The Dissertation Committee for Mark J. Lewko
certifies that this is the approved version of the following dissertation:

Combinatorial and Probabilistic Techniques in Harmonic Analysis

Committee:

Jeffrey Vaaler, Supervisor

William Beckner

Natasa Pavlovic

Fernando Rodriguez-Villegas

David Zuckerman

Combinatorial and Probabilistic Techniques in Harmonic Analysis

by

Mark J. Lewko, A.B.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2012

Combinatorial and Probabilistic Techniques in Harmonic Analysis

Publication No. _____

Mark J. Lewko, Ph.D.
The University of Texas at Austin, 2012

Supervisor: Jeffrey Vaaler

We prove several theorems in the intersection of harmonic analysis, combinatorics, probability and number theory. In the second section we use combinatorial methods to construct various sets with pathological combinatorial properties. In particular, we answer a question of P. Erdös and V. Sós regarding unions of Sidon sets. In the third section we use incidence bounds and bilinear methods to prove several new endpoint restriction estimates for the Paraboloid over finite fields. In the fourth and fifth sections we study a variational maximal operators associated to orthonormal systems. Here we use probabilistic techniques to construct well-behaved rearrangements and base changes. In the sixth section we apply our variational estimates to a problem in sieve theory. In the seventh section, motivated by applications to sieve theory, we disprove a maximal inequality related to multiplicative characters.

Table of Contents

Chapter 1

Introduction

In this dissertation we will discuss a number of problems in the intersection of harmonic analysis, combinatorics, number theory and probability. Each of the problems discussed will demonstrate interplay between at least two of these areas. One unifying feature of the problems considered is that they each reduce to understanding, detecting or estimating cancelation in oscillatory quantities.

In the second chapter we investigate the structure of finite sets $A \subseteq \mathbb{Z}$ where $|A+A|$ is large. We present a combinatorial construction that serves as a counterexample to natural conjectures in the pursuit of an "anti-Freiman" theory in additive combinatorics. In particular, we answer a question along these lines posed by O'Bryant. We are also able to construct a $B_2^\circ[2]$ set which is not a finite union of $B_2[g]$ sets, answering a question of Erdős and Sös. Finally, our methods also enable us to construct a $\Lambda(4)$ set which does not contain large $B_2[g]$ or $B_2^\circ[g]$ sets.

In the third chapter we prove certain endpoint restriction estimates for the paraboloid over finite fields. In particular, we slightly improve the range of known exponents for the 'finite field restriction conjecture' in 3 and

higher dimensions. This improves on prior work of Mockenhaupt and Tao, and Iosevich and Koh. A key ingredient here is a bilinear variant of the combinatorial incidence methods used in the earlier work on the problem. As of this writing, these results are the best known towards the conjecture.

In the fourth chapter we investigate the square variation operator V^2 (which majorizes the partial sum maximal operator) on general orthonormal systems (ONS) of size N. In complete generality, we obtain a sharp estimate that refines the classical Rademacher-Menshov theorem. We also obtain a stronger estimate in the case of the trigonometric system, which is also shown to be sharp. We show that for any choice of coefficients, this truncation of the trigonometric system can be rearranged so that the L^2 norm of the associated V^2 operator significantly improves over the standard ordering. We also show that for $p > 2$, a bounded ONS of size N can be rearranged so that the L^2 norm of the V^p operator is very small, uniformly for all choices of coefficients. This refines Bourgain's work on Garsia's conjecture, which is equivalent to the V^∞ case. The V^2 case of this problem is left open (but a variant is considered in the fifth chapter). These later proofs rely on the theory of random selector processes. Our work in this area has already found diverse applications in our work on sieve theory [38] (joint with A. Lewko), Yang and Lyons' work geometric rough processes [69], and Yen, Oberlin, and Eyvindur's work on the bilinear Hilbert transform [70].

In the fifth chapter we revisit the problem raised in the fourth chapter which asks if certain well behaved rearrangements of the trigonometric system

exist. We do not settle that problem, however we do obtain optimal bounds on the analogous problem where one seeks a well-behaved 'base change' instead of a rearrangement. A key ingredient in this work are strong distributional estimates for functions with small Fourier support with respect to a random base change. These estimates are very general and likely will find further applications. The methods are based on theory of Gaussian processes which are better understood than the selector processes that arise in the rearrangement problems (as discussed in chapter four).

In the sixth chapter we prove a variational form of the Barban-Davenport-Halberstam Theorem related to the distribution of prime numbers. A key ingredient in this work is the variational Rademacher-Menshov theorem from chapter four. We use these results to prove a weakened, averaged variant of a conjecture of Erdős regarding the sum of the squares of prime differences.

In the seventh chapter we show that the natural analog of the Carleson-Hunt inequality fails in the multiplicative groups $\mathbb{Z}_n^*$. This problem is motivated by the applications to sieve theory discussed in chapter six. This chapter also discusses the more delicate problem of obtaining optimal quantitative bounds on the multiplicative maximal functions considered.

Many of these results were obtained and appear in joint work with Allison Lewko. See: [36], [37], [38], [39], [40] and [41].

Chapter 2

On the Structure of Sets of Large Doubling

2.1 Introduction

Freiman's theorem [20] states that if a finite set $A \subseteq \mathbb{Z}$ satisfies $|A+A| \leq \delta|A|$ for some constant δ, then A is contained in a generalized arithmetic progression of dimension d and size $c|A|$, where c and d depend only on δ and not on $|A|$. One might then ask about the opposite extreme: if $|A+A| \geq \delta|A|^2$, what can one say about the structure of A as a function only of δ? The natural candidate for the building blocks of such a theory are $B_2[g]$ sets (a set $S \subseteq \mathbb{Z}$ is a $B_2[g]$ set if any integer can be expressed in at most g ways as a sum of two elements in S). It is clear that finite $B_2[g]$ sets are sets of large doubling, but to what extent can we describe all sets of large doubling in terms of $B_2[g]$ sets?

A first attempt at an anti-Freiman theory might be to guess that if $|A + A| \geq \delta|A|^2$ for some positive constant δ, then A can be decomposed into a union of k $B_2[g]$ sets where k and g depend only on δ. This is easily shown to be false. For example, one can start with a $B_2[1]$ set of n elements, and take its union with an arithmetic progression with n elements. One then obtains an A such that $|A + A| \geq \delta|A|^2$ for some δ (independent of n), but the arithmetic

progression contained in A will not be decomposable into a union of k $B_2[g]$ sets with k and g depending only on δ as n tends infinity.

There are two ways we might try to fix this problem: first, we might ask only that A *contains* a $B_2[g]$ set of size $\delta'|A|$, where δ' and g depend only on δ (this question was posed by O'Bryant in [53]). Second, we might ask that $|A' + A'| \geq \delta|A'|^2$ hold for all subsets $A' \subseteq A$ for the same value of δ. Either of these changes would rule out the trivial counterexample given above. However, even applying both of these modifications simultaneously is not enough to make the statement true. We provide a sequence of sets $W_{n,k} \subseteq \mathbb{Z}$ where $|W' + W'| \geq \delta|W'|^2$ holds for all of their subsets W' for the same value of δ, but if we try to express each $W_{n,k}$ as a union of $B_2[g]$ sets for a fixed g, we are forced to let the union size tend to infinity as k tends to infinity. Our sequence of sets also fails to contain large $B_2[g]$ sets. (The parameter n will be chosen sufficiently large with respect to k and g for each k. We include n here for consistency with our later notation.)

Our initial sets $W_{n,k}$ are $B_2^\circ[2]$ sets (a set $S \subseteq \mathbb{Z}$ is a $B_2^\circ[g]$ set if any nonzero integer can be expressed in at most g ways as a difference of two elements in S). This may lead one to make the following weaker anti-Freiman conjecture:

Conjecture 1. (Weak Anti-Freiman) Suppose that $A \subseteq \mathbb{Z}$ is a finite set that satisfies $|A' + A'| \geq \delta|A'|^2$ and $|A' - A'| \geq \delta|A'|^2$ for all subsets $A' \subseteq A$. Then A contains either a $B_2[g]$ set or a $B_2^\circ[g]$ set of size $\geq \delta'|A|$, where g and δ' depend only on δ.

We show that even this very weak conjecture is false.

Our approach to obtaining a counterexample starts with constructing a union of k $B_2[g]$ sets that cannot be decomposed as a union of $k-1$ $B_2[g']$ sets for any g'. This is related to a problem previously studied, with the roles of k and g reversed: Erdős and Newman [14] independently conjectured that for every $g \geq 2$, there exists a $B_2[g]$ set that is not a finite union of $B_2[g-1]$ sets. Erdős [14] established the conjecture for certain values of g using Ramsey theory, and Nešetril and Rödl [51] proved the conjecture for all values of g using arguments based on Ramsey graphs. Instead of considering $B_2[g]$ sets that are not finite unions of $B_2[g-1]$ sets, we fix $g = 1$ and for each k, we construct a union of k $B_2[1]$ sets that is not a union of $k-1$ $B_2[g']$ sets for any g'. The key feature of our construction is that we can precisely control the form of the repeated sums (elements a, b, c, d in our set such that $a + b = c + d$) and repeated differences ($a - b = c - d$), which allows us to keep the sumsets large as we let the union size k tend to infinity.

Our construction is an explicit combinatorial object with many interesting properties, answering several questions about the nature of finite unions of $B_2[g]$ and $B_2^\circ[g]$ sets. In particular, for each positive integer $k \geq 5$, we construct:

1. a $B_2^\circ[2]$ set in $\mathbb{Z}$ which is a union of k $B_2[1]$ sets and cannot be decomposed as a union of $k-1$ $B_2[g]$ sets for any g

2. a $B_2[2]$ set in $\mathbb{Z}$ which is a union of k $B_2^\circ[1]$ sets and cannot be decomposed

as a union of $k-1$ $B_2^\circ[g]$ sets for any g

3. a set in $\mathbb{Z}^2$ which is a direct product of a $B_2[2]$ set in $\mathbb{Z}$ and a $B_2^\circ[2]$ set in $\mathbb{Z}$ and which cannot be expressed as a mixed union of $\frac{k}{3}-1$ $B_2^\circ[g]$ and $B_2[g]$ sets in $\mathbb{Z}^2$

(we say mixed union to simply mean that the union can include *both* $B_2[g]$ and $B_2^\circ[g]$ sets).

In [15], Erdős and Sós asked if there is a $B_2^\circ[g]$ set which is not a finite union of $B_2[1]$ sets. By a standard argument, our finite $B_2^\circ[2]$ sets for each k can be combined to yield an infinite $B_2^\circ[2]$ set which is not a finite union of $B_2[g]$ sets for any g, which provides an answer to this question. In contrast, note that any $B_2^\circ[1]$ set is also a $B_2[1]$ set.

2.1.1 Connection to $\Lambda(4)$ sets

There is a connection between sets of large doubling and $\Lambda(4)$ sets, as illustrated in Lemma 20. If S is a $\Lambda(4)$ set, then $|A+A| \geq \delta|A|$ holds for all finite subsets A of S where δ depends only on S, and not on the choice of A. In his 1960 paper [61], Rudin asked if every $\Lambda(2h)$ set is a finite union of $B_h[g]$ sets (for definitions of $\Lambda(2h)$ sets and $B_h[g]$ sets, see subsection 2.1.3). Rudin's question is natural because any finite union of $B_h[g]$ sets is a $\Lambda(2h)$ set, and most known examples of $\Lambda(2h)$ sets are constructed as finite unions of $B_h[g]$ sets.

Meyer [43] demonstrated a negative answer to Rudin's question by con-

structing a set $E \subseteq \mathbb{Z}$ which is a $\Lambda(p)$ set for all $p > 2$ and is not a finite union of $B_2[g]$ sets. He let $t_0, t_1, t_2, \ldots$ denote a sequence such that $t_{n+1} \geq 3t_n$ for all n and let $E := \{t_n - t_m | 0 \leq m < n\}$. To see this is not a finite union of $B_2[g]$ sets for any g, Meyer considers sums of the form:

$$(t_i - t_j) + (t_j - t_\ell) = t_i - t_\ell,$$

where $\ell < j < i$. Meyer's argument proceeds via a recurrence argument. Alternatively, one can use Ramsey's theorem. We suppose that E is the union of $B_2[g]$ sets $G_1, \ldots, G_k$ for some finite values g, k, and we derive a contradiction. We color the pairs of natural numbers with k colors by giving (i, j) the color c when $t_i - t_j \in G_c$ (for $i > j$). A general version of Ramsey's Theorem (which can be found in [11], for example) says that there must be an infinite monochromatic set $M \subseteq \mathbb{N}$ (meaning that all pairs (i, j) for $i, j \in M$ have the same color). If we take $\ell, i \in M$ such that there are more than g values j such that $\ell < j < i$ and $j \in M$, then we have more than g ways of representing $t_i - t_\ell$ as sum of two elements from the set G_c, where c is the color of M. This contradicts that G_c is a $B_2[g]$ set.

Meyer's set E is not a finite union of $B_2[g]$ sets for any g, yet for some fixed δ, $|A+A| \geq \delta |A|^2$ for all finite $A \subset E$. However, this does not contradict our weak anti-Freiman conjecture, since finite subsets $A \subseteq E$ may still *contain* large $B_2[g]$ sets. More concretely, if we take $t_n = 5^n$ for all n, and A is any finite subset of $E = \{t_n - t_m | 0 \leq m < n\}$, then A must contain a $B_2[2]$ set of size at least $\frac{1}{4}|A|$. To see this, we partition the values $\{t_i\}$ into two disjoint

sets: U and L. We consider the subset A' of A consisting of values $t_i - t_j$ where $t_i \in U$ and $t_j \in L$. A sum of any two such values, e.g. $t_i - t_j + t_{i'} - t_{j'}$ for $t_i, t_i' \in U$, $t_j, t_j' \in L$, will involve no cancelation because $\{i, i'\} \cap \{j, j'\} = \emptyset$. Since base 5 expansions of integers with coefficients in $\{-2, -1, 0, 1, 2\}$ are unique, we will be able to determine the sets $\{i, i'\}$ and $\{j, j'\}$ from the value of the sum. This leaves only two possible ways of expressing the value as a sum of two elements in A': $(t_i - t_j) + (t_{i'} - t_{j'})$ or $(t_i - t_{j'}) + (t_{i'} - t_j)$. Now, if we independently place each t_i in either U or L randomly (probability $1/2$ for each), each element $t_i - t_j$ of A will have probability $\frac{1}{4}$ of ending up in A'. By linearity of expectation, this means the expected size of A' is $\frac{1}{4}|A|$. Hence, there must be a choice of U and L for which $|A'| \geq \frac{1}{4}|A|$.

In [1], Alon and Erdős asked if there exists a set E such that for some fixed $\delta > 0$, every finite subset $A \subset E$ contains a $B_2[1]$ set of size at least $\delta|A|$, but E is not a finite union of $B_2[1]$ sets. In [16], Erdős, Nešetril, and Rödl constructed such a set using sophisticated techniques. Meyer's set is a simpler construction which has a similar property: we have shown that its subsets contain large $B_2[2]$ sets instead of $B_2[1]$ sets.

Our techniques also give a $\Lambda(4)$ set which is not a finite union of $B_2[g]$ sets, and in fact we obtain a stronger negative result for $\Lambda(4)$ sets. We note that it is natural to consider not only $B_2[g]$ sets, but also $B_2^\circ[g]$ sets, since these are $\Lambda(4)$ sets as well. In light of Meyer's result, one may ask the weaker question: *Does a* $\Lambda(4)$ *set at least contain a large* $B_2[g]$ *or* $B_2^\circ[g]$ *set?* A precise version of this question is stated below (see Theorem 3). This statement is

suggested by the following connection with Sidon sets.

Notice that there is no interesting notion of a $\Lambda(\infty)$ set, since a subset of $\mathbb{Z}$ will be a $\Lambda(\infty)$ set (with the obvious extension of our definition below) if and only if it is finite. However, an often useful substitute for $\Lambda(\infty)$ sets are Sidon sets (Sidon sets are a name also attached to $B_2[1]$ sets, but we do not use that convention here). These are sets $S \subset \mathbb{Z}$ satisfying

$$\sum_{\xi \in S} |\hat{f}(\xi)| \leq K_\infty(S) \left|\left| \sum_{\xi \in S} \hat{f}(\xi) e(\xi x) \right|\right|_{L^\infty},$$

where $K_\infty(S)$ is a constant depending on the set S.

Clarifying our assertion that Sidon sets play the role of $\Lambda(\infty)$ sets, Pisier [57] has shown that S is a Sidon subset of $\mathbb{Z}$ if and only if $\sup_{p>2} \frac{K_p(S)}{\sqrt{p}} < \infty$. This can be used to show that finite unions of Sidon sets are Sidon sets. We call a set S independent if, for any distinct set of elements, say $\{s_1, s_2, \ldots, s_h\}$, there is no choice of $+$'s and $-$'s for each s_i such that

$$\pm s_1 \pm s_2 \pm \ldots \pm s_h = 0.$$

One can show that an independent set is a Sidon set, and hence finite unions of independent sets are Sidon sets. One will notice that the definition of independent is somewhat like a limiting case of the condition that the number of representations of an integer as a sum of h elements of the set (and certain generalizations of this) be bounded as h tends to infinity. In the Sidon setting, an obvious analog of Rudin's question is: *Is every Sidon set a finite union*

of independent sets? This question is open (although some progress has been made in other groups), however Pisier has shown that a Sidon set must contain a large independent set in the following sense:

Theorem 2. If $S \subset \mathbb{Z}$ is a Sidon set, then there exists a constant $\delta > 0$ so that for every finite subset $A \subset S$, there is an independent set $I \subseteq A$ satisfying $|I| \geq \delta |A|$.

In light of Pisier's theorem, one might ask if it is the case that a $\Lambda(4)$ set must contain a large $B_2[g]$ or $B_2^\circ[g]$ set. We show that the analog of Pisier's theorem fails in the $\Lambda(4)$ setting:

Theorem 3. There exists a $\Lambda(4)$ set $S \subset \mathbb{Z}$ such that for any fixed choice of $\delta > 0$ and g, there exists a finite subset A of S such that no subset A' of A satisfying $|A'| \geq \delta |A|$ is a $B_2[g]$ or $B_2^\circ[g]$ set.

We note that this result cannot be obtained from Meyer's set E, since any finite subset of E contains a large $B_2[2]$ set, as discussed above.

2.1.2 Related Work

We are aware of two other constructions of $\Lambda(4)$ sets which are not known to be finite unions of $B_2[g]$ sets. In [3], Bourgain probabilistically proved the existence of a $\Lambda(4)$ set S such that $|[0, n] \cap S| \gg n^{1/2}$ for every $n \in \mathbb{N}$. A theorem of Erdős (see [23], Theorem 8 on page 89) states that if A is a $B_2[1]$ set, then

$$|A \cap [0,n]| \ll \frac{n^{1/2}}{\ln^{1/2}(n)} \tag{2.1}$$

for infinitely many n. It follows from this that Bourgain's set is not the finite union of $B_2[1]$ sets. This observation essentially appears in [5]. If one could show (for infinitely many n) that

$$|A \cap [0,n]| = o(n^{1/2})$$

whenever A is a $B_2[g]$ set, it would follow that Bourgain's set is not a finite union of $B_2[g]$ sets. Such strong estimates are not currently known.

In [34], Klemes constructed an example of a $\Lambda(4)$ set using an intricate selection algorithm based on a tree structure. While he was able to establish that his set was a $\Lambda(4)$ set without deciding if his set was a finite union of $B_2[g]$ sets, he conjectured that the set could in fact be decomposed in this way.

2.1.3 Preliminaries

We now give formal definitions of $B_h[g]$ sets, $B_2^\circ[g]$, and $\Lambda(p)$ sets. We define these for all $2 < p < \infty$ and all positive integer values of h, although here we will only be concerned with $h = 2$ and $p = 4$. Below, d denotes a positive integer, and $\mathbb{Z}^d$ denotes the additive group of tuples of d integers.

$\mathbf{B_h[g]}$ sets A set $S \subseteq \mathbb{Z}^d$ is called a $B_h[g]$ set if the number of representations of every $\xi \in \mathbb{Z}^d$ as a sum $\xi = \nu_1 + \ldots + \nu_h$ for $\nu_1, \ldots, \nu_h \in S$ is at most $h!g$. The $h!$ is a matter of notational convenience (essentially, we do not wish to count

reorderings of summands separately). In particular, a $B_2[g]$ set in $\mathbb{Z}$ is a set such that any integer can be expressed as a sum of two elements in the set in at most g ways (where exchanging the order of the summands does not count as a new representation). We note that for a $B_2[1]$ set, all sums are unique.

$\mathbf{B_2^\circ[g]}$ sets A set $S \subseteq \mathbb{Z}^d$ is called a $B_2^\circ[g]$ set if every nonzero element of $\mathbb{Z}^d$ can be expressed as a difference of two elements of S in at most g ways. (We note that there are always many representations of 0 as $a - a$, $b - b$, and so on.)

$\mathbf{\Lambda(p)}$ sets Let $\mathbb{T}^d$ denote the d-dimensional torus. For a measurable complex-valued function f on $\mathbb{T}^d$, we define its L^p norm as $||f||_{L^p} = \left(\int_{\mathbb{T}^d} |f(x)|^p dx\right)^{1/p}$. We denote the space of all measurable complex-valued functions on $\mathbb{T}^d$ with finite L^p norm as $L^p(\mathbb{T}^d)$. Defining $e(x) := e^{2\pi i x}$, we have that a function $f \in L^2(\mathbb{T}^d)$ can be expressed as a Fourier series

$$f(x) \approx \sum_{\xi \in \mathbb{Z}^d} \hat{f}(\xi) e(\xi \cdot x).$$

To avoid issues regarding the convergence of the sum defining the series, one could always take f such that $\hat{f}(\xi)$ has finite support (i.e. trigonometric polynomials) in what follows. This restriction suffices since we are interested in establishing L^p inequalities, and functions with finitely supported Fourier expansions form a dense subspace of $L^p(\mathbb{T}^d)$. In [61], Rudin defined a subset

of $S \subseteq \mathbb{Z}^d$ to be a $\Lambda(p)$ set, for $p > 2$, if there exists a constant $K_p(S)$ such that

$$||f||_{L^p} \leq K_p(S)||f||_{L^2} \tag{2.2}$$

whenever $\text{supp}(\hat{f}) \subseteq S$. When we wish to emphasize the dimension d of the set S, we will write $K_p^d(S)$.

