot x_i = \sum_{j=1}^{n_i} r_{i(j)} x_{i(j)}$, $r_{i(j)}$ and $x_{i(j)}$ being the j^{th} component of r_i and x_i respectively.

► **Theorem 17** (Parseval). *For any two functions $f, g : \mathcal{G} \rightarrow \mathbb{C}$,*

$$\mathbb{E}_{x \in \mathcal{G}} [f(x) \overline{g(x)}] = \sum_{\chi \in \widehat{\mathcal{G}}} \widehat{f}(\chi) \overline{\widehat{g}(\chi)}.$$

More specifically, if $f : \mathcal{G} \rightarrow \{-1, +1\}$ is a Boolean-valued function then

$$\sum_{\chi \in \widehat{\mathcal{G}}} |\widehat{f}(\chi)|^2 = 1.$$

Now let us define the Fourier sparsity of a function f on \mathcal{G} .

► **Definition 18** (Sparsity and Fourier Support).

- The Fourier sparsity s_f of a function $f : \mathcal{G} \rightarrow \mathbb{C}$ is defined to be the number of non-zero Fourier coefficients in the Fourier expansion of f (Theorem 16). In this paper, by sparsity of a function, we will mean the Fourier sparsity of the function.
- Fourier support $\text{supp}(f)$ of a function $f : \mathcal{G} \rightarrow \mathbb{C}$ denotes the set $\{\chi \mid \widehat{f}(\chi) \neq 0\}$.

The following lemma states an important property of characters of a subgroup $H = H_1 \times \dots \times H_t$ of \mathcal{G} .

40:12 On Fourier Analysis of Sparse Boolean Functions over Certain Abelian Groups

► **Lemma 19.** $\sum_{h \in H} \chi_h = |H| \cdot 1_{H^\perp}$, where $H = H_1 \times \cdots \times H_t$ is a subgroup of \mathcal{G} , and $h = (h_1, \dots, h_t)$, $h_i \in H_i \forall i$. That is,

$$\sum_{h_1 \in H_1, \dots, h_t \in H_t} \chi_{h_1} \cdots \chi_{h_t} = |H_1| \cdots |H_t| \cdot 1_{H_1^\perp} \cdots 1_{H_t^\perp}.$$

Here, for each i , H_i is a subgroup of $\mathbb{Z}_{p_i}^{n_i}$ and hence a subspace $\mathbb{Z}_{p_i}^{n_i}$, as $\mathbb{Z}_{p_i}^{n_i}$ is a vector space.

The proof of Lemma 19 is given in the archived version of the paper [7] due to lack of space.

► **Lemma 20.** Let f, g be two Boolean valued functions from \mathcal{G} to $\{-1, +1\}$. Then,

$$|\widehat{fg}(\chi)| \leq \|f\|_2 \|g\|_2,$$

for any character $\chi \in \widehat{\mathcal{G}}$.

The proof of Lemma 20 is given in the archived version of the paper [7] due to lack of space.

Now let us formally define the notion of ϵ -close and ϵ -far in ℓ_2 below.

► **Definition 21** (μ -close to s -sparse). Let f and g be two functions with domain \mathbb{Z}_p^n and range \mathbb{C} . Then the square of the ℓ_2 distance between f and g is defined as $\mathbb{E}_{x \in \mathcal{G}} [|f(x) - g(x)|^2]$. By Parseval's identity the square of the ℓ_2 -distance between f and g can also be written as $\sum_{\chi \in \widehat{\mathbb{Z}_p^n}} |(\widehat{f - g})(\chi)|^2$.

We say that f is ϵ -close to g in ℓ_2 if the square of the ℓ_2 distance between f and g is less than ϵ . Similarly, f is ϵ -far from g in ℓ_2 if the square of the ℓ_2 distance between f and g is at least ϵ .

The following lemma gives us a relation between the ℓ_2 distance between two Boolean valued functions f and g defined in Definition 21 and $\Pr_x[x \in \mathcal{G} | f(x) \neq g(x)]$.

► **Lemma 22.** The square of the ℓ_2 distance between two Boolean valued functions f and g defined in Definition 21 is equal to $4 \Pr_x[x \in \mathcal{G} | f(x) \neq g(x)]$.²

The proof of Lemma 22 is given in the archived version of the paper [7] due to lack of space.