When p is an even integer, say $p = 2h$, one can expand the left-hand side of (2.2) and obtain

$$||f||_{L^{2h}}^h = \left|||f|^h\right|_{L^2} = \left(\sum_{\xi\in\mathbb{Z}^d}\left|\sum_{\substack{\xi=\nu_1+\ldots+\nu_h\\ \nu_1,\ldots,\nu_h\in S}}\hat{f}(\nu_1)\hat{f}(\nu_2)\ldots\hat{f}(\nu_h)\right|^2\right)^{1/2}$$

$$\leq \left(\sum_{\xi\in\mathbb{Z}^d}(R_h(\xi,S))^2\sup_{\substack{\left|\hat{f}(\nu_1)\hat{f}(\nu_2)\ldots\hat{f}(\nu_h)\right|^2\\ \xi=\nu_1+\ldots+\nu_h}}\left|\hat{f}(\nu_1)\hat{f}(\nu_2)\ldots\hat{f}(\nu_h)\right|^2\right)^{1/2}$$

$$\leq \sup_{\xi\in\mathbb{Z}^d}R_h(\xi,S)\left(\sum_{\nu\in\mathbb{Z}^d}|\hat{f}(\nu)|^2\right)^{h/2} \leq \sup_{\xi\in\mathbb{Z}^d}R_h(\xi,S)\,||f||_{L^2}^h\,, \tag{2.3}$$

where $R_h(\xi,S)$ denotes the number of representations of $\xi \in \mathbb{Z}^d$ as a sum $\xi = \nu_1 + \ldots + \nu_h$ for $\nu_1,\ldots,\nu_h \in S$. Thus any set S with the property that $R_h(\xi,S) \leq h!g < \infty$ is a $\Lambda(2h)$ set. In particular, every finite set is a $\Lambda(p)$ set for every $p > 2$.

We have now shown that every $B_h[g]$ set is a $\Lambda(2h)$ set. One might ask if every $\Lambda(2h)$ set is a $B_h[g]$ set. This is easily seen to be false. Notice that the union of two $\Lambda(p)$ sets, say $S = S_1 \cup S_2$, is also a $\Lambda(p)$ set. Letting $K_p(S_1)$ and $K_p(S_2)$ denote the $\Lambda(p)$ constants of the sets S_1 and S_2 respectively, for any f with $\hat{f}$ supported on S, the triangle inequality gives:

$$||f||_{L^p} = \left|\left| \sum_{\nu_1 \in S_1} \hat{f}(\nu_1) e(\nu_1 \cdot x) + \sum_{\nu_2 \in S_2 \setminus S_1} \hat{f}(\nu_2) e(\nu_2 \cdot x) \right|\right|_{L^p}$$

$$\leq \left|\left| \sum_{\nu_1 \in S_1} \hat{f}(\nu_1) e(\nu_1 \cdot x) \right|\right|_{L^p} +$$

$$\left|\left| \sum_{\nu_2 \in S_2 \setminus S_1} \hat{f}(\nu_2) e(\nu_2 \cdot x) \right|\right|_{L^p} \leq (K_p(S_1) + K_p(S_2)) \, ||f||_{L^2} \, . \tag{2.4}$$

Now we note that $S_1 = \{2^i : i \in \mathbb{N}\}$ and $S_2 = \{-2^j : j \in \mathbb{N}\}$ are each $B_2[1]$ sets but $S_1 \cup S_2$ is not a $B_2[g]$ for any finite g. The next natural question is Rudin's question: is every $\Lambda(2h)$ set a finite union of $B_h[g]$ sets? (Rudin asked this only for dimension $d = 1$, but it follows from the methods described below and a standard compactness argument that a counterexample in any dimension can be transformed into a counterexample in every other dimension.) Meyer's counterexample [43] shows that the answer to this question is no for all $h \geq 2$.

2.2 A First Attempt at a Combinatorial Construction

In [14], Erdős constructed a $B_2[3]$ set that is not a finite union of $B_2[g]$ sets for $g < 3$, which he proved by applying Ramsey theory. He conjectured that for any g, there exists a $B_2[g]$ set A that is not a finite union of $B_2[g-1]$ sets. This was later proven for all g by Nešetril and Rödl [51]. Informally, this result means that one cannot always tradeoff a larger union size to obtain a lower value of g when representing a set as a finite union of $B_2[g]$ sets.

Our approach to the anti-Freiman problem is to begin by solving a variant of Erdős' problem where the roles of g and the union size are switched. Informally put, we seek to prove that one cannot always tradeoff a higher value of g to obtain a smaller union size when representing a set as a finite union of $B_2[g]$ sets.

As a first attempt, we consider a Ramsey-theoretic approach, much like Erdős and somewhat reminiscent of Meyer's set E. For each positive integer k, we will construct an infinite $S \subseteq \mathbb{Z}$ such that S is a union of 2^k $B_2[2^{k-1}]$ sets, but not a union of $2^k - 1$ $B_2[g']$ sets for any constant g'. The undesirable feature of this construction is that the value of g is a function of k. This dependence of g on k is removed from our main construction in the next section, where we are able to fix $g = 1$, but it is instructive to consider this simpler construction first.

Proposition 4. For every positive integer k, there exists a set $S \subseteq \mathbb{Z}$ such that S is a union of 2^k $B_2[2^{k-1}]$ sets, and S cannot be decomposed as a union of $2^k - 1$ $B_2[g']$ sets for any finite g'.

Proof. We first define k disjoint sequences of positive integers, $X_1 = \{x_i^1\}_{i=1}^{\infty}$, $X_2 = \{x_i^2\}_{i=1}^{\infty}$, ..., $X_k = \{x_i^k\}_{i=1}^{\infty}$, where each consists of powers of 5. For concreteness, we can take X_j to be the sequence $\{5^{ik+j}\}_{i=1}^{\infty}$ for each j. We note that base 5 expansions of integers with coefficients in $\{-2, -1, 0, 1, 2\}$ are unique.

We let $v_1, \ldots, v_{2^k} \in \{1, -1\}^k$ denote all of the distinct vectors of length k with entries in $\{1, -1\}$. For j from 1 to k, we define the set

$$S_j := \{(x^1, x^2, \ldots, x^k) \cdot v_j \mid x^1 \in X_1, \ldots, x^k \in X_k\}.$$

We set $S := \bigcup_{j=1}^{k} S_j$. We note that each element of S has a unique representation as $(x^1, \ldots, x^k) \cdot v_j$ for $x^1 \in X_1, \ldots, x^k \in X_k$ and $1 \leq j \leq 2^k$.

We claim that each S_j is a $B_2[g]$ set, for $g = 2^{k-1}$. To see why, we consider adding two elements of S_j:

$$(x^1, x^2, \ldots, x^k) \cdot v_j + (y^1, y^2, \ldots, y^k) \cdot v_j = (x^1 + y^1, x^2 + y^2, \ldots, x^k + y^k) \cdot v_j.$$

Here, $x^1, y^1 \in X_1$, $x^2, y^2 \in X_2, \ldots, x^k, y^k \in X_k$. Recalling that the sequences $X_1, \ldots, X_k$ are disjoint sequences of powers of 5, we see that this is a base 5 expansion of an integer with coefficients in $[-2, 2]$ (coefficients of 2 or -2 will appear only where $x^i = y^i$). Since these expansions are unique, this sum uniquely determines the values of $x^1, y^1, x^2, y^2, \ldots, x^k, y^k$, up to exchanges of x^i and y^i. In other words, it determines the unordered sets $\{x^i, y^i\}$ for i from 1 to k. There are 2^k ways to choose two elements of S_j which match these sets: for each set $\{x^i, y^i\}$, we must decide whether x^i will be included in the first or second element. Thus, each S_j is a $B_2[2^{k-1}]$ set.

Now we prove that S cannot be decomposed into $2^k - 1$ $B_2[g']$ sets for any g'. We suppose that S can be decomposed into $2^k - 1$ $B_2[g']$ sets, $A_1, \ldots, A_{2^k-1}$, and proceed to derive a contradiction. We will use this decomposition to give a $\binom{2^k}{2}$-coloring of all k-element subsets of $\mathbb{N}$.

To color the set $(i_1, \ldots, i_k)$ for $i_1 < i_2 < \ldots < i_k$, we consider the following 2^k elements of S:

$$(x^1_{i_1}, x^2_{i_2}, \ldots, x^k_{i_k}) \cdot v_1 \in S_1,$$

$$\vdots$$

$$(x^1_{i_1}, x^2_{i_2}, \ldots, x^k_{i_k}) \cdot v_{2^k} \in S_{2^k}.$$

Since we have decomposed S into $2^k - 1$ sets, some pair of these elements must belong in the same A_n. We color $(i_1, \ldots, i_k)$ according to which pair this is (if several pairs are in the same A_n, we choose one arbitrarily). For example, if the element of S_1 and the element of S_2 are placed in the same A_n, we may assign the color corresponding to the pair (1,2).

Since we are coloring k-element subsets of $\mathbb{N}$ with finitely many colors, a general version of Ramsey's Theorem (again, this can be found in e.g. [11]) tells us that there exists an infinite monochromatic set $M \subseteq \mathbb{N}$. This means that for any two k-element subsets of M, the color assigned to them is the same. We call this single color $c(M)$.

Now, $c(M)$ corresponds to a pair (i, j) of indices between 1 and 2^k. We note that the corresponding vectors v_i and v_j differ in some coordinate ℓ

(i.e. $v_i + v_j = 0$ in the ℓ^{th} coordinate). We consider k-element subsets of M: $(m_1 < m_2 < \ldots < m_k)$.

We consider fixing elements of M in the indices $\neq \ell$ and letting the element m_ℓ vary over M (while satisfying the ordering condition). For each value of m_ℓ, we get two corresponding elements of some A_n whose sum is equal to

$$(x^1_{m_1}, \ldots, x^k_{m_k}) \cdot (v_i + v_j),$$

which does not depend on m_ℓ. Since M is infinite, the number of values of m_ℓ satisfying the ordering relation $m_1 < \ldots < m_k$ can be made arbitrarily large. This means that one of $A_1, \ldots, A_{2^k-1}$ must contain arbitrarily many pairs of elements with the same sum, which contradicts that it is a $B_2[g']$ set for some fixed g'.

□

2.3 Our Main Construction

We now give our main construction, which improves upon our initial construction as described in the last section. Our previous construction had the undesirable feature that our value of g grew as function of our union size. This was due to the fact that a sum of two elements both from the same S_j uniquely determined the pairs of values from each of the sequences $X_1, \ldots, X_k$ going into it, but these could be recombined arbitrarily to get another occurrence of the same sum. We will overcome this problem by introducing an error

correcting code, which will enforce that the occurrence of the sum is unique. We do not need to adapt our Ramsey theory argument to this more complex situation, since an alternative counting argument replaces it.

We construct, for each positive integer k, a union of k $B_2[1]$ sets which is not a union of $k-1$ $B_2[g]$ sets for any finite g. This resolves the variant of Erdős' problem mentioned above, showing that one cannot always reduce the union size of a finite union of $B_2[1]$ sets, even if one is willing to use $B_2[g]$ sets for an arbitrarily high g. Extending this result to $B_h[g]$ sets for values of $h > 2$ is an interesting problem which we do not address.

We begin by defining k vectors $v_1, \ldots, v_k \in \{+1, -1\}^d$ with two key properties. First, we require that for each $i \neq j$, $v_i + v_j$ has $> \frac{d}{2}$ coordinates equal to 0 (in other words, these vectors form an error correcting code with relative distance strictly greater than $\frac{1}{2}$). Second, we require the values $v_i + v_j$ to be distinct (i.e. $v_i + v_j = v_h + v_\ell$ holds if and only if the sets $\{i, j\}$ and $\{h, \ell\}$ are equal). Such vectors can be easily constructed from Hadamard matrices when $d = 2^j - 1$ for some j such that $2^j \geq k$.

Lemma 5. For any fixed positive integer k and for $d = 2^j - 1$ such that $2^j \geq k$, there exist vectors $v_1, \ldots, v_k \in \{1, -1\}^d$ such that the pairwise vector sums $v_i + v_j$ are distinct, and have $> \frac{d}{2}$ 0's when $i \neq j$.

Proof. We let H be a $2^j \times 2^j$ Hadamard matrix with all 1's in its first column (these can be recursively constructed, and are also known as Walsh matrices). This matrix has entries in $\{1, -1\}$, and any two distinct rows are orthogonal.

We take $v_1, \ldots, v_k$ to be the first k rows of H, where we omit from each the first column's entry, which is always equal to 1. These are distinct vectors of length $d = 2^j - 1$, and we claim that each $v_i + v_j$ for $i \neq j$ has $> \frac{d}{2}$ 0's. To see why, we note that $v_i \cdot v_j = -1$ (because the rows of H are orthogonal and we have omitted the initial 1's), and each coordinate of v_i, v_j contributes 1 to $v_i \cdot v_j$ if v_i and v_j are equal in this coordinate, and contributes -1 if they are unequal. Hence, v_i and v_j must be unequal in strictly more than half the coordinates, so $v_i + v_j$ has $> \frac{d}{2}$ 0's.

We now suppose that $v_i + v_j = v_h + v_\ell$ and that $i \notin \{h, \ell\}$. Then we have:

$$v_i \cdot (v_h + v_\ell) = v_i \cdot v_h + v_i \cdot v_\ell = -1 - 1 = -2.$$

However,

$$v_i \cdot (v_i + v_j) = v_i \cdot v_i + v_i \cdot v_j = d - 1 > -2,$$

so we have a contradiction. Thus, $i \in \{h, \ell\}$. It follows that $\{i, j\} = \{h, \ell\}$. $\square$

We now define d disjoint sequences of positive integers, $X_1 = \{x_i^1\}_{i=1}^\infty$, $X_2 = \{x_i^2\}_{i=1}^\infty$, ..., $X_d = \{x_i^d\}_{i=1}^\infty$, where each consists of powers of 5. For concreteness, we take X_j to be the sequence $\{5^{id+j}\}_{i=1}^\infty$ for each j. We additionally define an infinite set $S \subset \mathbb{N}^d$ as follows. We let M be the $d \times \lceil \frac{d}{2} \rceil$ Vandermonde matrix:

$$M = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 2^2 & \ldots & 2^{\lceil \frac{d}{2} \rceil - 1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & d & d^2 & \ldots & d^{\lceil \frac{d}{2} \rceil - 1} \end{pmatrix}$$

We note that any $\lceil \frac{d}{2} \rceil$ rows of the matrix form an invertible $\lceil \frac{d}{2} \rceil \times \lceil \frac{d}{2} \rceil$ Vandermonde matrix. We also note that invertibility remains even if we reduce the entries modulo any prime which is $> d$ (because $1, \ldots, d$ will have distinct modular reductions). By Bertrand's Postulate, we know such a prime exists which is $\leq 2d$. Hence, we obtain a reduced matrix M with positive entries $< 2d$ such that any $\lceil \frac{d}{2} \rceil$ rows form an invertible matrix (invertible over $\mathbb{R}$).

We now define S as:

$$S := \left\{ M \cdot (i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil})^t : (i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil}) \in \mathbb{N}^{\lceil \frac{d}{2} \rceil} \right\}.$$

(We use the notation $(i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil})^t$ to denote the transpose, i.e. $(i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil})^t$ denotes a column vector whose first entry is i'_1, etc.) The key property of S that we will use is that if we are given at least half of the coordinates of some tuple $(i_1, \ldots, i_d) \in S$, we can uniquely solve for the remaining coordinates (by solving a linear system of $\lceil \frac{d}{2} \rceil$ linearly independent equations in $\lceil \frac{d}{2} \rceil$ unknowns). In other words, S is an error-correcting code. (More precisely, a Vandermonde matrix modulo a prime p is the generating matrix for a Reed-Solomon code over $\mathbb{F}_p$.)

For each j from 1 to k, we define $W_j \subset \mathbb{Z}$ as:

$$W_j := \{(x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_j : (i_1, \ldots, i_d) \in S\}.$$

In other words, an element of W_j is formed by taking a d-tuple in S, using the coordinates as indices into the d disjoint sequences $X_1, \ldots, X_d$, and taking the linear combination of the corresponding values with coefficients equal to the coordinates of v_j.

We will prove that each W_j is a $B_2[1]$ set, and that $W := W_1 \cup W_2 \cup \ldots \cup W_k$ is a union of k $B_2[1]$ sets that cannot be decomposed as a union of $k-1$ $B_2[g]$ sets for any finite value of g. (We note that W and S are defined with respect to a fixed k, and we leave this dependence implicit. In other words, W and S actually represent a family of constructions, parameterized by k.) We start by proving some useful lemmas.

Lemma 6. Each element of W has a unique expression as $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_j$ for $(i_1, \ldots, i_d) \in S$ and $1 \leq j \leq k$. In particular, the sets W_j are disjoint.

Proof. This simply follows from the fact that base 5 expansions of integers with coefficients in $\{-2, -1, 0, 1, 2\}$ are unique. Any value of the form $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_j$ has a base 5 expansion with coefficients in $\{-1, 0, 1\}$. From this expansion, we can uniquely determine the values of $x_{i_1}^1, \ldots, x_{i_d}^d$ and the coordinates of v_j. □

Next, we will obtain a precise characterization of the repeated sums and differences in W. We start with the following lemma:

Lemma 7. The sets $W_i + W_j$ $(1 \leq i, j \leq k)$ are disjoint. In other words, $W_i + W_j$ intersects $W_h + W_\ell$ if and only if $\{i, j\}$ and $\{h, \ell\}$ are equal.

Proof. Again, this follows from the fact that base 5 expansions of integers with coefficients in $\{-2, -1, 0, 1, 2\}$ are unique. We suppose that $\{i, j\} \neq \{h, \ell\}$, so (from Lemma 5) we have that $v_i + v_j \neq v_h + v_\ell$. Without loss of generality, we suppose that $v_i + v_j$ and $v_h + v_\ell$ differ in the first coordinate.

We suppose that $W_i + W_j$ intersects $W_h + W_\ell$. This means that there exist tuples $(i_1, \ldots, i_d), (j_1, \ldots, j_d), (h_1, \ldots, h_d), (\ell_1, \ldots, \ell_d) \in S$ such that:

$$(x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_i + (x^1_{j_1}, \ldots, x^d_{j_d}) \cdot v_j = (x^1_{h_1}, \ldots, x^d_{h_d}) \cdot v_h + (x^1_{\ell_1}, \ldots, x^d_{\ell_d}) \cdot v_\ell.$$

Since base 5 expansions with coefficients in $[-2, 2]$ are unique, we must have the same contribution of terms from sequence X_1 on both sides. This can only occur when the set of the first coordinates of v_i, v_j and the set of the first coordinates of v_h, v_ℓ contain the same number of +1's and -1's, i.e. when $v_i + v_j$ and $v_h + v_\ell$ agree in the first coordinate. This contradicts our assumption that $v_i + v_j$ and $v_h + v_\ell$ differ in the first coordinate, so we have shown that $W_i + W_j$ and $W_h + W_\ell$ are disjoint when $v_i + v_j \neq v_h + v_\ell$, i.e. when $\{i, j\} \neq \{h, \ell\}$. □

We now prove a very helpful general lemma. We let $\phi : S \to \mathbb{Z}^d$ denote the map which takes a d-tuple $(i_1, \ldots, i_d)$ in S to the vector $(x^1_{i_1}, \ldots, x^d_{i_d}) \in \mathbb{Z}^d$. We note that each element of our set W can be expressed as $\phi(M \cdot y) \cdot v_i$ for some i and some vector $y \in \mathbb{Z}^{\lceil \frac{d}{2} \rceil}$, where M is the matrix described above.

Lemma 8. We let v'_i and v'_j denote **any two vectors** in $\{+1, -1\}^d$. We suppose that $y, z, y', z' \in \mathbb{Z}^{\lceil \frac{d}{2} \rceil}$ satisfy:

$$\phi(M \cdot y) \cdot v'_i + \phi(M \cdot z) \cdot v'_j = \phi(M \cdot y') \cdot v'_i + \phi(M \cdot z') \cdot v'_j.$$

If $v'_i + v'_j$ is equal to 0 in $\geq \frac{d}{2}$ coordinates, then either $y = y'$ and $z = z'$ or $y = z$ and $y' = z'$. If $v'_i + v'_j$ is non-zero in $\geq \frac{d}{2}$ coordinates, then either $y = y'$ and $z = z'$ or $y = z'$ and $z = y'$.

Proof. We let C denote the value $\phi(M \cdot y) \cdot v'_i + \phi(M \cdot z) \cdot v'_j$, which is equal to $\phi(M \cdot y') \cdot v'_i + \phi(M \cdot z') \cdot v'_j$. We consider the base 5 expansion of C with coefficients in $[-2, 2]$. We let $n \in [d]$ denote a coordinate where $v'_i + v'_j$ is equal to 0. If the base 5 expansion of C includes no terms from the sequence X_n, we may conclude that the n^{th} coordinate of $M \cdot y$ and the n^{th} coordinate of $M \cdot z$ are equal. In other words, if we let M_n denote the n^{th} row of M, we have that $y - z$ is orthogonal to M_n, as is $y' - z'$. We let $EQUAL$ denote the set of coordinates n where $v'_i + v'_j$ is equal to 0 and no terms from X_n appear in our base 5 expansion of C. We let $Null(EQUAL)$ denote the space in $\mathbb{R}^{\lceil \frac{d}{2} \rceil}$ of vectors orthogonal to all the rows M_n of M for $n \in EQUAL$. Then we have shown so far that $y - z$ and $y' - z'$ are in $Null(EQUAL)$.

We now consider a coordinate $n \in [d]$ where $v'_i + v'_j = 0$ but we see two terms (of opposite sign) from the sequence X_n in the base 5 expansion of C. Since these terms have different signs, we can tell which came from dotting with v'_i and which came from dotting with v'_j. Thus, we must have that the n^{th} coordinate of $M \cdot y$ and the n^{th} coordinate of $M \cdot y'$ are equal, and similarly, the n^{th} coordinates of $M \cdot z$ and $M \cdot z'$ must be equal. Thus, $y - y'$ and $z - z'$ are both orthogonal to M_n. We define the set $SAME$ to include all such coordinates n, and we let $Null(SAME)$ denote the space in $\mathbb{R}^{\lceil \frac{d}{2} \rceil}$ of vectors orthogonal to all the rows M_n of M for $n \in SAME$. We have shown that $y - y', z - z' \in Null(SAME)$.

Next, we consider a coordinate $n \in [d]$ where $v'_i + v'_j \neq 0$. In such coordinates, we see two terms of the same sign from the sequence X_n in the

base 5 expansion of C. There are then two possibilities: either $y-y'$ and $z-z'$ are both orthogonal to M_n, or $y-z'$ and $z-y'$ are both orthogonal to M_n. If $y-y'$ and $z-z'$ are both orthogonal to M_n, we add n to the set $SAME$. If this does not hold, then we must have $y-z'$ and $z-y'$ both orthogonal to M_n, and we define a new set $DIFF$ to include such coordinates n. We let $Null(DIFF)$ denote the space in $\mathbb{R}^{\lceil \frac{d}{2} \rceil}$ of vectors orthogonal to all the rows M_n of M for $n \in DIFF$. Then we have that $y-z', z-y' \in Null(DIFF)$. We note that we have defined the sets $EQUAL$, $SAME$, and $DIFF$ so that they are disjoint, and their union is $[d]$ (all of the d coordinates).

We now examine 4 possible cases:

1. $|EQUAL| \geq \frac{d}{2}$
2. $|SAME| \geq \frac{d}{2}$
3. $|DIFF| \geq \frac{d}{2}$
4. $|EQUAL|, |SAME|, |DIFF| \leq \frac{d}{2}$.

In case 1., $y-z$ and $y'-z'$ are each orthogonal to at least $\frac{d}{2}$ rows of M, so we must have $y=z$ and $y'=z'$. In case 2., $y-y'$ and $z-z'$ are each orthogonal to at least $\frac{d}{2}$ rows of M, so we must have $y=y'$ and $z=z'$. In case 3., $y-z'$ and $z-y'$ are each orthogonal to at least $\frac{d}{2}$ rows of M, so we must have $y=z'$ and $z=y'$.

In case 4., we note that $y-y'+z-z' \in Null(SAME) \cup Null(DIFF)$, $y-z+y'-z' \in Null(EQUAL) \cup Null(DIFF)$, and $y-y'-z+z' \in$

$Null(SAME) \cup Null(EQUAL)$. Since $|EQUAL|, |SAME|, |DIFF| \leq \frac{d}{2}$, we have that $|SAME \cup DIFF|, |EQUAL \cup DIFF|, |SAME \cup EQUAL|$ are all $\geq \frac{d}{2}$. Hence, we have that: $y - y' + z - z' = 0 = y - z + y' - z' = y - y' - z + z'$, which implies that $y = y' = z = z'$.

Now, if $v'_i + v'_j$ is equal to 0 in $\geq \frac{d}{2}$ coordinates, then being exclusively in case 3. is impossible. Thus, we may conclude that either $y = y'$ and $z = z'$ or $y = z$ and $y' = z'$. If $v'_i + v'_j$ is nonzero in $\geq \frac{d}{2}$ of the coordinates, then being exclusively in case 1. is impossible, so either $y = y'$ and $z = z'$ or $y = z'$ and $z = y'$.

□

This lemma has a few useful corollaries:

Corollary 9. Each W_i is a $B_2[1]$-set.

Proof. We apply Lemma 8 with $v'_i = v_i$ and $v'_j = v_i$. Since $2v_i$ is nonzero in all d coordinates, we can conclude that either $y = y'$ and $z = z'$ or $y = z'$ and $z = y'$. This means that if $a + b$ is a sum of two elements of W_i, the only other way to express it as a sum of two elements of W_i is as $b + a$. Hence W_i is a $B_2[1]$ set. □

Corollary 10. W is a $B_2^\circ[2]$-set.

Proof. We suppose that we have y, z, y', z' such that

$$\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_j = \phi(M \cdot y') \cdot v_h - \phi(M \cdot z') \cdot v_\ell.$$

By the same argument employed in the proof of Lemma 7, this can only occur when $v_i - v_j = v_h - v_\ell$, i.e. when $v_i + v_\ell = v_h + v_j$. Since the sums of these vectors are unique, we must have either:

1. $v_i = v_h$ and $v_j = v_\ell$ (and $i \neq j$) or

2. $v_j = v_i$ and $v_h = v_\ell$.

In case 1., we have: $\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_j = \phi(M \cdot y') \cdot v_i - \phi(M \cdot z') \cdot v_j$. We then apply Lemma 8 with $v'_i = v_i$ and $v'_j = -v_j$. Then $v'_i + v'_j$ is nonzero in more than half of the coordinates (since $i \neq j$), so either $y = y'$ and $z = z'$ or $y = z'$ and $z = y'$. This gives us at most two ways of representing this value as a difference of two elements of W.

In case 2., we have: $\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_i = \phi(M \cdot y') \cdot v_h - \phi(M \cdot z') \cdot v_h$. We can rearrange this to be:

$$\phi(M \cdot y) \cdot v_i + \phi(M \cdot z') \cdot v_h = \phi(M \cdot z) \cdot v_i + \phi(M \cdot y') \cdot v_h.$$

We then apply Lemma 8 with $v'_i = v_i$, and $v'_j = v_h$ and the roles of y, z, y', z' appropriately exchanged. If $i = h$, then $v_i + v_h$ is nonzero in all of the coordinates. In this case, we conclude that either $y = z$ and $y' = z'$ (in which case, the difference $\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_i$ is 0), or $y = y'$ and $z = z'$ (in which case, we are looking at the very same representation of the difference). Neither of these cases results in an alternate way of expressing a nonzero element as a difference of elements in W.

If $i \neq h$, then $v_i + v_h$ is 0 in more than half of the coordinates. We conclude that either $y = z$ and $y' = z'$ (again, the difference being represented is then equal to 0), or $y = z'$ and $z = y'$. In this case, we see that we may have two ways of representing a nonzero value as a difference of two elements of W. We then ask, could we have more? In other words, could we have distinct representations

$$\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_i = \phi(M \cdot z) \cdot v_h - \phi(M \cdot y) \cdot v_h = \phi(M \cdot u) \cdot v_\ell - \phi(M \cdot w) \cdot v_m$$

for some u, w, v_ℓ, v_m where $y \neq z$? We first note that $v_m = v_\ell$ must then hold, again by the agrument employed in Lemma 7.

This gives us:

$$\phi(M \cdot y) \cdot v_i - \phi(M \cdot z) \cdot v_i = \phi(M \cdot z) \cdot v_h - \phi(M \cdot y) \cdot v_h = \phi(M \cdot u) \cdot v_\ell - \phi(M \cdot w) \cdot v_\ell.$$

Applying the argument above with v_i and v_ℓ instead of v_h, we conclude that if $y \neq z$, we must have $u = z$ and $w = y$. However, if we apply the above argument to v_h and v_ℓ instead, we conclude that $u = y$ and $w = z$. Since these must simultaneously hold, we get that $y = z$, which is a contradiction. Putting it all together, we have now proven that only 0 can be represented as a difference of two elements of W in more than 2 ways, so W is a $B_2^\circ[2]$ set.

□

We now have a rather complete understanding of the sums and differences of W. We have shown that W is a $B_2^\circ[2]$ set and is a union of k $B_2[1]$ sets. We also know that W is not a $B_2[g]$ set for any g, since Lemma 8 does

reveal some repeated sums in W. For each $i \neq j$, we can get many representations of a single integer as a sum of an element in W_i and an element of W_j by examining sums of the form $\phi(M \cdot y) \cdot v_i + \phi(M \cdot y) \cdot v_j$. The value of this sum will only depend on the coordinates of $M \cdot y$ for which $v_i + v_j$ is nonzero, and this is less than half of the coordinates. This means that the sum does not fully determine y: in fact, there are infinitely many values y' such that $M \cdot y'$ will agree with $M \cdot y$ in these coordinates where $v_i + v_j \neq 0$. This shows that for $i \neq j$, $W_i \cup W_j$ is not a $B_2[g]$ set for any g. Lemma 8 also tells us that these repeated sums of the form $\phi(M \cdot y) \cdot v_i + \phi(M \cdot y) \cdot v_j = \phi(M \cdot y') \cdot v_i + \phi(M \cdot y') \cdot v_j$ are the *only repeated sums* in $W + W$. Essentially, this means that $W' + W'$ will still be large for any subset W' of W, even though W is not a $B_2[g]$ set for any g. In fact, W is not a union of $k-1$ $B_2[g]$ sets for any g, which we prove next:

Lemma 11. $W := W_1 \cup W_2 \cup \ldots \cup W_k$ is not a union of $k-1$ $B_2[g]$ sets, for any finite g.

Proof. We suppose that this is not true, i.e. there exist sets $A_1, \ldots, A_{k-1}$ such that $W = A_1 \cup A_2 \cup \ldots \cup A_{k-1}$, where each A_i is a $B_2[g]$ set for some fixed g. We consider each d-tuple $(i_1, \ldots, i_d)$ in S. This corresponds to k elements of W, namely $(x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_1, \ldots, (x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_k$. By the pigeonhole principle, some pair of these must belong to the same set A_ℓ. This means we have a distinct way of achieving a sum of the form $(x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_i + (x^1_{i_1}, \ldots, x^d_{i_d}) \cdot v_j$ in $A_\ell + A_\ell$ (this is a distinct way of achieving this sum because elements of W

have unique representations as $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_i$ by Lemma 6). We note that:

$$(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_i + (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_j = (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i + v_j),$$

and that $(v_i + v_j)$ is 0 in $> \frac{d}{2}$ of the coordinates.

We consider tuples $(i_1, \ldots, i_d) \in S$ such that all of $i_1, \ldots, i_d$ are $\leq n$, for some fixed positive integer n. We first count how many of these tuples there are. We note that $(i_1, \ldots, i_d) = M \cdot (i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil})$ for some $(i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil}) \in \mathbb{N}^{\lceil \frac{d}{2} \rceil}$. Thus, each of $i_1, \ldots, i_d$ is a linear combination of the values $i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil}$, with positive coefficients all $\leq 2d$. Thus, if we choose any $i'_1, \ldots, i'_{\lceil \frac{d}{2} \rceil}$ values such that each is $\leq \frac{n}{2d\lceil \frac{d}{2} \rceil}$, we will have $i_1, \ldots, i_d \leq n$. This shows that there are at least $\left(\frac{n}{2d\lceil \frac{d}{2} \rceil}\right)^{\lceil \frac{d}{2} \rceil}$ tuples $(i_1, \ldots, i_d) \in S$ such that all of $i_1, \ldots, i_d$ are $\leq n$.

As discussed above, each of these d-tuples in S contributes a unique way of forming a sum $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i + v_j)$ in $A_\ell + A_\ell$ for some A_ℓ. When all of $i_1, \ldots, i_d$ are $\leq n$, there are at most $\binom{k}{2} n^{\lceil \frac{d}{2} \rceil - 1}$ possibilities for the value of $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i + v_j)$. We can see this by noting that there are $\binom{k}{2}$ possibilities for $v_i + v_j$, and each of them only has at most $\lceil \frac{d}{2} \rceil - 1$ non-zero coordinates. In each such coordinate, we know our index value is at most n.

We note that d is a fixed function of k, and we consider letting n grow to infinity. Since $\left(\frac{n}{2d\lceil \frac{d}{2} \rceil}\right)^{\lceil \frac{d}{2} \rceil}$ grows faster as a function of n than $\binom{k}{2} n^{\lceil \frac{d}{2} \rceil - 1}$, and there are only k possibilities for A_ℓ, we must have that for any fixed g, there is some A_ℓ such that some element of $A_\ell + A_\ell$ can be expressed in $> g$ ways as a sum of two elements of A_ℓ. This contradicts that A_ℓ is a $B_2[g]$ set.

Hence we have proven that W is not a union of $k-1$ $B_2[g]$ sets for any finite g. $\square$

We have now shown:

Theorem 12. $W \subseteq \mathbb{Z}$ is a union of k $B_2[1]$ sets that cannot be decomposed as a union of $k-1$ $B_2[g]$ sets for any g. W is also a $B_2^\circ[2]$ set.

By employing the same counting argument as above for a fixed n (sufficiently large with respect to k and g), we can restate our result in the context of finite sets. We let $W_{n,k}$ denote the finite subset of W formed by restricting to tuples $(i_1, \ldots, i_d) \in S$ such that $i_1, \ldots, i_d \leq n$. (Here we make the dependence on k explicit.)

Theorem 13. For any positive integers g and k, we can choose n sufficiently large so that the finite set $W_{n,k} \subseteq \mathbb{Z}$ is a $B_2^\circ[2]$ set that is a union of k $B_2[1]$ sets, but cannot be decomposed as a union of $k-1$ $B_2[g]$ sets.

2.4 Adapting Our Construction for Mixed Unions

In the previous section, we constructed a set $W \subset Z$ for each k such that W could not be decomposed as a union of $k-1$ $B_2[g]$ sets for any g. However, our W is a $B_2^\circ[2]$ set, and we would like to arrive at a set in $\mathbb{Z}$ which cannot be decomposed as a mixed union of k $B_2[g]$ and $B_2^\circ[g]$ sets for each k. Constructing such a set will put us well on our way toward obtaining an explicit counterexample to the weak anti-Freiman conjecture. To accomplish this, we will first adjust our techniques to obtain a $B_2[2]$ set $W^\circ \subseteq \mathbb{Z}$ for each

k that cannot be decomposed as a union of $k-1$ $B_2^\circ[g]$ sets for any g. We will then consider $W^\circ \times W$ in $\mathbb{Z}^2$ for each k, and show that this cannot be decomposed as a mixed union of $\frac{k}{3}-1$ $B_2[g]$ and $B_2^\circ[g]$ sets for any g.

For each positive integer k, we set $d = k$ and we let v_j be the vector in $\{1,-1\}^d$ with a -1 in the j^{th} coordinate and 1's in all other coordinates. We note that for $k \geq 5$, v_j and v_h will agree in $> \frac{d}{2}$ coordinates for all $1 \leq j,h \leq k$. We define the sequences $X_1,\ldots,X_d$ and the set $S \subset \mathbb{Z}^d$ as in the previous section. For each i from 1 to k, we define:

$$W_j^\circ := \{(x_{i_1}^1,\ldots,x_{i_d}^d)\cdot v_j : (i_1,\ldots,i_d) \in S\}.$$

We define $W^\circ := W_1^\circ \cup W_2^\circ \ldots \cup W_k^\circ$. We now prove the relevant properties of W°. The dependence of W° on k is implicit.

Lemma 14. Each element of W° has a unique expression as $(x_{i_1}^1,\ldots,x_{i_d}^d)\cdot v_j$ for $(i_1,\ldots,i_d) \in S$ and $1 \leq j \leq k$. In particular, the sets W_j° are disjoint.

Proof. This is the same as the proof of Lemma 6. □

Lemma 15. For each j, W_j° is a $B_2^\circ[1]$ set.

Proof. We can represent any element of W_j° as $\phi(M\cdot y)\cdot v_j$ for some vector $y \in Z^{\lceil \frac{d}{2} \rceil}$. We suppose that there are vectors y,z,y',z' such that:

$$\phi(M\cdot y)\cdot v_j - \phi(M\cdot z)\cdot v_j = \phi(M\cdot y')\cdot v_j - \phi(M\cdot z')\cdot v_j.$$

We now apply Lemma 8 with $v_i' = v_j$ and $v_j' = -v_j$. Since $v_j - v_j$ is 0 in all of the coordinates, we conclude that either $y = y'$ and $z = z'$ (so we do not

get a new way of representing the value as a difference) or $y = z$ and $y' = z'$ (in which case, we are representing 0). Therefore, every nonzero value can be represented in at most one way as a difference of two elements of W_j°. $\square$

Lemma 16. For $k \geq 5$, W° is a $B_2[2]$ set.

Proof. We note that the sums $v_i + v_j$ are distinct (e.g. i and j can be determined from the sum as the two coordinates where the sum is 0 for $i \neq j$). As shown in Lemma 7, this implies that the sets $W_i^\circ + W_j^\circ$ are disjoint. Therefore, it suffices to consider vectors $y, z, y', z' \in \mathbb{Z}^{\lceil \frac{d}{2} \rceil}$ such that:

$$\phi(M \cdot y) \cdot v_i + \phi(M \cdot z) \cdot v_j = \phi(M \cdot y') \cdot v_i + \phi(M \cdot z') \cdot v_j.$$

Now we can apply Lemma 8 with $v_i' = v_i$ and $v_j' = v_j$. Since $k \geq 5$, $v_i + v_j$ will be nonzero in more than half the coordinates, so either $y = y'$ and $z = z'$ or $y = z'$ and $z = y'$. This gives us at most 2 ways of representing any value as a sum of two elements of W°, so W° is a $B_2[2]$ set. $\square$

Lemma 17. For $k \geq 5$, W° cannot be decomposed as a union of $k - 1$ $B_2^\circ[g]$ sets for any g.

Proof. We suppose that this is not true, i.e. there exist sets $A_1^\circ, \ldots, A_{k-1}^\circ$ such that $W^\circ = A_1^\circ \cup A_2^\circ \cup \ldots \cup A_{k-1}^\circ$, where each A_i° is a $B_2^\circ[g]$ set for some fixed g. We consider each d-tuple $(i_1, \ldots, i_d)$ in S. This corresponds to k elements of W°, namely $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_1, \ldots, (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_k$. By the pigeonhole principle, some pair of these must belong to the same set A_ℓ°. This means we have a

distinct way of achieving a difference of the form $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_i - (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_j$ in $A_\ell^\circ - A_\ell^\circ$ (this is a distinct way of achieving this difference because elements of W° have unique representations as $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_i$ by Lemma 14). We note that:

$$(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_i - (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot v_j = (x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i - v_j),$$

and that $v_i - v_j$ is 0 in all but 2 of the coordinates.

We consider tuples $(i_1, \ldots, i_d) \in S$ such that each of $i_1, \ldots, i_d \leq n$, for some fixed positive integer n. From the proof of Lemma 11, we know there are at least $\left(\frac{n}{2d\lceil \frac{d}{2} \rceil}\right)^{\lceil \frac{d}{2} \rceil}$ of these tuples.

As discussed above, each of these d-tuples in S contributes a unique way of forming a difference $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i - v_j)$ in $A_\ell^\circ - A_\ell^\circ$ for some A_ℓ°. When all of $i_1, \ldots, i_d$ are $\leq n$, there are at most $\binom{k}{2} n^2$ possibilities for the value of $(x_{i_1}^1, \ldots, x_{i_d}^d) \cdot (v_i - v_j)$. We can see this by noting that there are $\binom{k}{2}$ possibilities for $v_i - v_j$, and each of them only has 2 nonzero coordinates. In each such coordinate, we know our index value is at most n.

We note that d is a fixed function of k, and we consider letting n grow to infinity. Since $\left(\frac{n}{2d\lceil \frac{d}{2} \rceil}\right)^{\lceil \frac{d}{2} \rceil}$ grows faster as a function of n than $\binom{k}{2} n^2$, and there are only k possibilities for A_ℓ°, we must have that for any fixed g, there is some A_ℓ° such that some element of $A_\ell^\circ + A_\ell^\circ$ can be expressed in $> g$ ways as a difference of two elements of A_ℓ°. This contradicts that A_ℓ° is a $B_2^\circ[g]$ set. Hence we have proven that W° is not a union of $k-1$ $B_2^\circ[g]$ sets for any finite g. $\square$

By employing the same counting argument as above with a fixed n (sufficiently large with respect to k and g), we can state our result in the context of finite sets:

Theorem 18. For any positive integers g and $k \geq 5$, there exists a finite $B_2[2]$ set $W_{n,k}^{\circ} \subseteq \mathbb{Z}$ such that $W_{n,k}^{\circ}$ is a union of k $B_2^{\circ}[1]$ sets but cannot be decomposed as a union of $k-1$ $B_2^{\circ}[g]$ sets.

Here, $W_{n,k}^{\circ}$ is the finite subset of W° formed by restricting to tuples $(i_1, \ldots, i_d) \in S$ such that $i_1, \ldots, i_d \leq n$.

We now fix k and g and consider the set $W_{n,k}^{\circ} \times W_{n,k} \subseteq \mathbb{Z}^2$, where n is chosen to be sufficiently large with respect to k and g, and $W_{n,k}$ is defined as in Theorem 13.

Theorem 19. For each fixed g and $k \geq 5$, there exists a sufficiently large n such that $W_{n,k}^{\circ} \times W_{n,k} \subseteq \mathbb{Z}^2$ cannot be expressed as a union of $\leq \frac{k}{3} - 1$ $B_2^{\circ}[g]$ and $B_2[g]$ sets.

Proof. We let $k' := \frac{k}{3} - 1$. We suppose that

$$W_{n,k}^{\circ} \times W_{n,k} = \left(\bigcup_{i=1}^{j} A_i \right) \bigcup \left(\bigcup_{i=j+1}^{k'} A_i^{\circ} \right),$$

where each A_i is a $B_2[g]$ set and each A_i° is a $B_2^{\circ}[g]$ set. We note that at least half of the elements of $W_{n,k}^{\circ} \times W_{n,k}$ must be contained in either the union of the A_i's or the union of the A_i°'s. We suppose that $\geq \frac{1}{2}$ the elements are contained in the A_i's. This implies that there must exist some $a \in W_{n,k}^{\circ}$ such that at

least half of the elements $a \times b$ for $b \in W_{n,k}$ are contained in the union of the A_i's.

We let S_n denote the set of d-tuples $(i_1, \ldots, i_d) \in S$ such that $i_1, \ldots, i_d \leq n$. We define $N := |S_n|$, and we number these tuples from 1 to N. For each j from 1 to N, we let I_j denote the set of k elements of $W_{n,k}$ corresponding to the tuple j. We suppose that for $(1-\alpha)N$ of these sets I_j, we have less than $\frac{k}{3}$ elements of $a \times I_j$ in the union of the A_i's. Then α must satisfy:

$$(1-\alpha)N\left(\frac{k}{3}\right)+\alpha Nk \geq \frac{1}{2}Nk \Leftrightarrow (1-\alpha)\left(\frac{1}{3}\right)+\alpha \geq \frac{1}{2} \Leftrightarrow \frac{1}{3}-\frac{\alpha}{3}+\alpha \geq \frac{1}{2} \Leftrightarrow \alpha \geq \frac{1}{4}.$$

This means that for at least $\frac{1}{4}N$ values of j, we have at least $\frac{k}{3}$ elements of $a \times I_j$ in the union of the A_i's. Now, there are at most $k' < \frac{k}{3}$ of the A_i's, so for these tuples j, we must have that two distinct elements of $a \times I_j$ will be in the same A_i. Each of these will correspond to a distinct representation of one of $\binom{k}{2}n^{\lceil \frac{d}{2} \rceil - 1}$ possible sum values in $\mathbb{Z}^2$ (note that all of these will be equal to $2a$ in the first coordinate). Since this will occur at least

$$\frac{1}{4}N \geq \frac{1}{4}\left(\frac{n}{2d\lceil \frac{d}{2} \rceil}\right)^{\lceil \frac{d}{2} \rceil}$$

times, and there are only k' A_i's, we can choose n large enough to contradict that each A_i is a $B_2[g]$ set (note that k, d, g are all fixed).