Now let us define the total variation distance between two probability distributions.

► **Definition 23.** Let (Ω, \mathcal{F}) be a probability space, and P and Q be probability distributions defined on (Ω, \mathcal{F}) . The total variation distance between P and Q is defined in the following way.

$$\|P - Q\|_{TV} = \sup_{A \in \mathcal{F}} |P(A) - Q(A)|.$$

► **Lemma 24.** Given two probability distributions P and Q on a probability space (Ω, \mathcal{F}) , the total variation distance between P and Q is half of the L_1 distance between them. That is,

$$\|P - Q\|_{TV} = \frac{1}{2} \sum_x |P(x) - Q(x)|.$$

² If f and g are two Boolean-valued functions then $\Pr_x[x \in \mathcal{G} | f(x) \neq g(x)]$ is also called the Hamming distance between the two functions. So the ℓ_2 norm between two Boolean-valued functions is 4 times the Hamming distance between two Boolean-valued functions.

3 Lower bound on the Fourier coefficients

In this section, we will prove Theorem 5 assuming Theorem 3, which gives us a lower bound on the Fourier coefficients of functions from \mathbb{Z}_p^n to $\{-1, +1\}$, where p is a prime number. This is a generalization on the granularity of a function $f : \mathbb{Z}_2^n \rightarrow \mathbb{R}$ when the domain of the function is \mathbb{Z}_p^n . We will use the following theorem; for more details see the archived version of the paper [7].

► **Theorem 25.** For $n \in \mathbb{Z}$, let ω_n be a primitive root of unity. Let $f \in \mathbb{Z}[x]$, such that $f(\omega_n) \neq 0$. Then,

$$\left| \prod_{i \in \mathbb{Z}_n^*} f(\omega_n^i) \right| \geq 1.$$

Proof of Theorem 5. If we put $\mu = 0$ in Theorem 3, we get that there exists a $g \in \mathbb{Z}[X]$, such that $|\widehat{f}(\chi)| \geq |g(\omega_p)/p^k|$, where $k = \lceil \log_p s_f \rceil + 1$, s_f being the sparsity of the Boolean valued function f . We know by Theorem 25 that $|\prod_{i=1}^{p-1} g(\omega_p^i)| \geq 1$. Therefore,

$$\left| \prod_{i=1}^{p-1} g(\omega_p^i) \right| \geq 1 \Rightarrow \prod_{i=1}^{p-1} \left| \frac{g(\omega_p^i)}{p^k} \right| \geq \left(\frac{1}{p^k} \right)^{p-1} \Rightarrow \left| \frac{g(\omega_p)}{p^k} \right| \geq \frac{1}{p^{k(p-1)}} \geq \frac{1}{(p^2 s_f)^{p-1}}.$$

For $p = 2$, $g(\omega_p^i)$ is an integer, so

$$\left| \frac{g(\omega_p)}{p^k} \right| \geq \frac{1}{4s_f} \quad (3.1)$$

For $p \neq 2$, the conjugate of $g(\omega_p^i)$, namely $\overline{g(\omega_p^i)}$, is nothing but $= g(\omega_p^{p-i})$. Since $|g|_1 \leq p^k$, it follows that for any $i \in [p-1]$, $|g(\omega_p^i)/p^k| \leq 1$. Therefore,

$$\begin{aligned} \left| \prod_{i=1}^{p-1} g(\omega_p^i) \right| \geq 1 &\Rightarrow \prod_{i=1}^{(p-1)/2} |g(\omega_p^i)|^2 \geq 1 \\ &\Rightarrow \prod_{i=1}^{(p-1)/2} \left| \frac{g(\omega_p^i)}{p^k} \right|^2 \geq \left(\frac{1}{p^k} \right)^{p-1} \\ &\Rightarrow \left| \frac{g(\omega_p)}{p^k} \right|^2 \geq \frac{1}{p^{k(p-1)}} \\ &\Rightarrow \left| \frac{g(\omega_p)}{p^k} \right| \geq \frac{1}{p^{k(p-1)/2}} \geq \frac{1}{(p^2 s_f)^{(p-1)/2}}. \end{aligned} \quad (3.2)$$

So, from Equation (3.1) and Equation (3.2), we have

$$\left| \frac{g(\omega_p)}{p^k} \right| \geq \frac{1}{(p^2 s_f)^{\lceil (p-1)/2 \rceil}}. \quad \blacktriangleleft$$

► **Remark 26.** Let p be a prime. The proof-technique of Theorem 5 gives the following. If the Fourier coefficients of a Boolean function f are k granular, where $k = \lceil \log_p s \rceil + 1$, then the Fourier coefficients of f^2 are $2k$ -granular, and their absolute values are $\geq \frac{1}{(p^2 s)^{(p-1)/2}}$.