Similarly, if at least half of the elements of $W^{\circ}_{n,k} \times W_{n,k}$ are contained in the union of the A°_i's, then there must be some fixed $b \in W_{n,k}$ such that at least half of the elements of $W^{\circ}_{n,k} \times b$ are contained in the A°_i's. Then for at least $\frac{1}{4}$ of the N d-tuples in S_n, we will get a distinct representation of one of

$\binom{k}{2}n^2$ values as a difference of two elements of some A_i°. We can then choose n large enough to contradict that each A_i° is a $B_2^\circ[g]$ set. $\square$

2.5 A Counterexample to the Weak Anti-Freiman Conjecture

We now use our sets $W_{n,k}^\circ \times W_{n,k}$ to disprove the weak anti-Freiman conjecture (Conjecture 1). We first prove a lemma about $\Lambda(4)$ sets. This is essentially Lemma 4.30 from [66].

Lemma 20. Let $S \subset \mathbb{Z}^d$ such that $K_4(S) < \infty$. (Recall the definition of $K_4(S)$ from equation (2.2) in subsection 2.1.3.) Furthermore if $(h_1, h_2) \in \{(2,0),(1,1)\}$, then for any finite $S' \subseteq S$,

$$|h_1 S' - h_2 S'| \geq \frac{|S'|^2}{(K_4(S))^4}.$$

Proof. First, from the definition of $K_4(S)$ we have

$$\left|\left|\sum_{\xi \in S'} e(\xi \cdot x)\right|\right|_{L^4}^4 \leq (K_4(S))^4 |S'|^2. \tag{2.5}$$

Now we also have that

$$\left|\left|\sum_{\xi \in S'} e(\xi \cdot x)\right|\right|_{L^4}^4 = \left|\left|\left(\sum_{\xi \in S'} e(\xi \cdot x)\right)^{h_1} \left(\sum_{\xi \in S'} e(-\xi \cdot x)\right)^{h_2}\right|\right|_{L^2}^2.$$

We let

$$R_{2,0}(\nu) = |\,((\xi_1, \xi_2) \in S' \times S') : \xi_1 + \xi_2 = \nu)\,|$$

and we also let

$$R_{1,1}(\nu) = |\,((\xi_1, \xi_2) \in S' \times S') : \xi_1 - \xi_2 = \nu)\,|.$$

We then have:

$$\sum_{\nu \in \mathbb{Z}^d} R^2_{h_1,h_2}(\nu) \leq (K_4(S))^4 \, |S'|^2.$$

We also note that:

$$\sum_{\nu \in \mathbb{Z}^d} R_{h_1,h_2}(\nu) = |S'|^2. \tag{2.6}$$

Finally, by Cauchy-Schwarz, (2.5), and the fact that $R_{h_1,h_2}(\nu)$ is supported on the set $h_1 S' - h_2 S'$, we have

$$\begin{aligned} \sum_{\nu \in \mathbb{Z}^d} 1_{\{h_1 S' - h_2 S'\}}(\nu) R_{h_1,h_2}(\nu) &\leq ||1_{\{h_1 S' - h_2 S'\}}||_{L^2(\mathbb{Z}^d)} \, ||R_{h_1,h_2}||_{L^2(\mathbb{Z}^d)} \\ &\leq |h_1 S' - h_2 S'|^{1/2} \, (K_4(S))^2 \, |S'|. \end{aligned} \tag{2.7}$$

From (2.6) and (2.7), we have that

$$|S'|^2 \leq |h_1 S' - h_2 S'|^{1/2} \, (K_4(S))^2 \, |S'|,$$

which completes the proof.

□

Lemma 21. There is a universal constant $\delta > 0$ such that for any $k \geq 5$, for any finite subset W' of $W^\circ \times W$ (recall that $W^\circ \times W$ is defined with respect to k), $|W' + W'| \geq \delta |W'|^2$ and $|W' - W'| \geq \delta |W'|^2$.

Proof. We fix a value of $k \geq 5$. We note that W° is a $B_2[2]$ set, and hence it is a $\Lambda(4)$ set, with its $\Lambda(4)$ constant bounded independently of k. Similarly, W is $B_2^\circ[2]$, so it is also a $\Lambda(4)$ set, with its $\Lambda(4)$ constant bounded independently of k. Thus, by Lemma 25, we conclude that $W^\circ \times W$ is also a $\Lambda(4)$ set, with its

$\Lambda(4)$ constant bounded independently of k. By the lemma above, there exists $\delta > 0$ independent of k such that $|W' + W'| \geq \delta |W'|^2$ and $|W' - W'| \geq \delta |W'|^2$ for any finite subset W' of $W^\circ \times W$. (We note that this can be proved directly from the combinatorial properties of our construction, but we prefer this proof because it highlights the connection between the anti-Freiman problem and $\Lambda(4)$ sets.) $\square$

Theorem 22. We let δ be as above, so for every n and $k \geq 5$, we have that $|W' + W'| \geq \delta |W'|^2$ and $|W' - W'| \geq \delta |W'|^2$ for all finite subsets W' of $W^\circ_{n,k} \times W_{n,k}$. For every g and δ', there exist k and n sufficiently large such that $W^\circ_{n,k} \times W_{n,k}$ does not contain either a $B_2[g]$ set or a $B_2^\circ[g]$ set of size $\geq \delta' |W^\circ_{n,k} \times W_{n,k}|$.

Proof. We again let N denote the size of S_n, so $|W_{n,k}| = |W^\circ_{n,k}| = kN$. We suppose we have $A \subseteq W^\circ_{n,k} \times W_{n,k}$ such that $|A| \geq \delta' |W^\circ_{n,k} \times W_{n,k}| = \delta' k^2 N^2$. We again number the tuples of S_n as 1 to N. We let I_j denote the set of k elements of $W_{n,k}$ corresponding to tuple j and we let I_j° denote the set of k elements of $W^\circ_{n,k}$ corresponding to tuple j. We note that for some fixed $a \in W^\circ_{n,k}$, A must contain at least $\delta' kN$ elements of $a \times W_{n,k}$. We consider the sets $a \times I_j$. We suppose that $1 - \gamma$ of them have $< \frac{\delta'}{2} k$ elements in A. Then γ must satisfy:

$$(1 - \gamma)\frac{\delta'}{2} + \gamma \geq \delta' \Leftrightarrow \gamma \geq \frac{\frac{\delta'}{2}}{1 - \frac{\delta'}{2}}.$$

We can then set $\gamma = \frac{\frac{\delta'}{2}}{1 - \frac{\delta'}{2}}$, and we have that at least a γ-fraction of the I_j's have at least $\frac{\delta'}{2} k$ elements of $a \times I_j$ in A. As long as we choose k so that

$\delta' \frac{k}{2} \geq 2$, these will lead to repeated sums in A. More precisely, each pair of distinct elements in $a \times I_j$ will sum to one of $\binom{k}{2} n^{\lceil \frac{d}{2} \rceil - 1}$ values, and there are at least $\binom{\delta' \frac{k}{2}}{2} \gamma N$ such pairs in A. Since N is a faster growing function of n than $n^{\lceil \frac{d}{2} \rceil - 1}$, we can choose n sufficiently large to contradict that A is a $B_2[g]$ set.

Similarly, there is some fixed $b \in W_{n,k}$ such that at least $\delta' k N$ elements of $W_{n,k}^{\circ} \times b$ are contained in A. We then have that at least a γ-fraction of the sets $I_j^{\circ} \times b$ have at least $\frac{\delta'}{2} k$ elements in A. This will lead to repeated differences in A: each pair of distinct elements in $I_j^{\circ} \times b$ will have a difference equal to one of $\binom{k}{2} n^2$ values, and there are at least $\binom{\delta' \frac{k}{2}}{2} \gamma N$ such pairs in A. Since N is a faster growing function of n than n^2, we can choose n sufficiently large to contradict that A is a $B_2^{\circ}[g]$ set. Thus, if we choose k so that $\delta' \frac{k}{2} \geq 2$ and n sufficiently large with respect to k, g, d, δ', we have that A cannot be a $B_2[g]$ set or a $B_2^{\circ}[g]$ set. $\square$

This is a counterexample to Conjecture 1 in $\mathbb{Z}^2$. To obtain a counterexample in $\mathbb{Z}$, we can use F_2-isomorphisms, which are discussed in the next section. We note that each $W_{n,k}^{\circ} \times W_{n,k}$ is a finite set, and thus there is a F_2-isomorphic copy of this set inside $\mathbb{Z}$ by Lemma 27 (which we prove in the next section). If this image in $\mathbb{Z}$ contained a large $B_2[g]$ or $B_2^{\circ}[g]$ set, then this would correspond to a $B_2[g]$ or $B_2^{\circ}[g]$ set in $W_{n,k}^{\circ} \times W_{n,k}$, which we know does not exist. (If two finite sets are F_2-isomorphic, then one is a $B_2[g]$ or $B_2^{\circ}[g]$ set if and only if the other one is as well, by Lemma 29, which is also proved in the next section.)

2.6 $\Lambda(4)$ Sets

We provide an alternate counterexample to Rudin's question for $\Lambda(4)$ sets: we give an explicit set in $\mathbb{Z}$ that is a $\Lambda(4)$ set, but cannot be expressed as finite union of $B_2[g]$ sets for any g. However, one might also ask about $B_2^\circ[g]$ sets, since all $B_2^\circ[g]$ sets are $\Lambda(4)$ sets as well:

Lemma 23. Let $S \subset \mathbb{Z}^d$ be a $B_2^\circ[g]$ set. Then for any function $f \in L^2(\mathbb{T}^d)$ such that $\hat{f}$ is supported on S, we have:

$$\left|\left|\sum_{\xi\in S} \hat{f}(\xi)e(\xi\cdot x)\right|\right|_{L^4} \leq (1+g^2)^{1/4}||f||_{L^2}.$$

Proof. We note:

$$\left|\left|\sum_{\xi\in S} \hat{f}(\xi)e(\xi\cdot x)\right|\right|_{L^4}^4 = \left|\left|\sum_{\xi_1\in S} \hat{f}(\xi_1)e(\xi_1\cdot x)\sum_{\xi_2\in S}\overline{\hat{f}(\xi_2)}e(-\xi_2\cdot x)\right|\right|_{L^2}^2$$

$$= \sum_{\nu\in\mathbb{Z}^d}\left|\sum_{\xi_1-\xi_2=\nu}\hat{f}(\xi_1)\overline{\hat{f}(\xi_2)}\right|^2 = \left(\sum_{\xi\in S}|\hat{f}(\xi)|^2\right)^2 + \sum_{\nu\neq 0}\left|\sum_{\xi_1-\xi_2=\nu}\hat{f}(\xi_1)\overline{\hat{f}(\xi_2)}\right|^2$$

$$\leq \left(\sum_{\xi\in S}|\hat{f}(\xi)|^2\right)^2 + g^2\sum_{\nu\neq 0}\max_{\substack{|\hat{f}(\xi_1)\hat{f}(\xi_2)|^2\\ \xi_1-\xi_2=\nu}}|\hat{f}(\xi_1)\hat{f}(\xi_2)|^2$$

$$\leq \left(\sum_{\xi\in S}|\hat{f}(\xi)|^2\right)^2 + g^2\left(\sum_{\xi\in S}|\hat{f}(\xi)|^2\right)^2 = \left(1+g^2\right)\left(\sum_{\xi\in S}|\hat{f}(\xi)|^2\right)^2.$$

□

This shows that every $B_2^\circ[g]$ set is also a $\Lambda(4)$ set, so any finite union of $B_2[g]$ sets and $B_2^\circ[g]$ sets is also a $\Lambda(4)$ set. This raises a variant of Rudin's

question: is every $\Lambda(4)$ set a finite union of $B_2[g]$ and $B_2^\circ[g]$ sets? The answer to this question is also no, and we give a $\Lambda(4)$ set in $\mathbb{Z}$ which cannot be decomposed as a finite mixed union of $B_2[g]$ and $B_2^\circ[g]$ sets. In this section, we describe how to obtain this from our combinatorial construction above and we prove the following stronger result:

Theorem 3. There exists a $\Lambda(4)$ set S such that for any fixed choice of $\delta > 0$ and g, there exists a finite subset A of S such that no subset A' of A satisfying $|A'| \geq \delta |A|$ is a $B_2[g]$ or $B_2^\circ[g]$ set.

We will need the following integral form of Minkowski's inequality (see [24], Theorem 202).

Lemma 24. Let $f(x,y) \in L^p(\mathbb{T}^{d_1} \times \mathbb{T}^{d_2})$ be a complex-valued function. For $p > 1$, we have that

$$\left(\int_{\mathbb{T}^{d_1}} \left| \int_{\mathbb{T}^{d_2}} f(x,y) dy \right|^p dx \right)^{1/p} \leq \int_{\mathbb{T}^{d_2}} \left(\int_{\mathbb{T}^{d_1}} |f(x,y)|^p dx \right)^{1/p} dy.$$

Lemma 25. Let S_1 and S_2 be $\Lambda(p)$ sets in $\mathbb{Z}^{d_1}$ and $\mathbb{Z}^{d_2}$ respectively ($p > 2$). The direct product $S = S_1 \times S_2 \subseteq \mathbb{Z}^{d_1+d_2}$ is a $\Lambda(p)$ subset of $\mathbb{Z}^{d_1+d_2}$ with $\Lambda(p)$ constant equal to $K_p^{d_1+d_2}(S) = K_p^{d_1}(S_1) K_p^{d_2}(S_2)$.

Proof. We let $f(x,y) \in L^2(\mathbb{T}^{d_1+d_2})$, with $\hat{f}$ supported on $S_1 \times S_2 \subseteq \mathbb{Z}^{d_1+d_2}$. First we notice that if we fix $x_0 \in \mathbb{T}^{d_1}$, then the Fourier transform of the function $f(x_0, y)$ is supported on S_2. Similarly, if we fix $y_0 \in \mathbb{T}^{d_2}$, then $f(x, y_0)$ is a function with Fourier transform supported on S_1. We have:

$$\left(\int_{\mathbb{T}^{d_1+d_2}} |f(x,y)|^p dydx\right)^{1/p} = \left(\int_{\mathbb{T}^{d_1}}\int_{\mathbb{T}^{d_2}} |f(x,y)|^p dydx\right)^{1/p}$$

$$\leq K_p^{d_2}(S_2)\left(\int_{\mathbb{T}^{d_1}}\left(\int_{\mathbb{T}^{d_2}} |f(x,y)|^2 dy\right)^{p/2} dx\right)^{1/p}$$

$$\leq K_p^{d_2}(S_2)\left(\int_{\mathbb{T}^{d_2}}\left(\int_{\mathbb{T}^{d_1}} |f(x,y)|^p dx\right)^{2/p} dy\right)^{1/2}$$

$$\leq K_p^{d_1}(S_1)K_p^{d_2}(S_2)\left(\int_{\mathbb{T}^{d_2}}\int_{\mathbb{T}^{d_1}} |f(x,y)|^2 dxdy\right)^{1/2}.$$

This establishes that $K_p^{d_1+d_2}(S) \leq K_p^{d_1}(S_1)K_p^{d_2}(S_2)$. To see that $K_p^{d_1+d_2}(S)$ $\geq K_p^{d_1}(S_1)K_p^{d_2}(S_2)$, we can consider a sequence of functions $\{g_n\}$ with Fourier coefficients supported on S_1 with $\frac{||g_n||_{L^p}}{||g_n||_{L^2}}$ approaching $K_p^{d_1}(S_1)$ and a sequence of functions $\{h_n\}$ with Fourier coefficients supported on S_2 with $\frac{||h_n||_{L^p}}{||h_n||_{L^2}}$ approaching $K_p^{d_2}(S_2)$. If we then consider the functions $f_n(x,y) := g_n(x)h_n(y)$, we see that $K_p^{d_1+d_2}(S) \geq K_p^{d_1}(S_1)K_p^{d_2}(S_2)$. □

Let G_1 and G_2 be abelian groups, and S a finite subset of G_1. We say a map $\tau : S \to G_2$ is a F_2-isomorphism if τ is injective and

$$\tau(a) + \tau(b) = \tau(c) + \tau(d) \Leftrightarrow a + b = c + d$$

$$\tau(a) - \tau(b) = \tau(c) - \tau(d) \Leftrightarrow a - b = c - d$$

for $a, b, c, d \in S$. We say that S and $\tau(S)$ are F_2-isomorphic. We note that τ^{-1} is a F_2-isomorphism from $\tau(S)$ to S. However, τ is not an isomorphism in

the full sense of group theory, since S and $\tau(S)$ may not be groups. We will need the following lemmas concerning F_2-isomorphisms.

Lemma 26. If S is a finite subset of $\mathbb{Z}^d$, then translation of S by $\alpha \in \mathbb{Z}^d$ is a F_2-isomorphism.

Proof. We define $\tau(a) := a + \alpha$ for all $a \in S$. Then, for any $a, b, c, d \in S$, we have:

$$\tau(a) + \tau(b) = \tau(c) + \tau(d) \Leftrightarrow a + b + 2\alpha = c + d + 2\alpha \Leftrightarrow a + b = c + d,$$

$$\tau(a) - \tau(b) = \tau(c) - \tau(d) \Leftrightarrow a - b + \alpha - \alpha = c - d + \alpha - \alpha \Leftrightarrow a - b = c - d.$$

Hence, translation by a constant α is a F_2-isomorphism. □

Lemma 27. Let $S \subset \mathbb{Z}^d$ be a finite set. Then there exists a F_2-isomorphism of S into $\mathbb{Z}$.

Proof. We let

$$M = 5 \max_{\vec{s} \in S} \left\{ \max_{1 \le i \le d} |\vec{s}_i| \right\}.$$

We then define our F_2-isomorphism τ by:

$$\tau(\vec{s}) = \sum_{i=1}^{d} \vec{s}_i M^i.$$

For any $\vec{s}, \vec{t} \in S$, we have:

$$\tau(\vec{s}) + \tau\left(\vec{t}\right) = \sum_{i=1}^{d} \vec{s}_i M^i + \sum_{i=1}^{d} \vec{t}_i M^i = \sum_{i=1}^{d} \left(\vec{s}_i + \vec{t}_i\right) M^i.$$

Now, the range of possible values taken by $\vec{s}_i + \vec{t}_i$ falls within

$[-2\max_{1\leq i\leq d}|\vec{s}_i|, 2\max_{1\leq i\leq d}|\vec{s}_i|]$. By definition of M, this range is contained in $(-\frac{M}{2}, \frac{M}{2})$, so base M expansions of integers with coefficients in this range are unique.

Hence, for other vectors $\vec{u}, \vec{v} \in S$, we will have $\tau(\vec{u})+\tau(\vec{v}) = \tau(\vec{s})+\tau\left(\vec{t}\right)$ if and only if $\vec{u}+\vec{v} = \vec{s}+\vec{t}$ in $\mathbb{Z}^d$. Similarly,

$$\tau(\vec{s}) - \tau\left(\vec{t}\right) = \sum_{i=1}^{d} \left(\vec{s}_i - \vec{t}_i\right) M^i,$$

and $\tau(\vec{u}) - \tau(\vec{v}) = \tau(\vec{s}) - \tau\left(\vec{t}\right)$ if and only if $\vec{u}-\vec{v} = \vec{s}-\vec{t}$.

□

Lemma 28. If $U \subset \mathbb{Z}^{d_1}$ and $V \subset \mathbb{Z}^{d_2}$ are F_2-isomorphic, then $K_4^{d_1}(U) = K_4^{d_2}(V)$.

Proof. We consider $f \in L^2(\mathbb{T}^{d_1})$ such that $\hat{f}$ is supported on U. As in equation (3) above, we have:

$$||f||_{L^4}^2 = \left(\sum_{\xi\in\mathbb{Z}^{d_1}} \left| \sum_{\substack{\nu_1+\nu_2=\xi \\ \nu_1,\nu_2\in U}} \hat{f}(\nu_1)\hat{f}(\nu_2) \right|^2 \right)^{\frac{1}{2}}.$$

We define $g \in L^2(\mathbb{T}^{d_2})$, a function such that $\hat{g}$ is supported on V, by $\hat{g}(\xi) = \hat{f}(\tau(\xi))$, where τ is an F_2-isomorphism from V to U (we let $\hat{g}(\xi)$ be 0 for $\xi \notin V$). Now we have:

$$||g||_{L^4}^2 = \left(\sum_{\xi\in\mathbb{Z}^{d_2}} \left| \sum_{\substack{\mu_1+\mu_2=\xi \\ \mu_1,\mu_2\in V}} \hat{g}(\mu_1)\hat{g}(\mu_2) \right|^2 \right)^{\frac{1}{2}}$$

$$= \left(\sum_{\xi \in \mathbb{Z}^{d_2}} \left| \sum_{\substack{\mu_1+\mu_2=\xi \\ \mu_1,\mu_2 \in V}} \hat{f}(\tau(\mu_1))\hat{f}(\tau(\mu_2)) \right|^2 \right)^{\frac{1}{2}}.$$

We can let ν_1 denote $\tau(\mu_1)$ and ν_2 denote $\tau(\mu_2)$, and since τ is a bijection between V and U that preserves sum relations, this can be rewritten as:

$$\left(\sum_{\xi \in \mathbb{Z}^{d_1}} \left| \sum_{\substack{\nu_1+\nu_2=\xi \\ \nu_1,\nu_2 \in U}} \hat{f}(\nu_1)\hat{f}(\nu_2) \right|^2 \right)^{\frac{1}{2}} = ||f||_{L^4}^2.$$

Conversely, we could start with a function f such that $\hat{f}$ is supported on V and obtain g with $\hat{g}$ supported on U via $\hat{g}(\xi) = \hat{f}(\tau^{-1}(\xi))$. We would again obtain $||g||_{L^4}^2 = ||f||_{L^4}^2$. This shows that $K_4^{d_1}(U) = K_4^{d_2}(V)$.

□

Lemma 29. Let $U \subset \mathbb{Z}^{d_1}$ and $V \subset \mathbb{Z}^{d_2}$ be F_2-isomorphic (U and V are finite sets). For any fixed positive integer g, the following two statements are equivalent (a) k is the smallest integer such that U is the union of k $B_2[g]$ sets, and (b) k is the smallest integer such that V is the union of k $B_2[g]$ sets. The analogous statement holds for $B_2^\circ[g]$ sets.

Proof. We suppose that $\tau : U \to V$ is a F_2-isomorphism. We suppose that U can be expressed as the union of k $B_2[g]$ sets, say $A_1, \ldots, A_k$. We consider each $\tau(A_i)$ as a set in V. If this is not a $B_2[g]$ set, then we must have distinct pairs $\{a_1, b_1\}, \ldots, \{a_{g+1}, b_{g+1}\}$ in $\tau(A_i)$ such that:

$$a_1 + b_1 = a_2 + b_2 = \ldots = a_{g+1} + b_{g+1}.$$

By the properties of τ, we then have that

$$\tau^{-1}(a_1) + \tau^{-1}(b_1) = \ldots = \tau^{-1}(a_{g+1}) + \tau^{-1}(b_{g+1})$$

holds in A_i, and the pairs $\{\tau^{-1}(a_1), \tau^{-1}(b_1)\}, \ldots, \{\tau^{-1}(a_{g+1}), \tau^{-1}(b_{g+1})\}$ are distinct in A_i, since τ is a bijection. This contradicts that A_i is a $B_2[g]$ set. Hence, $\tau(A_i)$ must be a $B_2[g]$ set for each i, and V is the union of the these sets. Thus, V can also be expressed as the union of k $B_2[g]$ sets. By reversing the roles of U and V and considering τ^{-1} in place of τ, we also see that if V is a union of k $B_2[g]$ sets, then so is U. This proves the equivalence of the statements in the lemma. The same statement for unions of $B_2^\circ[g]$ holds by noting that τ also preserves difference relations. □

We will use the following inequality of Littlewood and Paley (see [64], for example):

Lemma 30. *(Littlewood-Paley)*Let $f \in L^p(\mathbb{T})$ such that $f(x) = \sum_{\xi \in \mathbb{N}} \hat{f}(\xi) e(\xi x)$. Define $S_n := [2^n, 2^{n+1})$ for $n \in \mathbb{N}$. There exists, for $1 < p < \infty$, a positive constant c_p such that

$$c_p^{-1} \left\| \left(\sum_{n=1}^{\infty} \left| \sum_{\xi \in S_n} \hat{f}(\xi) e(\xi x) \right|^2 \right)^{1/2} \right\|_{L^p(\mathbb{T})} \leq \left\| \sum_{\xi \in \mathbb{Z}} \hat{f}(\xi) e(\xi x) \right\|_{L^p(\mathbb{T})}$$

$$\leq c_p \left\| \left(\sum_{n=1}^{\infty} \left| \sum_{\xi \in S_n} \hat{f}(\xi) e(\xi x) \right|^2 \right)^{1/2} \right\|_{L^p(\mathbb{T})}.$$

From Theorem 19 above, we obtain finite sets $W_{n,k}^{\circ} \times W_{n,k}$ in $\mathbb{Z}^2$ for each $k \geq 5$ which cannot be decomposed as a mixed union of $\frac{k}{3} - 1$ $B_2[k]$ and $B_2^{\circ}[k]$ sets in $\mathbb{Z}^2$, where each $W_{n,k}^{\circ}$ is a $B_2[2]$ set in $\mathbb{Z}$ and each $W_{n,k}$ is a $B_2^{\circ}[2]$ set in $\mathbb{Z}$. We drop the parameter n from our notation in the lemma statement below, since n is a function of k, i.e. any n sufficiently large with respect to k will do.

Lemma 31. There exists a $\Lambda(4)$ subset of $\mathbb{Z}$ that cannot be decomposed as a finite (mixed) union of $B_2[g]$ and $B_2^{\circ}[g]$ sets.

Proof. Let us write $C_k' := W_k^{\circ} \times W_k \subset \mathbb{Z}^2$. Now W_k° is a $B_2[2]$ set and W_k is a $B_2^{\circ}[2]$ set. Thus, W_k° and W_k are $\Lambda(4)$ sets with $\Lambda(4)$ constant bounded by some universal constant D, independent of k. It then follows from Lemma 25 that $C_k' \subset \mathbb{Z}^2$ is a $\Lambda(4)$ set with $\Lambda(4)$ constant at most D^2.

By Lemma 27, we can find a finite subset of $\mathbb{Z}$ satisfying the same properties and having a $\Lambda(4)$ constant at most D^2. Let us denote this set as C_k. Since the translation of C_k by $\alpha \in \mathbb{Z}$ is a F_2-isomorphism, we may translate C_k without affecting its $\Lambda(4)$ constant and without destroying the combinatorial properties established above. We may thus assume that $C_k \subset [2^{\psi(k)}, 2^{\psi(k)+1})$ where $\psi(k) : \mathbb{N} \to \mathbb{N}$ is injective and C_k has $\Lambda(4)$ constant at most D^2.

We now appeal to the Littlewood-Paley inequality to show that $C = \cup_{k=5}^{\infty} C_k$ is a $\Lambda(4)$ set. Let $f(x) = \sum_{\xi \in C} \hat{f}(\xi) e(\xi x)$ such that $||f||_{L^2(\mathbb{T})} < \infty$. Then

$$||f||_{L^4(\mathbb{T})} \leq c_4 \left|\left| \left(\sum_{n=5}^{\infty} \left| \sum_{\xi \in C_n} \hat{f}(\xi) e(\xi x) \right|^2 \right)^{1/2} \right|\right|_{L^4(\mathbb{T})}$$

$$\leq c_4 \left(\sum_{n=5}^{\infty} \left|\left| \sum_{\xi \in C_n} \hat{f}(\xi) e(\xi x) \right|\right|_{L^4(\mathbb{T})}^2 \right)^{1/2}$$

$$\leq c_4 \left(\sum_{n=5}^{\infty} \left(D^2 \left|\left| \sum_{\xi \in C_n} \hat{f}(\xi) e(\xi x) \right|\right|_{L^2(\mathbb{T})} \right)^2 \right)^{1/2} \leq c_4 D^2 ||f||_{L^2(\mathbb{T})}.$$

Lastly, we note that C is not a finite union of $B_2[g]$ and $B_2^\circ[g]$ sets. To see this, notice that a partition of C as a union of j $B_2[j]$ sets and j $B_2^\circ[j]$ sets would imply a partition of C_k as a union of j $B_2[j]$ sets and j $B_2^\circ[j]$ sets, which, by construction is impossible for large enough k. $\square$

Theorem 3 easily follows. The fact that for every $\delta > 0$ and g there exists a finite subset A of our $\Lambda(4)$ set such that any subset $A' \subseteq A$ satisfying $|A'| \geq \delta |A|$ is not a $B_2[g]$ or $B_2^\circ[g]$ set follows from the fact that this holds (by Theorem 22 above) for the sets $C_k' := W_k^\circ \times W_k \subset \mathbb{Z}^2$ when k is sufficiently large, and that C contains a F_2-isomorphic copy of these sets.

Chapter 3

Endpoint Restriction Estimates for the Paraboloid over Finite Fields

3.1 Introduction

Let S denote a hypersurface in $\mathbb{R}^n$ with measure $d\sigma$. The restriction problem for S is to determine for which pairs of (p, q) does there exist an inequality of the form

$$||\hat{f}||_{L^{p'}(S,d\sigma)} \leq C||f||_{L^{q'}(\mathbb{R}^n)}. \tag{3.1}$$

We note that the left-hand side is not necessarily well-defined since we have restricted the function $\hat{f}$ to the hypersurface S, a set of measure zero in $\mathbb{R}^n$. However, if we can establish this inequality for all Schwartz functions f, then the operator that restricts $\hat{f}$ to S can be defined whenever $f \in L^q$. In the Euclidean setting, the restriction problem has been extensively studied for many surfaces. In particular, it has been observed that restriction estimates are intimately connected to questions about certain partial differential equations as well as problems in geometric measure theory such as the Kakeya conjecture. The restriction conjecture states sufficient conditions on (p, q) for the above inequality to hold. In the case of the sphere and paraboloid, the question is

open in dimensions three and higher. For a survey of restriction results in the Euclidean setting, see [65].

In [44], Mockenhaupt and Tao initiated the study of the restriction phenomena in the finite field setting. This is motivated by both the similarities and the differences between the Euclidean and finite field settings, which suggest that studying restriction phenomena in finite fields may yield insights which are portable to the Euclidean setting, but also that the problems in the finite field setting present unique and independently interesting challenges. In addition, these problems in the finite field setting are closely related to other areas of mathematics, and particularly seem amenable to the use of combinatorial techniques.

We now introduce some notation to formally define the problem. We let F denote a finite field of characteristic $p > 2$. We let S^1 denote the unit circle in $\mathbb{C}$ and define $e : F \to S^1$ to be a non-principal character of F. For example, when $F = \mathbb{Z}/p\mathbb{Z}$, we can set $e(x) := e^{2\pi ix/p}$. We will be considering the vector space F^n and its dual space F_*^n. Following the conventions of [44], we think of F^n as endowed with the counting measure dx which assigns mass 1 to each point and F_*^n as endowed with the normalized counting measure $d\xi$ which assigns mass $|F|^{-n}$ to each point (where $|F|$ denotes the size of F, so the total mass is equal to 1 here). To be clear in our calculations, we will always include the appropriate powers of $|F|$ explicitly.

For a complex-valued function f on F^n, we define its Fourier transform

$\hat{f}$ on F_*^n by:

$$\hat{f}(\xi) := \sum_{x \in F^n} f(x) e(-x \cdot \xi).$$

For a complex-valued function g on F_*^n, we define its inverse Fourier transform $g^\vee$ on F^n by:

$$g^\vee(x) := \frac{1}{|F|^n} \sum_{\xi \in F_*^n} g(\xi) e(x \cdot \xi).$$

It is easy to verify that $(\hat{f})^\vee = f$ and $\widehat{(g^\vee)} = g$.

We define the paraboloid $\mathcal{P} \subset F_*^n$ as: $\mathcal{P} := \{(\gamma, \gamma \cdot \gamma) : \gamma \in F_*^{n-1}\}$. This is endowed with the normalized "surface measure" $d\sigma$ which assigns mass $|\mathcal{P}|^{-1}$ to each point in $\mathcal{P}$. We note that $|\mathcal{P}| = |F|^{n-1}$. For a function $f : \mathcal{P} \to \mathbb{C}$, we define the function $(f d\sigma)^\vee : F^n \to \mathbb{C}$ as follows:

$$(f d\sigma)^\vee(x) := \frac{1}{|\mathcal{P}|} \sum_{\xi \in \mathcal{P}} f(\xi) e(x \cdot \xi).$$

For a complex-valued function f on F^n and $q \in [1, \infty)$, we define $||f||_{L^q(F^n, dx)} := \left(\sum_{x \in F^n} |f(x)|^q\right)^{\frac{1}{q}}$. For a complex-valued function f on $\mathcal{P}$, we similarly define $||f||_{L^q(\mathcal{P}, d\sigma)} := \left(\frac{1}{|\mathcal{P}|} \sum_{\xi \in \mathcal{P}} |f(\xi)|^q\right)^{\frac{1}{q}}$. (These are the standard definitions of the L^q norms, and hence they satisfy the usual properties of norms.)

Now we define a restriction inequality to be an inequality of the form

$$||\hat{f}||_{L^{p'}(S, d\sigma)} \leq \mathcal{R}(p \to q) ||f||_{L^{q'}(F^n)}, \tag{3.2}$$

where $\mathcal{R}(p \to q)$ denotes the best constant such that the above inequality holds. Here p' and q' denote the conjugate exponents of p and q respectively

(i.e. $\frac{1}{p} + \frac{1}{p'} = 1$). By duality, this is equivalent to the following extension estimate:

$$||(fd\sigma)^{\vee}||_{L^q(F^n,dx)} \leq \mathcal{R}(p \to q)||f||_{L^p(S,d\sigma)}. \tag{3.3}$$

We will only be considering the case of $S = \mathcal{P}$. We will use the notation $X \ll Y$ to denote that quantity X is at most a constant times quantity Y, where this constant may depend on the dimension n but not on the field size, $|F|$. For a finite field F, the constant $\mathcal{R}(p \to q)$ will always be finite. The restriction problem in this setting is to determine for which (p, q) can we upper bound $\mathcal{R}(p \to q)$ independently of $|F|$ (i.e. for which (p, q) does $\mathcal{R}(p \to q) \ll 1$ hold).

Mockenhaupt and Tao [44] solved this problem for the paraboloid in two dimensions. In three dimensions, we require -1 not be a square in F. For such F, they showed that $\mathcal{R}(8/5+\epsilon \to 4) \ll 1$ and $\mathcal{R}(2 \to \frac{18}{5}+\epsilon) \ll 1$ for every $\epsilon > 0$. When $\epsilon = 0$, their bounds were polylogarithmic in $|F|$. Mockenhaupt and Tao's argument for the $\mathcal{R}(8/5 \to 4)$ estimate proceeded by first establishing the estimate for characteristic functions. Here one can expand the L^4 norm and reduce the problem to combinatorial estimates. A well-known dyadic pigeonhole argument then allows one to pass back to general functions at the expense of a logarithmic power of $|F|$. The work of Iosevich and Koh in [30], [31], and [29] follows the same approach: first proving restriction estimates for characteristic functions in the finite field setting, and then incurring an extra

logarithmic power of $|F|$ in the general estimates obtained through the dyadic pigeonhole argument.

We introduce a method for obtaining general estimates which avoids the polylogarithmic cost of the dyadic pigeonhole technique. Our argument begins by rewriting the L^4 norm as $||(fd\sigma)^\vee||_{L^4} = ||(fd\sigma)^\vee(fd\sigma)^\vee||_{L^2}^{1/2}$. We then adapt the arguments of [44] and [30] to the bilinear variant $||(fd\sigma)^\vee(gd\sigma)^\vee||_{L^2}^{1/2}$ in the case that f and g are characteristic functions. The key point is that we allow f and g to be different characteristic functions - this is what makes our method more powerful than the standard dyadic pigeonhole technique.

To obtain estimates for arbitrary functions f, we can assume that f is non-negative real-valued and decompose f as a linear combination of characteristic functions, where the coefficients are negative powers of two (we can do this without loss of generality by adjusting only the constant of our bound). We can then employ the triangle inequality to upper bound $||(fd\sigma)^\vee||_{L^4}$ by a double sum of terms like $||(\chi_j d\sigma)^\vee(\chi_k d\sigma)^\vee||_{L^2}^{1/2}$, where χ_j and χ_k are characteristic functions, weighted by negative powers of two. We then apply our bilinear estimate for characteristic functions to these inner terms and use standard bounds on sums to obtain the final estimates.

Our method yields the following theorems:

Theorem 32. For the paraboloid in 3 dimensions with -1 not a square, we have $\mathcal{R}(8/5 \to 4) \ll 1$ and $\mathcal{R}(2 \to \frac{18}{5}) \ll 1$.

This improves upon Proposition 5.2 in [44] by removing the logarithmic

power of $|F|$. While our argument is elementary and does not use multilinear interpolation, the proof is certainly in the spirit of real interpolation. The second estimate, $\mathcal{R}(2 \to \frac{18}{5}) \ll 1$, follows from the first using the machinery of [44] without modification. After discovering our proof, we learned that in unpublished work Bennett, Carbery, Garrigos, and Wright [6] have independently obtained the end-point results in the 3-dimensional case. Their argument proceeds rather differently than ours and it is unclear if their argument can be extended to the higher dimensional settings. In higher dimensions, we prove:

Theorem 33. For the paraboloid in n dimensions when $n \geq 4$ is even or when n is odd and $|F| = q^m$ for a prime q congruent to 3 modulo 4 such that $m(n-1)$ is not a multiple of 4, we have $\mathcal{R}(\frac{4n}{3n-2} \to 4) \ll 1$ and $\mathcal{R}(2 \to \frac{2n^2}{n^2-2n+2}) \ll 1$.

This improves upon Theorems 1, 2, and 3 of [**?**] by removing the logarithmic power of $|F|$. We will only prove $\mathcal{R}(\frac{4n}{3n-2} \to 4) \ll 1$ here. The estimate $\mathcal{R}(2 \to \frac{2n^2}{n^2-2n+2}) \ll 1$ follows from the previous estimate from the arguments of [30].

We have restricted our attention to the case of the parabaloid, however our methods are more generic and likely can be combined with the arguments of [31] and [29] for the cases of spheres and more general quadratic surfaces, respectively.

3.2 A Restriction Theorem for the Paraboloid in F_*^3

We first prove Theorem 32 for the paraboloid in F_*^3, restated below in an equivalent formulation:

Theorem 32. For every function $f : \mathcal{P} \to \mathbb{C}$, we have that:

$$||(fd\sigma)^\vee||_{L^4(F^3,dx)} \leq C||f||_{L^{8/5}(\mathcal{P},d\sigma)}$$

for some constant C.

More concretely, we show below that
$C = 4\left(\frac{1}{\left(1-2^{-1/5}\right)\left(1-2^{-2/5}\right)} + \frac{1}{1-2^{-3/5}}\right)^{1/2} \leq 6$ suffices.

We start by following the strategy of [44], generalizing to the bilinear setting. We employ the following two lemmas. The first one is standard.

Lemma 34. Let P be a collection of points in F^2, and let L be a collection of lines in F^2. Then:

$$|\{(p,\ell) \in P \times L : p \in \ell\}| \leq \min\left(|P|^{1/2}|L| + |P|, |P||L|^{1/2} + |L|\right).$$

Lemma 35. We let $A, B \subseteq \mathcal{P}$ be arbitrary subsets of $\mathcal{P}$. We define χ_A, χ_B to be the corresponding characteristic functions from $\mathcal{P}$ to $\{0,1\}$. Then:

$$||(\chi_A d\sigma)^\vee(\chi_B d\sigma)^\vee||^2_{L^2(F^3,dx)} \leq 2\cdot\frac{|F|^3}{|\mathcal{P}|^4}\cdot\min\left(|A|^{1/2}|B|^2 + |A||B|, |A||B|^{3/2} + |B|^2\right).$$

Proof. By definition of the L^2 norm, we have:

$$||(\chi_A d\sigma)^\vee(\chi_B d\sigma)^\vee||^2_{L^2(F^3,dx)} = \sum_{x\in F^3} \left|(\chi_A d\sigma)^\vee(x)(\chi_B d\sigma)^\vee(x)\right|^2.$$

Using the definitions of $(\chi_A d\sigma)^\vee$ and $(\chi_B d\sigma)^\vee$, we can expand this as:

$$= \sum_{x \in F^3} \left| \frac{1}{|\mathcal{P}|} \sum_{\xi_1 \in \mathcal{P}} \chi_A(\xi_1) e(x \cdot \xi_1) \cdot \frac{1}{|\mathcal{P}|} \sum_{\xi_2 \in \mathcal{P}} \chi_B(\xi_2) e(x \cdot \xi_2) \right|^2 .$$

We can rewrite this as: $\frac{1}{|\mathcal{P}|^4} \sum_{x \in F^3} \left| \sum_{\xi_1 \in \mathcal{P}} \chi_A(\xi_1) e(x \cdot \xi_1) \cdot \sum_{\xi_2 \in \mathcal{P}} \chi_B(\xi_2) e(x \cdot \xi_2) \right|^2$.

For any complex number z, we note that $|z|^2 = z\overline{z}$, where $\overline{z}$ denotes the complex conjugate of z. This allows us to express the above quantity as:

$$= \frac{1}{|\mathcal{P}|^4} \sum_{x \in F^3} \sum_{a,b,c,d \in \mathcal{P}} \chi_A(a) \chi_B(b) \chi_A(c) \chi_B(d) e(x \cdot a) e(x \cdot b) e(-x \cdot c) e(-x \cdot d).$$

Here, we have used that $\overline{\chi_A} = \chi_A$, $\overline{\chi_B} = \chi_B$, and $\overline{e(x \cdot \xi)} = e(-x \cdot \xi)$.

Since these are finite sums, we can interchange their order to obtain:

$$= \frac{1}{|\mathcal{P}|^4} \sum_{\substack{a,c \in A \\ b,d \in B}} \sum_{x \in F^3} e(x \cdot (a + b - c - d)).$$

This inner sum will be equal to zero except when $a + b = c + d$. When this occurs, the inner sum will equal $|F|^3$. Thus, we get:

$$= \frac{1}{|\mathcal{P}|^4} \sum_{\substack{a+b=c+d \\ a,c \in A \\ b,d \in B}} |F|^3 = \frac{|F|^3}{|\mathcal{P}|^4} \sum_{\substack{a+b=c+d \\ a,c \in A \\ b,d \in B}} 1.$$

Using the fact that $A \subseteq \mathcal{P}$, we observe:

$$\sum_{\substack{a+b=c+d \\ a,c \in A \\ b,d \in B}} 1 = \sum_{\substack{a-d=c-b \\ a,c \in A \\ b,d \in B}} 1 \leq \sum_{\substack{a-d=c-b \\ a \in A \\ b,d \in B \\ c \in \mathcal{P}}} 1.$$

This can be bounded above by:

$$\leq |B| \cdot \max_{b \in B} \sum_{\substack{a-d=c-b \\ a \in A \\ d \in B \\ c \in \mathcal{P}}} 1 \leq |B| \cdot \max_{b \in \mathcal{P}} \sum_{\substack{a-d=c-b \\ a \in A \\ d \in B \\ c \in \mathcal{P}}} 1.$$

We now consider the quantity inside the maximum for an arbitrary, fixed $b \in \mathcal{P}$. To bound this, we will use the Galilean transformation $g_\delta : \mathcal{P} \to \mathcal{P}$, which is defined for each $\delta \in F_*^2$ by:

$$g_\delta(\gamma, \tau) := (\gamma + \delta, \tau + 2\gamma \cdot \delta + \delta \cdot \delta),$$

where $(\gamma, \tau) \in F_*^2 \times F_* = F_*^3$. We note that for each $\delta \in F_*^2$, this is a bijective map from $\mathcal{P}$ to itself.

Claim 36. We write $b \in \mathcal{P}$ as $b = (\nu, \nu \cdot \nu)$, for $\nu \in F_*^2$. We also define $A' := g_{-\nu}(A)$ and $B' := g_{-\nu}(B)$. We then have:

$$\sum_{\substack{a-d=c-b \\ a \in A \\ d \in B \\ c \in \mathcal{P}}} 1 = \sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A' \\ d' \in B'}} 1.$$

Proof of Claim. We first observe that

$$\sum_{\substack{a-d=c-b \\ a \in A \\ d \in B \\ c \in \mathcal{P}}} 1 = \sum_{\substack{a-d+b \in \mathcal{P} \\ a \in A \\ d \in B}} 1.$$

We will show that for $a \in A, d \in B$, $a-d+b \in \mathcal{P}$ if and only if $g_{-\nu}(a) - g_{-\nu}(d) \in \mathcal{P}$.