4 Sparse Boolean-valued function with small Fourier coefficients

In this section, for a fixed prime $p \geq 5$, and arbitrarily large s , we give an example of a function $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$, such that the minimum of the absolute value of its Fourier coefficients is at most $o(1/s)$. In this section, we give the details of the construction of Theorem 6; see the archived version of the paper [7].

To prove Theorem 6 we define a function, which is basically composition of AND_n and univariate Threshold functions; we call AT.

► **Definition 27.** Let us define function $\text{AT} : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$ by

$$\text{AT}(x_1, x_2, \dots, x_n) := \text{AND}_n \left(\mathbb{I}_{\geq \frac{p+1}{2}}(x_1), \mathbb{I}_{\geq \frac{p+1}{2}}(x_2), \dots, \mathbb{I}_{\geq \frac{p+1}{2}}(x_n) \right),$$

where the univariate Threshold function $\mathbb{I}_{\geq \frac{p+1}{2}} : \mathbb{Z}_p \rightarrow \{-1, +1\}$, is defined as:

$$\mathbb{I}_{\geq \frac{p+1}{2}}(x) = \begin{cases} 1 & \text{for } x \geq \frac{p+1}{2} \\ -1 & \text{otherwise.} \end{cases}$$

► **Lemma 28.** There is a Fourier coefficient of AT, whose absolute value is $\frac{1}{p^{nc}}$, where c is a constant > 1 .

The proof of Lemma 28 is given in the archived version of the paper [7]. Now we are ready to prove Theorem 6.

Proof of Theorem 6. This directly follows, as we can claim from Lemma 28 that there exists a family of functions in \mathbb{Z}_p^n whose absolute value of the minimum coefficient is not linear in $\frac{1}{\text{sparsity}}$, but actually $= \Omega\left(\frac{1}{\text{sparsity}^{1+\epsilon_p}}\right)$, where $\epsilon_p > 0$, is a p -dependent constant. ◀

► **Lemma 29.** There exists a function whose one of the Fourier coefficients is less than that of AT.

The proof of Lemma 29 is given in the archived version of the paper [7].

5 Testing Algorithm for Sparsity

Here we present the whole algorithm (Algorithm 1) for sparsity testing over \mathbb{Z}_p^n (see next page). However, we describe the various steps of the algorithm in the archived version of the paper [7], including the correctness and the analysis of the algorithm in the archived version of the paper [7].

6 Conclusion

Gopalan et al. [15] was the first to study the problem of testing Fourier sparsity of Boolean function over \mathbb{Z}_2^n . Along the way, they were able to drive fundamental properties of Boolean functions over \mathbb{Z}_2^n , like *Granularity* of the Fourier spectrum, that have found many other applications [3]. In this work, we have extended their results for groups that can be written as $\mathbb{Z}_{p_1}^{n_1} \times \dots \times \mathbb{Z}_{p_t}^{n_t}$.

The most natural question that arises from our work will be to study this problem for (finite) general Abelian groups. Unfortunately, our work does not extend to finite Abelian groups, because of the *absence* of the component-wise vector space structure. In particular, it would be nice to get a lower bound on the absolute value of non-zero Fourier coefficients of a sparse Boolean-valued function over $\mathbb{Z}_{p^2}^n$. In any way, our results in this paper should be seen as a first step toward solving the lower bound problem over finite Abelian group.

Finally, we ask whether it is possible to show a better (p -dependent) lower bound over \mathbb{Z}_p^n on the query-complexity of any adaptive sparsity testing algorithm.

Algorithm 1 Test Sparsity.