We can write a as $(\alpha, \alpha \cdot \alpha)$ for some $\alpha \in F_*^2$, and d as $(\eta, \eta \cdot \eta)$ for some $\eta \in F_*^2$. We can then compute $g_{-\nu}(a) - g_{-\nu}(d)$ as:

$$g_{-\nu}(a) - g_{-\nu}(d) = (\alpha - \eta, \alpha \cdot \alpha - \eta \cdot \eta - 2(\alpha - \eta) \cdot \nu).$$

This will be an element of $\mathcal{P}$ if and only if:

$$(\alpha - \eta) \cdot (\alpha - \eta) = \alpha \cdot \alpha - \eta \cdot \eta - 2(\alpha - \eta) \cdot \nu,$$

which is equivalent to:

$$\eta \cdot \eta - \alpha \cdot \eta + (\alpha - \eta) \cdot \nu = 0.$$

Now, $a - d + b \in \mathcal{P}$ holds if and only if:

$$(\alpha - \eta + \nu) \cdot (\alpha - \eta + \nu) = \alpha \cdot \alpha - \eta \cdot \eta + \nu \cdot \nu,$$

which is also equivalent to:

$$\eta \cdot \eta - \alpha \cdot \eta + \alpha \cdot \nu - \eta \cdot \nu = 0.$$

Thus, $a - d + b \in \mathcal{P}$ if and only if $g_{-\nu}(a) - g_{-\nu}(d) \in \mathcal{P}$. We may then conclude that

$$\sum_{\substack{a-d=c-b \\ a \in A \\ d \in B \\ c \in \mathcal{P}}} 1 = \sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A' \\ d' \in B'}} 1,$$

since $g_{-\nu}$ is a bijection from $\mathcal{P}$ to $\mathcal{P}$. □

We are now interested in bounding the quantity

$$\sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A' \\ d' \in B'}} 1.$$

We note that the contribution to this sum from terms where $d = 0$ is at most $|A'| = |A|$. We note there can be no contribution from terms where $a = 0$ and $d \neq 0$, since having both of $d, -d$ in $\mathcal{P}$ is impossible for $d \neq 0$. Hence, we have:

$$\sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A' \\ d' \in B'}} 1 \leq |A| + \sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A'-\{0\} \\ d' \in B'-\{0\}}} 1.$$

We now define the sets $X_{A'} := \{\gamma \in F_*^2 : (\gamma, \gamma \cdot \gamma) \in A' - \{0\}\}$, $X_{B'} := \{\gamma \in F_*^2 : (\gamma, \gamma \cdot \gamma) \in B' - \{0\}\}$. Letting $a' = (x, x \cdot x)$ and $d' = (y, y \cdot y)$, we note that $a' - d' \in \mathcal{P}$ is equivalent to $x \cdot y = y \cdot y$.

For each $y \in F_*^2$, we can define a line in F_*^2 by $\ell(y) := \{x \in F_*^2 : y \cdot x = y \cdot y\}$. We now prove that these lines are distinct, i.e. y and $\ell(y)$ are in bijective correspondence. We suppose that $\ell(y) = \ell(y')$ for $y, y' \in F_*^2$. We note that $y \in \ell(y)$ and $y' \in \ell(y')$. Since these lines are the same, we must also have $y \in \ell(y')$ and $y' \in \ell(y)$. By definition of $\ell(y), \ell(y')$, this implies that $y \cdot y = y' \cdot y = y' \cdot y'$. Hence, $(y - y') \cdot (y - y') = y \cdot y - 2y' \cdot y + y' \cdot y' = 0$. However, since -1 is not a square in F, this implies that $y - y'$ must be the zero vector in F_*^2. Thus, $y = y'$.

We define $L_{B'}$ to be the collection of lines $L_{B'} := \{\ell(y) : y \in X_{B'}\}$. Since these lines are distinct and $a' - d' \in \mathcal{P}$ if and only if the corresponding x, y satisfy $x \in \ell(y)$, we have that:

$$\sum_{\substack{a'-d' \in \mathcal{P} \\ a' \in A'-\{0\} \\ d' \in B'-\{0\}}} 1 = \left|\{(\ell(y), x) \in L_{B'} \times X_{A'} : x \in \ell(y)\}\right|.$$

We now apply Lemma 34 to conclude:

$$\sum_{\substack{a'-d'\in\mathcal{P}\\ a'\in A'-\{0\}\\ d'\in B'-\{0\}}} 1 \leq \min\left(|X_{A'}|^{1/2}|L_{B'}| + |X_{A'}|, |X_{A'}||L_{B'}|^{1/2} + |L_{B'}|\right).$$

Since $|L_{B'}| = |B'|$, $|X_{A'}| \leq |A'| = |A|$, and $|X_{B'}| \leq |B'| = |B|$, we have:

$$\sum_{\substack{a'-d'\in\mathcal{P}\\ a'\in A'-\{0\}\\ d'\in B'-\{0\}}} 1 \leq \min\left(|A|^{1/2}|B| + |A|, |A||B|^{1/2} + |B|\right).$$

This yields:

$$\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1 \leq |B|\left(|A| + \min\left(|A|^{1/2}|B| + |A|, |A||B|^{1/2} + |B|\right)\right).$$

Since $|B||A| \leq \min\left(|A|^{1/2}|B|^2 + |A||B|, |A||B|^{3/2} + |B|^2\right)$, we have:

$$\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1 \leq 2\min\left(|A|^{1/2}|B|^2 + |A||B|, |A||B|^{3/2} + |B|^2\right).$$

Recalling that

$$||(\chi_A d\sigma)^\vee (\chi_B d\sigma)^\vee||^2_{L^2(F^3,dx)} = \frac{|F|^3}{|\mathcal{P}|^4} \sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1,$$

we see that

$$||(\chi_A d\sigma)^\vee (\chi_B d\sigma)^\vee||^2_{L^2(F^3,dx)}$$
$$\leq 2 \cdot \frac{|F|^3}{|\mathcal{P}|^4} \cdot \min\left(|A|^{1/2}|B|^2 + |A||B|, |A||B|^{3/2} + |B|^2\right).$$

This concludes the proof of the lemma. □

Proof of Theorem. Our task reduces to proving:

$$||(fd\sigma)^\vee||_{L^4(F^3,dx)} = |F|^{3/4-2}(\sum_{\substack{a+b=c+d\\ a,b,c,d\in\mathcal{P}}} f(a)f(b)\overline{f(c)f(d)}\,)^{1/4}$$

$$\leq C|F|^{-5/4}(\sum_{\xi\in\mathcal{P}}|f(\xi)|^{8/5})^{\frac{5}{8}} = C||f||_{L^{8/5}(\mathcal{P},d\sigma)}. \tag{3.4}$$

We note that if we replace f by the non-negative, real-valued function $|f|$, then the quantity $\sum_{\substack{a+b=c+d\\ a,b,c,d\in\mathcal{P}}} f(a)f(b)\overline{f(c)f(d)}$ cannot decrease (by the triangle inequality), and $||f||_{L^{8/5}(\mathcal{P},d\sigma)}$ remains the same. Therefore, we can assume without loss of generality that f is a non-negative, real-valued function. Moreover, if we replace $|f(\xi)|$ by the smallest power of 2 larger than $|f(\xi)|$, so that f is a dyadic step-function, the left-hand side will not decrease, while the right-hand side will increase by at most a factor of 2. Thus if we can establish inequality (3.4) for dyadic step functions for C', the same inequality will hold for all complex-valued functions with $C = 2C'$). By the homogeneity of each side of (3.4), we may assume that $\left(\sum_{\xi\in\mathcal{P}}|f(\xi)|^{8/5}\right)^{\frac{5}{8}} = 1$, and from the previous remarks we may assume that $f(\xi) = \sum_{j=0}^{\infty} 2^{-j}\chi_{E_j}(\xi)$, where the E_j's are disjoint subsets of $\mathcal{P}$. We use later the simple consequences that $\sum_{j=0}^{\infty} 2^{-j\cdot 8/5}|E_j| = 1$ and $|E_j| \leq 2^{j\cdot 8/5}$ for all j. It therefore suffices to show that:

$$||(fd\sigma)^\vee||^2_{L^4(F^3,dx)} = ||(fd\sigma)^\vee(fd\sigma)^\vee||_{L^2(F^3,dx)} \leq (C')^2|F|^{-5/2}.$$

We calculate

$$||(fd\sigma)^\vee(fd\sigma)^\vee||_{L^2(F^3,dx)} = \left|\left|\left(\sum_{j=0}^{\infty} 2^{-j}\chi_{E_j}d\sigma\right)^\vee\left(\sum_{k=0}^{\infty} 2^{-k}\chi_{E_k}d\sigma\right)^\vee\right|\right|_{L^2(F^3,dx)}$$

$$\leq \sum_{j=0}^{\infty} 2^{-j} \sum_{k=0}^{\infty} 2^{-k} ||(\chi_{E_j} d\sigma)^\vee (\chi_{E_k} d\sigma)^\vee||_{L^2(F^3,dx)}$$

$$\leq 2 \sum_{0 \leq k \leq j} 2^{-j-k} ||(\chi_{E_j} d\sigma)^\vee (\chi_{E_k} d\sigma)^\vee||_{L^2(F^3,dx)}.$$

From Lemma 35, we have:

$$||(\chi_{E_j} d\sigma)^\vee (\chi_{E_k} d\sigma)^\vee||_{L^2(F^3,dx)} \leq 2^{1/2} |F|^{-5/2} (|E_j|^{1/2} |E_k|^2 + |E_j||E_k|)^{1/2}.$$

Using the fact that $(|E_j|^{1/2}|E_k|^2 + |E_j||E_k|)^{1/2}$

$\leq (2 \max(|E_j|^{1/2}|E_k|^2, |E_j||E_k|))^{1/2} \leq 2^{1/2}(|E_j|^{1/4}|E_k| + |E_j|^{1/2}|E_k|^{1/2})$,

we obtain:

$$||(\chi_{E_j} d\sigma)^\vee (\chi_{E_k} d\sigma)^\vee||_{L^2(F^3,dx)} \leq 2|F|^{-5/2} \left(|E_j|^{1/4}|E_k| + |E_j|^{1/2}|E_k|^{1/2} \right).$$

Thus it suffices to show

$$2^2 \sum_{0 \leq k \leq j} 2^{-j-k} \left(|E_j|^{1/4}|E_k| + |E_j|^{1/2}|E_k|^{1/2} \right) \leq (C')^2.$$

We consider the two sums $\sum_{0 \leq k \leq j} 2^{-j-k} |E_j|^{1/4}|E_k|$ and

$\sum_{0 \leq k \leq j} 2^{-j-k} |E_j|^{1/2}|E_k|^{1/2}$ separately. First we observe:

$$\sum_{0 \leq k \leq j} 2^{-j-k} |E_j|^{1/4}|E_k| \leq \sum_{0 \leq k \leq j} 2^{-j-k} 2^{j \cdot 2/5} |E_k| = \sum_{0 \leq k \leq j} 2^{-j \cdot 3/5} 2^{-k} |E_k|.$$

We can alternatively express this last quantity as:

$$\sum_{k=0}^{\infty} 2^{-k} |E_k| \left(\sum_{j=k}^{\infty} 2^{-j \cdot 3/5} \right) = \frac{1}{1 - 2^{-3/5}} \sum_{k=0}^{\infty} 2^{-8/5 \cdot k} |E_k|.$$

Recalling that $\sum_{k=0}^{\infty} 2^{-8/5 \cdot k}|E_k| = 1$, we have:

$$\sum_{0 \leq k \leq j} 2^{-j-k}|E_j|^{1/4}|E_k| \leq \frac{1}{1-2^{-3/5}}.$$

To bound the other sum, we simply use $|E_j| \leq 2^{j \cdot 8/5}$ and $|E_k| \leq 2^{k \cdot 8/5}$:

$$\sum_{0 \leq k \leq j} 2^{-j-k}|E_j|^{1/2}|E_k|^{1/2} \leq \sum_{k=0}^{\infty} 2^{-1/5 \cdot k}\left(\sum_{j=k}^{\infty} 2^{-1/5 \cdot j}\right) = \frac{1}{(1-2^{-1/5})(1-2^{-2/5})}.$$

This shows that for f of the form $f(\xi) = \sum_{j=0}^{\infty} 2^{-j}\chi_{E_j}(\xi)$, we have $||(fd\sigma)^{\vee}||^2_{L^4(F^3,dx)} \leq (C')^2|F|^{-5/2}$, for $C' = 2\left(\frac{1}{\left(1-2^{-1/5}\right)\left(1-2^{-2/5}\right)} + \frac{1}{1-2^{-3/5}}\right)^{1/2}$. Therefore, for arbitrary complex-valued functions f, we have $||(fd\sigma)^{\vee}||_{L^4(F^3,dx)} \leq C||f||_{L^{8/5}(\mathcal{P},d\sigma)}$, where C can be set to $4\left(\frac{1}{\left(1-2^{-1/5}\right)\left(1-2^{-2/5}\right)} + \frac{1}{1-2^{-3/5}}\right)^{1/2}$. This concludes the proof of the theorem. □

3.3 Restriction Theorem for the Paraboloid in Higher Dimensions

We now consider the paraboloid $\mathcal{P}$ in F^n for values of $n > 3$. We begin by presenting a combinatorial lemma.

3.3.1 A Combinatorial Lemma

Lemma 37. For any sets $A, B \subseteq \mathcal{P} \subseteq F^n$ where $n \geq 4$ is even or n is odd and $|F| = q^m$ for some prime q congruent to 3 modulo 4 with $m(n-1)$ not a

multiple of 4, we have:

$$\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1 \ll |F|^{(n-2)/4}|A||B|^{3/2} + |F|^{(n-2)/2}|A||B| + |F|^{-1}|A||B|^2,$$

which implies

$$\left(\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1\right)^{1/2} \ll |F|^{(n-2)/8}|A|^{1/2}|B|^{3/4} + |F|^{(n-2)/4}|A|^{1/2}|B|^{1/2} + |F|^{-1/2}|A|^{1/2}|B|.$$

Proof. We follow the strategy used to prove Lemmas 7 and 8 in [30], generalizing it appropriately to allow arbitrary A and B (in the [30] lemmas, $A = B$). We first note:

$$\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1 \leq \sum_{\substack{a+b=c+d\\ a\in A\\ b,d\in B\\ c\in\mathcal{P}}} 1 = \sum_{\substack{a+b-d\in\mathcal{P}\\ a\in A\\ b,d\in B}} 1.$$

We can express a point $a \in \mathcal{A}$ as $a = (\underline{a}, \underline{a}\cdot\underline{a})$, for some $\underline{a} \in F_*^{n-1}$. Then, $a + b - d \in \mathcal{P}$ if and only if $\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d} = 0$. We let δ denote the function on F_* which is 1 when the input is 0 and is 0 otherwise. We then have:

$$\sum_{\substack{a+b-d\in\mathcal{P}\\ a\in A\\ b,d\in B}} 1 = \sum_{\substack{a\in A\\ b,d\in B}} \delta(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d}).$$

Now, for any value $t \in F_*$, we note that $\delta(t) = |F|^{-1}\sum_{s\in F_*} e(st)$. Thus, we have:

$$\sum_{\substack{a\in A\\ b,d\in B}} \delta(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d}) = |F|^{-1}\sum_{\substack{a\in A\\ b,d\in B}}\sum_{s\in F_*} e(s(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d})).$$

We note that when $s = 0$, the value of the sum over a, b, d is equal to $|A||B|^2$. This gives us:

$$|F|^{-1} \sum_{\substack{a \in A \\ b,d \in B}} \sum_{s \in F_*} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d}))$$

$$= |F|^{-1}|A||B|^2 + |F|^{-1} \sum_{\substack{a \in A \\ b,d \in B}} \sum_{\substack{s \in F_* \\ s \neq 0}} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d})).$$

We now consider upper bounding the quantity

$$\left| \sum_{\substack{a \in A \\ b,d \in B}} \sum_{\substack{s \in F_* \\ s \neq 0}} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d})) \right|^2 .$$

By the triangle inequality, this is:

$$\leq \left(\sum_{a \in A} \left| \sum_{\substack{b,d \in B \\ s \in F_* \\ s \neq 0}} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d})) \right| \right)^2 .$$

By applying the Cauchy-Schwarz inequality to the sum over a, this is:

$$\leq |A| \sum_{a \in A} \left| \sum_{\substack{b,d \in B \\ s \in F_* \\ s \neq 0}} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d})) \right|^2 .$$

Again employing the triangle inequality, we have:

$$\leq |A| \sum_{a \in A} \left(\sum_{d \in B} \left| \sum_{\substack{b \in B \\ s \in F_* \\ s \neq 0}} e(s(\underline{a} \cdot \underline{b} - \underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{d} + \underline{d} \cdot \underline{d})) \right| \right)^2 .$$

By applying the Cauchy-Schwarz inequality to the sum over d, this is:

$$\leq |A||B| \sum_{a\in A} \sum_{d\in B} \left| \sum_{\substack{b\in B \\ s\in F_* \\ s\neq 0}} e(s(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d})) \right|^2 .$$

Since $B \subseteq \mathcal{P}$, this is:

$$\leq |A||B| \sum_{a\in A} \sum_{\underline{d}\in F_*^{n-1}} \left| \sum_{\substack{b\in B \\ s\in F_* \\ s\neq 0}} e(s(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d})) \right|^2 .$$

For any $\underline{a} \in F_*^{n-1}$, we define the quantity $M(\underline{a})$ (with respect to B) as in [30]:

$$M(\underline{a}) := \sum_{\underline{d}\in F_*^{n-1}} \left| \sum_{\substack{b\in B \\ s\in F_* \\ s\neq 0}} e(s(\underline{a}\cdot\underline{b} - \underline{a}\cdot\underline{d} - \underline{b}\cdot\underline{d} + \underline{d}\cdot\underline{d})) \right|^2 .$$

In [30], they prove for even $n \geq 4$ that[1]

$$M(\underline{a}) \ll |F|^{\frac{n+2}{2}}|B|^2 + |F|^n|B|$$

holds for all $\underline{a} \in F_*^{n-1}$.

This gives us:

$$|A||B| \sum_{a\in A} M(\underline{a}) \ll |A|^2|B| \left(|F|^{\frac{n+2}{2}}|B|^2 + |F|^n|B| \right).$$

[1]Actually, they state this for $\underline{a}$ such that $a \in B$ (since $A = B$ in their case), but their proof never uses that $a \in B$, so it extends without modification to all $\underline{a}$'s.

By substituting this into our bounds above, we have that:

$$\sum_{\substack{a+b-d\in\mathcal{P}\\ a\in A\\ b,d\in B}} 1 \ll |F|^{-1}|A||B|^2 + |F|^{-1}\left(|A|^2|B|\left(|F|^{\frac{n+2}{2}}|B|^2 + |F|^n|B|\right)\right)^{1/2},$$

which is

$$\ll |F|^{-1}|A||B|^2 + |F|^{-1}|F|^{\frac{n+2}{4}}|A||B|^{3/2} + |F|^{-1}|F|^{\frac{n}{2}}|A||B|$$

$$= |F|^{-1}|A||B|^2 + F^{\frac{n-2}{4}}|A||B|^{3/2} + |F|^{\frac{n-2}{2}}|A||B|.$$

For odd n when $|F| = q^m$ for some prime q congruent to 3 modulo 4 with $m(n-1)$ not a multiple of 4, they prove in [30] that [2]

$$M(\underline{a}) \ll |F|^n|B| + |F|^{\frac{n+1}{2}}|B|^2$$

holds for all $\underline{a} \in F_*^{n-1}$.

This gives us:

$$|A||B|\sum_{a\in A} M(\underline{a}) \ll |A|^2|B|\left(|F|^n|B| + |F|^{\frac{n+1}{2}}|B|^2\right).$$

By substituting this into our bounds above, we have that:

$$\sum_{\substack{a+b-d\in\mathcal{P}\\ a\in A\\ b,d\in B}} 1 \ll |F|^{-1}|A||B|^2 + |F|^{-1}|A||B|^{1/2}\left(|F|^n|B| + |F|^{\frac{n+1}{2}}|B|^2\right)^{1/2},$$

which is

$$\ll |F|^{-1}|A||B|^2 + |F|^{\frac{n-2}{2}}|A||B| + |F|^{\frac{n-3}{4}}|A||B|^{3/2}.$$

We note that this is actually a somewhat better estimate than the lemma requires, since $|F|^{\frac{n-3}{4}} < |F|^{\frac{n-2}{4}}$. □

[2] Again, they state this for $\underline{a}$ such that $a \in B$ (since $A = B$ in their case), but their proof never uses that $a \in B$, so it extends without modification to all $\underline{a}$'s.

3.3.2 Proof of the theorem

We recall that $p := \frac{4n}{3n-2}$. We now prove Theorem 2, restated below in an equivalent formulation:

Theorem 33. When $n \geq 4$ is even or when n is odd and $|F| = q^m$ for a prime q congruent to 3 modulo 4 such that $m(n-1)$ is not a multiple of 4, for every function $f : \mathcal{P} \to \mathbb{C}$ we have that:

$$||(fd\sigma)^\vee||_{L^4(F^n,dx)} \ll ||f||_{L^p(\mathcal{P},d\sigma)}.$$

Proof. Expanding the L^4 norm, we see that our task reduces to proving:

$$||(fd\sigma)^\vee||_{L^4(F^n,dx)} = |F|^{1-3n/4} \left(\sum_{\substack{a+b=c+d \\ a,b,c,d \in \mathcal{P}}} f(a)f(b)\overline{f(c)f(d)} \right)^{1/4}$$

$$\leq C|F|^{5/4-1/2n-3n/4} \left(\sum_{\xi \in \mathcal{P}} |f(\xi)|^{\frac{4n}{3n-2}} \right)^{\frac{3n-2}{4n}} = ||f||_{L^{\frac{4n}{3n-2}}(\mathcal{P},d\sigma)}. \tag{3.5}$$

We will find it more convenient to prove the equivalent formulation:

$$|F|^{3n/2-2}||(fd\sigma)^\vee (fd\sigma)^\vee||_{L^2(F^n,dx)} = \left(\sum_{\substack{a+b=c+d \\ a,b,c,d \in \mathcal{P}}} f(a)f(b)\overline{f(c)f(d)} \right)^{1/2}$$

$$\ll |F|^{1/2-1/n} \left(\sum_{\xi \in \mathcal{P}} |f(\xi)|^{\frac{4n}{3n-2}} \right)^{\frac{3n-2}{2n}}.$$

As before, we may assume that $f = \sum_{j=0}^{\infty} 2^{-j}\chi_{E_j}$ is a dyadic step function. Moreover, we will normalize f to have L^p norm 1 in the counting measure. In other words, $\sum_{j=0}^{\infty} 2^{-pj}|E_j| = 1$. It now suffices to prove

$$|F|^{(3n/2-5/2+1/n)} \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} 2^{-j}2^{-k}||(\chi_{E_j}d\sigma)^{\vee}(\chi_{E_k}d\sigma)^{\vee}||_{L^2(F^n,dx)} \ll 1.$$

Observe that $|F|^{3n/2-2}\,||(\chi_A d\sigma)^{\vee}(\chi_B d\sigma)^{\vee}||_{L^2(F^n,dx)} = (\sum_{\substack{a+b=c+d\\ a,c\in A\\ b,d\in B}} 1)^{1/2}$. Hence, we can rewrite the inequality to be proved as:

$$\sum_{j=0}^{\infty}\sum_{k=0}^{\infty} 2^{-j-k}(\sum_{\substack{a+b=c+d\\ a,c\in E_j\\ b,d\in E_k}} 1)^{1/2} \ll |F|^{1/2-1/n}.$$

By the symmetry of j and k, it suffices to show

$$\sum_{j=0}^{\infty}\sum_{k=j}^{\infty} 2^{-j-k}(\sum_{\substack{a+b=c+d\\ a,c\in E_j\\ b,d\in E_k}} 1)^{1/2} \ll |F|^{1/2-1/n}.$$

Lemma 37 gives us an upper bound on the quantity $(\sum_{\substack{a+b=c+d\\ a,c\in E_j\\ b,d\in E_k}} 1)^{1/2}$, but we can also obtain the simpler upper bound of $|E_j||E_k|^{1/2}$ by noting that for fixed values of $a, c \in E_j, b \in E_k$, there is at most one value of $d \in E_k$ which satisfies $a + b = c + d$.

We will split this sum into three pieces according to the following cases: 1. $|E_j| \leq |F|^{\frac{n-2}{2}}$, 2. $|E_k| \leq |F|^{\frac{n-2}{2}}$, and 3. $|F|^{\frac{n-2}{2}} \leq |E_j|, |E_k| \leq |F|^{n-1}$.

We note that the union of these three cases covers all possibilities for subsets $E_j, E_k \subseteq \mathcal{P}$. We first consider case 1. We let J denote the subset of j's

satisfying $|E_j| \leq |F|^{\frac{n-2}{2}}$. We also let U denote the value $\log_2\left(|F|^{\frac{(n-2)(3n-2)}{8n}}\right)$. We note that when $j \leq U$, the bound $|E_j| \leq 2^{pj}$ is better than the bound $|E_j| \leq |F|^{\frac{n-2}{2}}$, and when $j > U$, the latter bound is better.

We consider:

$$\sum_{j\in J}\sum_{k=j}^{\infty} 2^{-j-k}\,(\sum_{\substack{a+b=c+d\\ a,c\in E_j\\ b,d\in E_k}} 1)^{1/2} \leq \sum_{j\in J}\sum_{k=j}^{\infty} 2^{-j-k}|E_j||E_k|^{1/2}.$$

Here, we have used the simple upper bound of $|E_j||E_k|^{1/2}$ noted above. We can rewrite this as:

$$\sum_{\substack{j\in J\\ j\leq U}}\sum_{k=j}^{\infty} 2^{-j-k}|E_j||E_k|^{1/2} + \sum_{\substack{j\in J\\ j> U}}\sum_{k=j}^{\infty} 2^{-j-k}|E_j||E_k|^{1/2}.$$

Since we have assumed that $\sum_{j=0}^{\infty} 2^{-pj}|E_j| = 1$, we always have that $|E_j| \leq 2^{pj}$. Applying this to the first sum, we see that:

$$\sum_{\substack{j\in J\\ j\leq U}}\sum_{k=j}^{\infty} 2^{-j-k}|E_j||E_k|^{1/2} \ll \sum_{\substack{j\in J\\ j\leq U}}\sum_{k=j}^{\infty} 2^{-j-k}2^{pj}2^{pk/2}.$$

Since $p/2 < 1$, the geometric sum over the k values is convergent, and the value of the sum is bounded by a constant (depending on n) times its first term. Hence, we have that this is $\ll \sum_{\substack{j\in J\\ j\leq U}} 2^{j(3/2p-2)}$. The exponent $(3/2p-2)$ here is equal to $\frac{4}{3n-2} > 0$, so this geometric sum is bounded by a constant (depending on n) times its largest term, which is:

$$\ll 2^{U(3/2p-2)} = |F|^{\frac{(n-2)(3n-2)(3/2p-2)}{8n}} = |F|^{1/2-1/n}.$$

We now consider the sum:

$$\sum_{\substack{j\in J\\ j>U}}\sum_{k=j}^{\infty} 2^{-j-k}|E_j||E_k|^{1/2}.$$

Noting that $|E_j| \leq |F|^{\frac{n-2}{2}}$ and $|E_k| \leq 2^{pk}$, we have:

$$\ll |F|^{\frac{n-2}{2}} \sum_{\substack{j\in J\\ j>U}}\sum_{k=j}^{\infty} 2^{-j-k}2^{pk/2}.$$

Again, since $p/2 < 1$, the geometric sum of k is convergent, so

$\ll |F|^{\frac{n-2}{2}} \sum_{\substack{j\in J\\ j>U}} 2^{j(p/2-2)}$. The exponent $p/2-2$ is negative, so this geometric series in j converges, and we have:

$$\ll |F|^{\frac{n-2}{2}}2^{U(p/2-2)} = |F|^{\frac{n-2}{2}+\frac{(n-2)(3n-2)(p/2-2)}{8n}} = |F|^{1/2-1/n}.$$

This concludes our proof for values of $j \in J$.

We note cases 1 and 2 are symmetric, and we are left with considering case 3, where $j, k \notin J$. In this case, we apply the bound provided by Lemma 37 with $A := E_k$ and $B := E_j$:

$$\sum_{j\notin J}\sum_{\substack{k\notin J\\ k\geq j}} 2^{-j-k}\left(\sum_{\substack{a+b=c+d\\ a,c\in E_j\\ b,d\in E_k}} 1\right)^{1/2} \ll \sum_{j\notin J}\sum_{\substack{k\notin J\\ k\geq j}} 2^{-j-k}|F|^{(n-2)/8}|E_k|^{1/2}|E_j|^{3/4}$$

$$+\sum_{j\notin J}\sum_{\substack{k\notin J\\ k\geq j}} 2^{-j-k}|F|^{(n-2)/4}|E_k|^{1/2}|E_j|^{1/2} + \sum_{j\notin J}\sum_{\substack{k\notin J\\ k\geq j}} 2^{-j-k}|F|^{-1/2}|E_k|^{1/2}|E_j|.$$

We observe that

$$|F|^{(n-2)/4}|E_k|^{1/2}|E_j|^{1/2} \leq |F|^{(n-2)/8}|E_k|^{1/2}|E_j|^{3/4}$$

as long as $|F|^{(n-2)/2} \leq |E_j|$, i.e. whenever $j \notin J$. Thus, it suffices to bound the first and third sums. We consider the first sum with the change of variable $j = k - \ell$:

$$\sum_{j \notin J} \sum_{\substack{k \notin J \\ k \geq j}} 2^{-j-k} |F|^{(n-2)/8} |E_k|^{1/2} |E_j|^{3/4} \leq |F|^{(n-2)/8} \sum_{\ell=0}^{\infty} 2^{\ell} \sum_{\substack{k \geq \ell \\ k \notin J}} 2^{-2k} |E_k|^{1/2} |E_{k-\ell}|^{3/4}.$$

We define the values $0 \leq c_k \leq 1$ by $|E_k| = c_k 2^{kp}$. We recall that $\sum_{k=0}^{\infty} 2^{-kp} |E_k| = 1$ implies that the sum $\sum_{k=0}^{\infty} c_k$ converges (in particular, it is equal to 1). We can rewrite the quantity above as:

$$= |F|^{(n-2)/8} \sum_{\ell=0}^{\infty} 2^{\ell(1-3/4p)} \sum_{\substack{k \geq \ell \\ k \notin J}} c_k^{1/2} \; c_{k-\ell}^{3/4} \; 2^{k(5/4p-2)}.$$

For $k \notin J$, we have that $|F|^{\frac{n-2}{2}} \leq |E_k| \leq 2^{pk}$, so $2^k \geq |F|^{\frac{n-2}{2p}}$. We note that $5/4p - 2 = \frac{4-n}{3n-2} \leq 0$, so

$$2^{k(5/4p-2)} \leq |F|^{\frac{(n-2)(5/4p-2)}{2p}} = |F|^{\frac{(n-2)(4-n)}{8n}}.$$

We thus have:

$$|F|^{(n-2)/8} \sum_{\ell=0}^{\infty} 2^{\ell(1-3/4p)} \sum_{\substack{k \geq \ell \\ k \notin J}} c_k^{1/2} \; c_{k-\ell}^{3/4} \; 2^{k(5/4p-2)}$$

$$\ll |F|^{\frac{n-2}{8} + \frac{(n-2)(4-n)}{8n}} \sum_{\ell=0}^{\infty} 2^{\ell(1-3/4p)} \sum_{\substack{k \geq \ell \\ k \notin J}} c_k^{1/2} c_{k-\ell}^{3/4}.$$

We note that $\frac{n-2}{8} + \frac{(n-2)(4-n)}{8n} = 1/2 - 1/n$. For each fixed ℓ, we apply the Cauchy-Schwarz inequality to the inner sum over k to obtain:

$$\ll |F|^{1/2-1/n} \sum_{\ell=0}^{\infty} 2^{\ell(1-3/4p)} \left(\sum_{k=\ell}^{\infty} c_k \right)^{1/2} \left(\sum_{k=\ell}^{\infty} c_{k-\ell}^{3/2} \right)^{1/2}.$$

Since $0 \leq c_k \leq 1$, we have that $c_{k-\ell}^{3/2} \leq c_{k-\ell}$ for all k, ℓ, so $\sum_{k=0}^{\infty} c_k = 1$ implies this is:

$$\ll |F|^{1/2-1/n} \sum_{\ell=0}^{\infty} 2^{\ell(1-3/4p)}.$$

Now, $1 - 3/4p = \frac{-2}{3n-2} < 0$, so this geometric sum over ℓ converges, and we obtain $\ll |F|^{1/2-1/n}$, as desired.

We now consider the third sum, $\sum_{j \notin J} \sum_{\substack{k \notin J \\ k \geq j}} 2^{-j-k} |F|^{-1/2} |E_k|^{1/2} |E_j|$. We define the value U to be: $U := \log_2 \left(|F|^{(n-1)/p} \right)$. We note that when $j \leq U$, the bound $|E_j| \leq 2^{pj}$ is better than the bound $|E_j| \leq |F|^{n-1}$, and when $j > U$, the latter bound is better.

Our sum is then:

$$\ll |F|^{-1/2} \sum_{j \leq U} \sum_{k \geq j} 2^{-k-j} |E_j| |E_k|^{1/2} + |F|^{-1/2} \sum_{j \geq U} \sum_{k \geq j} 2^{-k-j} |E_j| |E_k|^{1/2}.$$

For the first of these two sums, we use $|E_j| \leq 2^{pj}$ and $|E_k| \leq 2^{pk}$:

$$|F|^{-1/2} \sum_{j \leq U} \sum_{k \geq j} 2^{-k-j} |E_j| |E_k|^{1/2} \ll |F|^{-1/2} \sum_{j \leq U} \sum_{k \geq j} 2^{j(p-1)} 2^{k(p/2-1)}.$$

Since $p/2 < 1$, the geometric sum over k is convergent, and we get

$\ll |F|^{-1/2} \sum_{j \leq U} 2^{j(3/2p-2)}$. Now, $3/2p - 2 = \frac{4}{3n-2} > 0$, so this is:

$$\ll |F|^{-1/2} 2^{U(3/2p-2)} = |F|^{-1/2} |F|^{\frac{(n-1)(3/2p-2)}{p}} = |F|^{1/2-1/n}.$$

To bound the sum for values of $j > U$, we use that $|E_j| \leq |F|^{n-1} = |\mathcal{P}|$ and $|E_k| \leq 2^{kp}$:

$$|F|^{-1/2} \sum_{j \geq U} \sum_{k \geq j} 2^{-k-j} |E_j| |E_k|^{1/2} \ll |F|^{-1/2+n-1} \sum_{j \geq U} \sum_{k \geq j} 2^{-j} 2^{k(p/2-1)}.$$

The geometric sum over k is convergent, so we have $\ll |F|^{-1/2+n-1} \sum_{j \geq U} 2^{j(p/2-2)}$.

The geometric sum over j is now also convergent, so we have:

$$\ll |F|^{-1/2+n-1} |F|^{\frac{(n-1)(p/2-2)}{p}} = |F|^{1/2-1/n}.$$

This concludes the proof of the theorem. $\square$

Chapter 4

Estimates for the Square Variation of Partial Sums of Fourier Series and their Rearrangements

4.1 Introduction

Let $\mathbb{T} := [0,1]$ denote the unit interval with Lebesgue measure dx and let $\Phi := \{\phi_n\}_{n\in\mathbb{N}}$ denote an orthonormal system (ONS) of real or complex valued functions on $\mathbb{T}$. By an ONS, we will always mean the set of orthonormal functions $\{\phi_n\}_{n\in\mathbb{N}}$ *and* the ordering inherited from the index set $\mathbb{N}$. For $f \in L^2$, we let $a_n = \langle f, \phi_n \rangle$ denote the Fourier coefficients of f with respect to the system Φ. Associated to an ONS is the maximal partial sum operator

$$\mathcal{M}f(x) := \sup_N \left| \sum_{n=1}^{N} a_n \phi_n(x) \right|.$$

It is well known that the L^2 boundedness of the operator $\mathcal{M}$ implies the almost everywhere convergence of the partial sums of the expansion of $f \in L^2$ in terms of the ONS Φ. Almost everywhere convergence is known to fail for some ONS, hence the maximal function $\mathcal{M}$ is known to be an unbounded operator on L^2 for some ONS. There is an optimal estimate known for general ONS.

Theorem 38. *(Rademacher-Menshov)* Let $\{\phi_n\}_{n\in\mathbb{N}} = \Phi$ and $f \in L^2$ be as above. Then,

$$||\mathcal{M}f||_{L^2} \ll \left(\sum_{n=1}^{\infty} |a_n|^2 \ln^2(n+1)\right)^{\frac{1}{2}}$$

where the implied constant is absolute. Moreover, the function $\ln^2(n+1)$ cannot be replaced with any function that is $o(ln^2(n+1))$.

This last claim is quite deep and is due solely to Menshov.

While this estimate is optimal in general, it can be improved for many specific systems. For instance, the inequality $||\mathcal{M}f||_{L^2} \ll ||f||_{L^2}$ is known to hold when Φ is taken to be the trigonometric, Rademacher, or Haar systems. We recall the definitions of these systems in the next section.

Recently, variational norm refinements of the maximal function results stated above have been investigated. To state these results, we first need to introduce some notation. Let $a = \{a_n\}_{n=1}^{\infty}$ be a sequence of complex numbers. Then we define the r-variation as:

$$||a||_{V^r} := \lim_{K\to\infty} \sup_{\mathcal{P}_K} \left(\sum_{I\in\mathcal{P}_K} \left|\sum_{n\in I} a_n\right|^r\right)^{1/r},$$

where the supremum is taken over all partitions $\mathcal{P}_K$ of $[K]$ (i.e. all ways of dividing $[K]$ into disjoint subintervals). When a is a finite sequence of length K, the quantity is defined by dropping the $\lim_{K\to\infty}$.

One can easily verify that this is a norm and is nondecreasing as r decreases. Now we will denote the sequence $\{a_n\phi_n(x)\}_{n=1}^{\infty}$ by $S[f](x)$. (Note

that this is slightly different than the notation used in [52].) When we write $||S[f]||_{V^r}(x)$, we mean the function on $\mathbb{T}$ whose value at $x \in \mathbb{T}$ is obtained by assigning the r-th variation of the sequence $S[f](x)$. Furthermore, $||S[f]||_{L^p(V^r)}$ is the L^p norm of this function. Alternately, we have

$$||f||_{V^2}(x) = \sup_K \sup_{n_0<\ldots<n_K} \left(\sum_{l=1}^{K} |S_{n_l}[f](x) - S_{n_{l-1}}[f](x)|^2 \right)^{1/2},$$

where $S_{n_l}[f](x) = \sum_{n=1}^{n_l} a_n \phi_n(x)$ is the n_l-th partial sum.

We note that the function $||S[f]||_{V^\infty}(x)$ is essentially the maximal function. More precisely, $\mathcal{M}f(x) \ll ||S[f]||_{V^\infty}(x) \ll \mathcal{M}f(x)$. Since the quantity $||a||_{V^r}$ is nondecreasing as r decreases, we see that $||S[f]||_{V^r}(x)$ majorizes the maximal function whenever $r < \infty$. In [52], the following is proved for the trigonometric system $\{e^{2\pi inx}\}_{n=1}^{\infty}$:

Theorem 39. Let $r > 2$ and $r' < p < \infty$, where $\frac{1}{r} + \frac{1}{r'} = 1$. Then

$$||S[f]||_{L^p(V^r)} \leq C_{p,r}||f||_{L^p},$$

where $C_{p,r}$ is a constant depending only on p and r.

This result is rather deep, being a strengthened version of the celebrated work of Carleson and Hunt on the almost everywhere convergence of Fourier series. The analogous inequalities were previously obtained in [32] in the simpler situation of Cesàro partial sums of the trigonometric system. Moreover, the above inequality is known to hold for the Haar system and more generally for martingale differences by Lepingles inequality, a variational variant of Doob's maximal inequality. In [52], it is shown that the condition $r > 2$

is necessary in case of the trigonometric system. Our focus here will be to study the case $p = r = 2$ for general ONS. In this direction, we prove (closely following the classical proof):

Theorem 40. Let Φ be an ONS. Then

$$||S[f]||_{L^2(V^2)} \ll \left(\sum_{n=1}^{\infty} |a_n|^2 \ln^2(n+1) \right)^{1/2}. \tag{4.1}$$

If $||\mathcal{M}f||_{L^2} \ll \Delta(N)||f||_{L^2}$ for all $f = \sum_{n=1}^{N} a_n \phi_n$ for some real valued function $\Delta(N)$, then

$$|||f||_{L^2(V^2)} \ll \left(\sum_{n=1}^{N} \Delta(n) \ln(n+1) |a_n|^2 \right)^{1/2}. \tag{4.2}$$

Interestingly, the first inequality strengthens the Rademacher-Menshov theorem stated above, since the right sides are the same (up to implicit constants), yet we have replaced the maximal function with the square variation operator V^2 on the left side. Since the V^2 operator dominates the maximal operator, this implies the Rademacher-Menshov theorem and the claim that this result is sharp follows from the sharpness of Rademacher-Menshov. This might lead one to think that the two operators behave similarly, however we will see that the V^2 operator is much larger than the maximal operator for the classical systems. Theorem 40 can be refined further for certain classes of ONS, see Section 4.7 for discussion of this.

We can apply (4.2) to the trigonometric system with $\Delta(N) = O(1)$, the Carleson-Hunt inequality, and obtain the following corollary:

Corollary 41. Let $\{e^{2\pi inx}\}_{n=1}^{\infty}$ be the trigonometric system. We then have

$$||S[f]||_{L^2(V^2)} \ll \left(\sum_{n=1}^{\infty} |a_n|^2 \ln(n+1)\right)^{1/2}. \tag{4.3}$$

Moreover, the function $\ln(n+1)$ cannot be replaced by a function that is $o(\ln(n+1))$.

The lower bound can be obtained by considering the Dirichlet kernel $D_N(x) = \sum_{n=1}^{N} e^{2\pi inx}$. A proof of this is contained in Section 2 of [52]. Strictly speaking, they work with the de la Vallee-Poussin kernel there, but the same proof works for the Dirichlet kernel.

As we will see below, it is easy to construct an infinite ONS such that $||S[f]||_{L^2(V^2)} \ll ||f||_{L^2}$ holds, by choosing the basis functions $\phi_n(x)$ to have disjoint supports. However, this is a very contrived ONS, and it is then natural to ask if there exists a complete ONS such that $||S[f]||_{L^2(V^2)} \ll ||f||_{L^2}$. This is not possible. In fact, we show slightly more:

Theorem 42. Let $\{\phi_n\}$ be a complete orthogonal system. There exists a L^∞ function such that $||S[f]||_{V^2}(x) = \infty$ for almost every x.

In general, this divergence cannot be made quantitative. We show that for any function $w(n) \to \infty$, there exists a complete ONS such that $||S[f]||_{L^2(V^2)} \ll w(N)||f||_{L^2}$ whenever $f(x) = \sum_{n=1}^{N} a_n\phi_n(x)$. However, a quantitative refinement is possible if we restrict our attention to uniformly bounded ONS:

Theorem 43. In the case of a uniformly bounded ONS, it is not possible for $w(N) = o(\sqrt{\ln\ln(N)})$. However, there do exist uniformly bounded ONS such that $w(N) = O(\sqrt{\ln\ln(N)})$.

The Rademacher system provides an example of the second claim. See Theorem 46 below.

Recall that we defined an ONS to be a sequence of orthonormal functions with a specified ordering. This is essential since the behavior of the maximal and variational operators depend heavily on the ordering. For instance, the Carleson-Hunt bound on the maximal function for the trigonometric system makes essential use of the ordering of the system, and the result is known to fail for other orderings. It is thus natural to ask what one can say about the V^2 operator for reorderings of the trigonometric system. Surprisingly, it turns out that the $O(\sqrt{\ln(N)})$ bound can be improved to $O(\sqrt{\ln\ln(N)})$ for any choice of coefficients by reordering the system. More generally:

Theorem 44. Let $\{\phi_n\}_{n=1}^N$ be an ONS such that $|\phi_n(x)| = 1$ for all x and n, and let $f(x) = \sum_{n=1}^N a_n\phi_n(x)$. Then there exists a permutation $\pi : [N] \to [N]$ such that

$$||f||_{L^2(V^2)} \ll \sqrt{\ln\ln(N)}||f||_{L^2}$$

holds (for sufficiently large N) with respect to the rearranged ONS $\{\psi_n\}_{n=1}^N$, where $\psi_n(x) := \phi_{\pi(n)}(x)$.