- 1: **Input:** s, ϵ , and query access to $f : \mathbb{Z}_p^n \rightarrow \{-1, +1\}$.
 - 2: **Output:** YES, if f is s -sparse, and NO, if it is ϵ -far from any Boolean valued function.
 - 3: **Parameter setting:** Set $t := \lceil 2 \log_p s + \log_p 20 \rceil + 1$, $\tau := \min(\frac{\epsilon^2}{40p^t}, \frac{1}{(p^2 s)^{p-1}})$ $M := O(\log(p^t) \cdot \frac{1}{\tau^2})$
 - 4: Choose v_1, \dots, v_t linearly independent vectors uniformly at random from \mathbb{Z}_p^n .
 - 5: Let $H = \text{Span}\{v_1, \dots, v_t\}$
 - 6: Pick $(z_1, x_1), \dots, (z_M, x_M)$ uniformly and independently from $H \times \mathbb{Z}_p^n$
 - 7: Query $f(x_1), \dots, f(x_M)$ and $f(x_1 - z_1), \dots, f(x_M - z_M)$
 - 8: **for** For every $r \in \mathbb{Z}_p^n$ **do**
 - 9: Let $\frac{1}{M} \sum_{i=1}^M \chi_r(z_i) f(x_i) f(x_i - z_i)$ be the estimate of $wt(r + H^\perp)$
 - 10: **end for**
 - 11: **if** number of r for which the estimate of $wt(r + H^\perp)$ is $\geq \frac{2\tau}{3}$ is $\leq s$ **then**
 - 12: Output YES
 - 13: **else**
 - 14: Output NO
 - 15: **end if**
-

References

- 1 Adi Akavia. *Learning noisy characters, multiplication codes, and cryptographic hardcore predicates*. PhD thesis, Massachusetts Institute of Technology, 2008.
- 2 Adi Akavia, Shafi Goldwasser, and Shmuel Safra. Proving Hard-Core Predicates Using List Decoding. In *FOCS*, pages 146–157, 2003.
- 3 Srinivasan Arunachalam, Sourav Chakraborty, Troy Lee, Manaswi Paraashar, and Ronald De Wolf. Two New Results About Quantum Exact Learning. *Quantum*, 5:587, 2021.
- 4 Mitali Bafna, Jack Murtagh, and Nikhil Vyas. Thwarting Adversarial Examples: An L_0 -Robust Sparse Fourier Transform. In *NeurIPS*, volume 31, 2018.
- 5 Eli Ben-Sasson, Noga Ron-Zewi, Madhur Tulsiani, and Julia Wolf. Sampling-Based Proofs of Almost-Periodicity Results and Algorithmic Applications. In *ICALP*, volume 8572, pages 955–966, 2014.
- 6 Anna Bernasconi and Bruno Codenotti. Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem. *IEEE Trans. Computers*, 48(3):345–351, 1999.
- 7 Sourav Chakraborty, Swarnalipa Datta, Pranjal Dutta, Arijit Ghosh, and Swagato Sanyal. On Fourier analysis of sparse Boolean functions over certain Abelian groups, 2024. [arXiv: 2406.18700](#).
- 8 Sourav Chakraborty, Nikhil S. Mande, Rajat Mittal, Tulasimohan Molli, Manaswi Paraashar, and Swagato Sanyal. Tight Chang’s-Lemma-Type Bounds for Boolean Functions. In *FSTTCS*, volume 213, pages 10:1–10:22, 2021.
- 9 Siu On Chan, James R. Lee, Prasad Raghavendra, and David Steurer. Approximate Constraint Satisfaction Requires Large LP Relaxations. *J. ACM*, 63(4):34:1–34:22, 2016.
- 10 Mei-Chu Chang. A polynomial bound in Freiman’s theorem. *Duke Mathematical Journal*, 113(3):399–419, 2002.
- 11 Xue Chen and Anindya De. Reconstruction under outliers for Fourier-sparse functions. In *SODA*, pages 2010–2029, 2020.
- 12 Hamza Fawzi, James Saunderson, and Pablo A Parrilo. Sparse sum-of-squares certificates on finite Abelian groups. In *IEEE Conference on Decision and Control (CDC)*, pages 5909–5914, 2015.

40:16 On Fourier Analysis of Sparse Boolean Functions over Certain Abelian Groups

- 13 Ehud Friedgut, Jeff Kahn, Gil Kalai, and Nathan Keller. Chvátal’s conjecture and correlation inequalities. *J. Comb. Theory, Ser. A*, 156:22–43, 2018.
- 14 Steven D. Galbraith, Joel Laity, and Barak Shani. Finding Significant Fourier Coefficients: Clarifications, Simplifications, Applications and Limitations. *Chic. J. Theor. Comput. Sci.*, 2018, 2018.
- 15 Parikshit Gopalan, Ryan O’Donnell, Rocco A Servedio, Amir Shpilka, and Karl Wimmer. Testing Fourier dimensionality and sparsity. *SIAM Journal on Computing*, 40(4):1075–1100, 2011.
- 16 Ben Green and Tom Sanders. Boolean functions with small spectral norm. *Geometric and Functional Analysis*, 18(1):144–162, 2008.
- 17 Haitham Hassanieh, Piotr Indyk, Dina Katabi, and Eric Price. Nearly optimal sparse Fourier transform. In *STOC*, pages 563–578, 2012.
- 18 Haitham Hassanieh, Piotr Indyk, Dina Katabi, and Eric Price. Simple and practical algorithm for sparse Fourier transform. In *SODA*, pages 1183–1194, 2012.
- 19 Hamed Hatami, Kaave Hosseini, and Shachar Lovett. Structure of protocols for XOR functions. *SIAM Journal on Computing*, 47(1):208–217, 2018.
- 20 Ishay Haviv and Oded Regev. The list-decoding size of Fourier-sparse Boolean functions. *ACM Transactions on Computation Theory*, 8(3):1–14, 2016.
- 21 Kaave Hosseini, Shachar Lovett, and Grigory Yaroslavtsev. Optimality of Linear Sketching Under Modular Updates. In *CCC*, volume 137, pages 13:1–13:17, 2019.
- 22 Nikhil Shekhar Mande and Swagato Sanyal. On Parity Decision Trees for Fourier-Sparse Boolean Functions. *ACM Transactions on Computation Theory*, 16(2):1–26, 2024.
- 23 Ashley Montanaro and Tobias Osborne. On the communication complexity of XOR functions, 2010. [arXiv:0909.3392](https://arxiv.org/abs/0909.3392).
- 24 Lucia Morotti. Reconstruction of Fourier sparse signals over elementary Abelian groups. *Electronic Notes in Discrete Mathematics*, 43:161–167, 2013.
- 25 Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):1–40, 2009.
- 26 Mark Rudelson and Roman Vershynin. On sparse reconstruction from Fourier and Gaussian measurements. *Communications on Pure and Applied Mathematics*, 61(8):1025–1045, 2008.
- 27 Swagato Sanyal. Fourier Sparsity and Dimension. *Theory Comput.*, 15:1–13, 2019.
- 28 Meera Sitharam. Pseudorandom generators and learning algorithms for AC. In *STOC*, pages 478–486, 1994.
- 29 Meera Sitharam and Timothy Straney. Sampling Boolean functions over Abelian groups and applications. *Applicable Algebra in Engineering, Communication and Computing*, 11:89–109, 2000.
- 30 Meera Sitharam and Timothy Straney. Derandomized Learning of Boolean Functions over Finite Abelian Groups. *International Journal of Foundations of Computer Science*, 12(04):491–516, 2001.
- 31 Hing Yin Tsang, Chung Hoi Wong, Ning Xie, and Shengyu Zhang. Fourier Sparsity, Spectral Norm, and the Log-Rank Conjecture. In *FOCS*, pages 658–667, 2013.
- 32 Jianting Yang, Ke Ye, and Lihong Zhi. Computing sparse Fourier sum of squares on finite abelian groups in quasi-linear time, 2023. [arXiv:2201.03912](https://arxiv.org/abs/2201.03912).
- 33 Jianting Yang, Ke Ye, and Lihong Zhi. Fourier sum of squares certificates, 2023. [arXiv:2207.08076](https://arxiv.org/abs/2207.08076).
- 34 Jianting Yang, Ke Ye, and Lihong Zhi. Lower Bounds of Functions on Finite Abelian Groups. In *International Computing and Combinatorics Conference*, pages 157–170, 2023.
- 35 Grigory Yaroslavtsev and Samson Zhou. Fast Fourier Sparsity Testing. In *SOSA*, pages 57–68, 2020.