This is perhaps the most technically interesting part of the paper. This result should be compared to Garsia's theorem [21], which states that the

Fourier series of an arbitrary function with respect to an arbitrary ONS can be rearranged so that the maximal function is bounded on L^2. Garsia's proof proceeds by selecting a uniformly random permutation, and arguing that it will satisfy the claim with positive probability. In our case, however, we randomize over a subset of all permutations. This subset is chosen based on structural information about the Fourier coefficients of the function. It is unclear if this restriction is necessary or an artifact of our proof techniques. It would be interesting to extend this result to more general ONS. We note that it can be seen from the work of Qian [58] (see also our refinement [36]) that $||\sum_{n=1}^{N} r_n||_{L^2(V^2)} \gg \sqrt{N \ln\ln(N)} = \sqrt{\ln\ln(N)}\ ||\sum_{n=1}^{N} r_n||_{L^2}$, regardless of the ordering of the Rademacher functions r_n, hence the $\sqrt{\ln\ln(N)}$ term in the statement of the theorem is sharp. A similar result can be obtained for general ONS when the coefficients are multiplied by random signs:

Theorem 45. Let $\{\phi_n\}_{n=1}^{N}$ be an ONS and $f(x) = \sum_{n=1}^{N} a_n \phi_n(x)$. Then there exists a sequence of signs ϵ_n such that

$$||g||_{L^2(V^2)} \ll_M \sqrt{\ln\ln(N)}\ ||g||_{L^2}$$

holds, where $g(x) = \sum_{n=1}^{N} \epsilon_n a_n \phi_n(x)$.

This easily follows from the following inequality:

Theorem 46. Let $\{r_n\}_{n=1}^{N}$ be a sequence of uniformly bounded independent random variables. Then

$$\left|\left|\sum_{n=1}^{N} a_n r_n\right|\right|_{L^2(V^2)} \ll \sqrt{\ln\ln(N)} \left(\sum_{n=1}^{N} a_n^2\right)^{1/2}.$$

In particular, combining this with Theorem 43, we see that the L^2 norm of the V^2 operator for the Rademacher system grows like $\sqrt{\ln \ln(N)}$.

Finally, we prove that the V^p norm of some systems can be improved uniformly for all choices of coefficients by a rearrangement, for $p > 2$.

Theorem 47. Let $\{\phi_n\}_{n=1}^N$ be an ONS such that $||\phi_n||_{L^\infty} \leq M$ for each n, and let $p > 2$. There exists a permutation $\pi : [N] \to [N]$ such that the orthonormal system $\{\phi_{\pi(n)}\}_{n=1}^N$ satisfies

$$||S[f]||_{L^2(V^p)} \ll_{M,p} \ln \ln(N) ||f||_{L^2} \tag{4.4}$$

for all $f = \sum_{n=1}^N a_n \phi_n$.

The maximal V^∞ version of this result is due to Bourgain [4] and represents the best progress known towards Garsia and Kolmogorov's rearrangement conjectures. Our methods rely heavily on those developed in that paper. This also leads us to perhaps the most interesting open problem relating to V^2 operators:

Question 48. Does there exist a permutation $\pi : [N] \to [N]$ such that the L^2 norm of the associated V^2 operator on the trigonometric system grows like $o(\sqrt{\ln(N)})$?

Our Theorems 44 and 47 may be viewed as evidence that this may in fact be possible. It is consistent with our knowledge that one could get growth as slow as $\sqrt{\ln \ln(N)}$. It is known that purely probabilistic techniques in the maximal (V^∞) case can only go as far as Bourgain's bound of $\ln \ln(N)$ (see

Remark 2 of [4]). Thus, finding a permutation that reduces the growth further (Garsia's conjecture is the assertion that there exists a rearrangement that gets to $O(1)$) would require fundamentally new ideas. However, it is consistent with our current knowledge that the purely probabilistic techniques could get one down to $\ln\ln(N)$ in the V^2 case. If true, this will certainly require a much more delicate analysis than the methods used here. Theorem 40 combined with the V^∞ case of the previous theorem does give a bound of $\sqrt{\ln(N)}\ln\ln(N)$ for general bounded ONS for the V^2 operator. This is a nontrivial improvement for some systems, but not the most interesting classical systems.

4.2 Notation and General Remarks

We will work with ONS defined on the unit interval $\mathbb{T}$. The underlying space $\mathbb{T}$ plays almost no role in our proofs (the role is similar to that of a probability space in probability theory), and one could replace it with an abstract probability space.

We assume that the ONS is real valued in most of our results. In these cases, one can obtain the same results for complex valued ONS by splitting into real and imaginary parts and applying the arguments to each. The details are routine so we omit them. The proof of Theorem 44 is the one place where this requires some care, and thus we work with complex valued functions directly there.

We define the trigonometric system to be the system of complex exponentials $\{e^{2\pi inx}\}_{n=1}^{\infty}$. Typically the trigonometric system is defined to be

the doubly infinite system $\{e^{2\pi inx}\}_{n=-\infty}^{\infty}$ and the maximal and variational operators are defined with respect to the symmetric partial sums. However, we find it more convenient to define the trigonometric system this way and avoid having to state all of the following results for both singly and doubly infinite systems. All of our results can easily be transferred to the doubly infinite setting (using symmetric partial sums) by splitting the Fourier series of a function $f \in L^2(\mathbb{T})$ with respect to a doubly infinite system into two functions with singly infinite Fourier series and applying the results in this setting. For instance, note that

$$\mathcal{M}f(x) := \sup_N \left| \sum_{n=-N}^{N} a_n \phi_n(x) \right| \ll \sup_N \left| \sum_{n=-N}^{0} a_n \phi_n(x) \right| + \sup_N \left| \sum_{n=1}^{N} a_n \phi_n(x) \right|.$$

Thus it follows that the L^2 boundedness of the maximal operator associated to the system $\{e^{2\pi inx}\}_{n=1}^{\infty}$ implies the L^2 boudedness of the symmetric maximal operator associated to $\{e^{2\pi inx}\}_{n=-\infty}^{\infty}$, and similarly for the V^p operators.

The Haar system, which we denote by $\{\mathcal{H}_n\}_{n=0}^{\infty}$, is a complete ONS comprised of the following functions. For $k \in \mathbb{N}$ and $1 \leq j \leq 2^k$, we define $\{\mathcal{H}_{k,j}\}$ by

$$\mathcal{H}_{k,j}(x) = \begin{cases} \sqrt{2^k} & x \in \left(\frac{j-1}{2^k}, \frac{j-1/2}{2^k} \right), \\ -\sqrt{2^k} & x \in \left(\frac{j-1/2}{2^k}, \frac{j}{2^k} \right), \\ 0 & \text{otherwise.} \end{cases}$$

We form the system $\mathcal{H}_n$ by ordering the basis functions $\{\mathcal{H}_{k,j}\}$ first by the

parameter k and then by the parameter j, or $\mathcal{H}_n = \mathcal{H}_{j,k}$ for $n = 2^k + j$. Lastly, we set $H_0 = 1$.

The Rademacher system, denoted $\{r_n(x)\}_{n=1}^{\infty}$, is defined by

$$r_n(x) = \operatorname{sign} \sin (2^n \pi x) .$$

The Rademacher system can also be thought of as independent random variables which take each of the values $\{-1, 1\}$ with probability $1/2$.

4.3 Variational Rademacher-Menshov-Type Results

We start by giving a proof of Theorem 40.

It suffices to assume that N is a power of 2, say $N = 2^\ell$. For all i, k such that $0 \leq i \leq \ell$ and $0 \leq k \leq 2^{\ell - i} - 1$, we consider the collection of intervals $I_{k,i} := (k2^i, (k+1)2^i]$.

Lemma 49. Any subinterval of $S \subset [0, 2^\ell]$ can be expressed as the disjoint union of intervals of the form $I_{k,i}$, such as

$$S = \bigcup_m I_{k_m, i_m} \tag{4.5}$$

where at most two of the intervals I_{k_m, i_m} in the union are of each size, and where the union consists of at most 2ℓ intervals.

Proof. Let $S = [a, b]$ and set $i' := \max_{I_{k,i} \subseteq S} i$. It follows that there are at most two intervals of the form $I_{k,i'}$ contained in S (otherwise S would contain an interval of the form $I_{k,i'+1}$). Let r denote the right-most element of the

interval with the largest k value satisfying $I_{k,i'} \subseteq S$. Now $b - r$ has a unique binary expansion. It easily follows from this that $(r, b]$ can be written as $[r, b] = \bigcup_m I_{k_m,i_m}$ where the union contains only one interval of the form I_{k_m,i_m} of any particular size, and these intervals are disjoint. An analogous argument allows us to obtain a decomposition of this form also for $[a, r']$, where r' is the left-most element of an interval with the smallest k value satisfying $I_{k,i'} \subseteq S$. The lemma follows by taking the union of these two decompositions. □

We now prove

Lemma 50. In the notation above, we have that

$$||S[f]||_{L^2(V^2)} \ll \ln(N) \left(\sum_{n=1}^{\infty} |a_n|^2 \right)^{1/2}. \tag{4.6}$$

Proof. By rounding up to the nearest power of two, we can assume without loss of generality that $N = 2^\ell$ for some positive integer ℓ (this change will only affect the constants absorbed by the $\ll$ notation). Now, for each x, we have some disjoint intervals $J_1, \ldots, J_b \subseteq [N]$ such that:

$$||S[f]||_{V^2}(x) = \sqrt{\sum_{j=1}^{b} \left(\sum_{n \in J_j} a_n \phi_n(x) \right)^2}.$$

It is important to note that these intervals depend on x.

By Lemma 49, each J_j can be decomposed as a disjoint union of the form (4.5). In this disjoint union of intervals I_{k_m,i_m}, each value of i_m appears at most twice. For each j and i, we let I_i^j denote the union of the (at most

two) intervals in the decomposition of J_j which are of length 2^i. We then have:

$$||S[f]||_{V^2}(x) = \sqrt{\sum_{j=1}^{b} \left(\sum_{i=0}^{\ell} \sum_{n \in I_i^j} a_n \phi_n(x) \right)^2}.$$

Applying the triangle inequality for the ℓ^2 norm, this is:

$$\leq \sum_{i=0}^{\ell} \sqrt{\sum_{j=1}^{b} \left(\sum_{n \in I_i^j} a_n \phi_n(x) \right)^2}.$$

Now, since each I_i^j is a union of at most two intervals, this implies:

$$||S[f]||_{V^2}(x) \ll \sum_{i=0}^{\ell} \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left(\sum_{n \in I_{k,i}} a_n \phi_n(x) \right)^2}. \tag{4.7}$$

Notice that we are now summing over all intervals $I_{k,i}$ for each i, regardless of the value of x.

We take the L^2 norm of both sides of (4.7), and apply the triangle inequality to obtain:

$$||S[f]||_{L^2(V^2)} \ll \sum_{i=0}^{\ell} \left\| \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left(\sum_{n \in I_{k,i}} a_n \phi_n(x) \right)^2} \right\|_{L^2}. \tag{4.8}$$

By linearity of the integral and Parseval's identity, we have that

$$\left\| \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left(\sum_{n \in I_{k,i}} a_n \phi_n(x) \right)^2} \right\|_{L^2} = \left(\sum_{k=0}^{2^{\ell-i}-1} \sum_{n \in I_{k,i}} a_n^2 \right)^{\frac{1}{2}} = \left(\sum_{n=1}^{N} a_n^2 \right)^{\frac{1}{2}},$$

for each i. Combining this with (4.8) and noting that there are $\ll \ln N$ values of i, we have:

$$||S[f]||_{L^2(V^2)} \ll \ln(N) \left(\sum_{n=1}^{\infty} |a_n|^2 \right)^{1/2}.$$

□

We now define a variant of the function $||S[f]||_{V^2}(x)$ which we will denote by $||S_{\mathrm{L}}[f]||_{V^2}(x)$. For each x, we define $S_{\mathrm{L}}[f](x)$ to be the sequence of differences of lacunary partial sums of f at x, i.e. $S_{\mathrm{L}}[f](x) := \{S_{2^0}[f](x), S_{2^1}[f](x) - S_{2^0}[f](x), S_{2^2}[f](x) - S_{2^1}[f](x), \ldots\}$. As usual, we let $||S_{\mathrm{L}}[f]||_{V^2}(x)$ denote the 2-variation of this function.

Lemma 51. In the notation above we have that

$$||S_{\mathrm{L}}[f]||_{L^2(V^2)} \ll \left(\sum_{n=1}^{\infty} \ln(n+1)|a_n|^2 \right)^{1/2}.$$

Proof. We will need the inequality $|a|^2 \leq 2|a-b|^2 + 2|b|^2$ for any real numbers a, b. For each x, there exists some sequence $m_0(x), m_1(x), m_2(x), \ldots$ such that:

$$||S_{\mathrm{L}}[f]||^2_{V^2}(x) = |S_{2^{m_0(x)}}[f](x)|^2 + \sum_{i=1}^{\infty} \left| S_{2^{m_i(x)}}[f](x) - S_{2^{m_{i-1}(x)}}[f](x) \right|^2. \quad (4.9)$$

Setting $a := S_{2^{m_i(x)}}[f](x) - S_{2^{m_{i-1}(x)}}[f](x)$ and $b := f(x) - S_{2^{m_{i-1}(x)}}[f](x)$, we can apply the inequality above to obtain:

$$\left| S_{2^{m_i(x)}}[f](x) - S_{2^{m_{i-1}(x)}}[f](x) \right|^2$$

$$\leq 2 \left| S_{2^{m_i(x)}}[f](x) - f(x) \right|^2 + 2 \left| S_{2^{m_{i-1}(x)}}[f](x) - f(x) \right|^2$$

for each $i \geq 1$. Combining this with (4.9), we have:

$$\begin{aligned} ||S_{\mathrm{L}}[f]||^2_{V^2}(x) &\ll |S_{2^{m_0(x)}}[f](x)|^2 \\ &\quad + \sum_{i=1}^{\infty} |S_{2^{m_i(x)}}[f](x) - f(x)|^2 + \left|S_{2^{m_{i-1}(x)}}[f](x) - f(x)\right|^2 \\ &\ll |S_{2^{m_0(x)}}[f](x)|^2 + \sum_{i=0}^{\infty} |S_{2^{m_i(x)}}[f](x) - f(x)|^2 \\ &\ll |S_{2^{m_0(x)}}[f](x)|^2 + \sum_{m=0}^{\infty} |S_{2^m}[f](x) - f(x)|^2 . \end{aligned}$$

Note that in this last quantity, we are always summing over all values of m, instead of summing over a subsequence dependent on x.

This gives us

$$||S_{\mathrm{L}}[f]||_{V^2}(x) \ll \left(|S_{2^{m_0(x)}}[f](x)|^2 + \sum_{m=0}^{\infty} |S_{2^m}[f](x) - f(x)|^2 \right)^{\frac{1}{2}} .$$

Now we take the L^2 norm of both sides of this inequality to obtain:

$$||S_{\mathrm{L}}[f]||_{L^2(V^2)} \ll \left(\sum_{n=1}^{\infty} \ln(n+1) a_n^2 \right)^{\frac{1}{2}} .$$

To see this, note that $|S_{2^m}[f](x) - f(x)| = \left|\sum_{n=2^m+1}^{\infty} a_n \phi_n(x)\right|$ and each n is greater than 2^m for $\ll \ln(n)$ values of m. The result then follows from Parseval's identity.

□

We now combine these two results to prove the following theorem.

Theorem 52. For an arbitrary ONS, in the notation above, we have

$$||S[f]||_{L^2(V^2)} \ll \left(\sum_{n=1}^{\infty} \ln^2(n+1) a_n^2 \right)^{\frac{1}{2}} .$$

Proof. We write $U_k(x) := \sum_{n=2^{k-1}+1}^{2^k} a_n \phi_n(x)$ (when $k = 0$, $U_0(x) := a_1\phi_1(x)$.). We claim that

$$||S[f]||^2_{L^2(V^2)} \ll \int_{\mathbb{T}} \left(||S_{\mathrm{L}}[f]||^2_{V^2}(x) + \sum_{k=0}^{\infty} ||U_k||^2_{V^2}(x) \right) dx.$$

To see this, note that any interval $[a, b]$ can be decomposed as the disjoint union of at most three intervals I_l, I_c, I_r, where $I_c = (2^k, 2^{k'}]$ and $I_l \subseteq (2^{k-1}, 2^k]$ and $I_r \subseteq (2^{k'}, 2^{k'+1})$ (here, 2^k can be set as the smallest integral power of 2 contained in $[a, b]$, and $2^{k'}$ can be set as the largest integral power of 2 contained in $[a, b]$). Now, $\int_{\mathbb{T}} ||S_{\mathrm{L}}[f]||^2_{V^2}(x)dx \ll \sum_{n=1}^{\infty} \ln(n+1)|a_n|^2$ from the previous lemma, which is clearly bounded by $\sum_{n=1}^{\infty} \ln^2(n+1)a_n^2$. By Lemma 50, we have

$$\int_{\mathbb{T}} ||U_k||^2_{V^2}(x)dx \ll \ln^2(2^k + 1) \sum_{n=2^{k-1}+1}^{2^k} a_n^2 \ll \sum_{n=2^{k-1}+1}^{2^k} \ln^2(n+1)a_n^2.$$

Combining these estimates completes the proof. □

Next we show that these estimates can be improved if one has additional information regarding the ONS. In particular, if the partial sum maximal operator $\mathcal{M}$ associated to the system is bounded then one can replace the $\ln^2(n)$ above with an $\ln(n)$.

Theorem 53. Let $f(x) = \sum_{n=1}^{N} a_n \phi_n(x)$ and assume that $||\mathcal{M}f||_{L^2} \ll \Delta(N) \left(\sum_{n=1}^{N} a_n^2 \right)^{1/2}$ for any choice of f. Then

$$||f||_{L^2(V^2)} \ll \Delta(N)\sqrt{\ln(N)} \left(\sum_{n=1}^{N} a_n^2 \right)^{1/2}$$

and

$$||f||_{L^2(V^2)} \ll \left(\sum_{n=1}^{N} \Delta(n) \ln(n+1) a_n^2 \right)^{1/2}.$$

In particular, if the quantity on the right is finite, then the variational operator applied to f must be finite almost everywhere.

Proof. As before, without loss of generality, we may assume that $N = 2^\ell$ for some positive integer ℓ. And we consider the collection of dyadic subintervals of $[1, N]$ of the form $I_{k,i} = (k2^i, (k+1)2^i]$ for each $0 \leq i \leq \ell$, $0 \leq k \leq 2^{\ell-i} - 1$. We will refer to intervals of this form as admissible intervals.

Now we note that an arbitrary interval $J = [a, b] \subseteq [N]$ can be written as a disjoint union $J = J_l \cup J_r$, where $J_r \subseteq I_{k_r,i_r}$ and $J_l \subseteq I_{k_l,i_l}$ and $|J_l| \geq \frac{1}{2}|I_{k_l,i_l}|$ and $|J_r| \geq \frac{1}{2}|I_{k_r,i_r}|$. We allow one of the intervals to be empty if needed, although in the following we will always assume that the intervals are not empty, since estimating the contribution from an empty interval is trivial. That is, we can write an arbitrary interval J as the union of two intervals which are contained within admissible intervals and the intersection with the admissible intervals is a constant fraction of the the admissible interval.

For $J \subseteq [N]$, let $S_J := \sum_{n \in J} a_n \phi_n(x)$. We now claim the pointwise inequality

$$||f||_{V^2}^2(x) \ll \sum_{0 \leq i \leq \ell} \sum_{0 \leq k \leq 2^{\ell-i}-1} |\mathcal{M} S_{I_{k,i}}(x)|^2.$$

Note that the sum on the right is only over all admissible intervals. To see that this inequality holds, let $\{J_i\}_{i=1}^m$ be a partition of $[N]$ that maximizes

the square variation (at x). From the discussion above, we can associate disjoint J_i^l and J_i^r to J_i such that $J_i \subset J_i^l \cup J_i^r$. Moreover, we can find disjoint admissible intervals I_i^l and I_i^r such that $J_i^s \subseteq I_i^s$ and $|J_i^s| \geq \frac{1}{2}|I_i^s|$ $(s \in \{r, l\})$.

We observe that $|S_{J_i}(x)|^2 \ll |\mathcal{M}S_{I_i^l}(x)|^2 + |\mathcal{M}S_{I_i^r}(x)|^2$. Moreover, any particular admissible interval I will be associated to at most two intervals in the partition $\{J_i\}$ since the intervals in the partition are disjoint and have at least half the length of the associated admissible interval. The pointwise inequality above now follows. Now integrating each side, applying the hypothesized inequality $||\mathcal{M}S_J||_{L^2}^2 \ll \Delta^2(N) \sum_{n \in J} a_n^2$, and noting that every point in $[N]$ is in $O(\ln(N))$ admissible intervals, we have that

$$\int_{\mathbb{T}} ||f||_{V^2}^2 dx \ll \sum_{0 \leq i \leq \ell} \sum_{0 \leq k \leq 2^{\ell - i} - 1} \int_{\mathbb{T}} |\mathcal{M}S_{I_{k,i}}(x)|^2 dx$$

$$\ll \Delta^2(N) \ln(N) \sum_{n=1}^{N} a_n^2.$$

Taking the square root of each side completes the the proof of the first inequality in the theorem statement. The second statement follows from the first via the argument used to prove Theorem 52. Note that we obtained a bound on the lacunary partial sums in Lemma 51 of the order $\sqrt{\ln(n)}$. This estimate was better than we needed for the proof of Theorem 52, however is exactly the order we need here. □

This completes the proof of Theorem 40 and Corollary 41 follows.

4.4 Lower bounds

In this section, we prove:

Theorem 42. Let $\{\phi_n(x)\}$ be a complete ONS. Then there exists a function $f \in L^\infty(\mathbb{T})$ such that for almost every $x \in \mathbb{T}$

$$||f||_{V^2}(x) = \infty. \tag{4.10}$$

Here, as before,

$||f||_{V^2}(x) = \sup_K \sup_{n_0<\ldots<n_K} \left(\sum_{l=1}^K |S_{n_l}[f](x) - S_{n_{l-1}}[f](x)|^2\right)^{1/2}$ where $S_{n_l}[f](x) = \sum_{n=1}^{n_l} a_n \phi_n(x)$ is the n_l-th partial sum.

Using Lemma 54 below and properties of the Dirichlet kernel, Jones and Wang showed (4.10) for the trigonometric system. In the case of general orthonormal systems, we do not have analytic information regarding the partial summation operator and need to proceed differently. We start by establishing the result for the Haar system.

We let $E_k : L^1 \to L^1$ denote the conditional expectation operator defined as follows. For $x \in [l2^{-k}, (l+1)2^{-k})$, $0 \leq l < 2^k$, $l \in \mathbb{N}$ we define

$$E_k f(x) = \int_{l2^{-k}}^{(l+1)2^{-k}} f(x)dx.$$

Using a probabilistic result of Qian [58], Jones and Wang [32] showed that:

Lemma 54. (Proposition 8.1 of [32]) There exists $f \in L^\infty(\mathbb{T})$ such that

$$\sup_K \sup_{n_0<\ldots<n_K} \left(\sum_{\ell=1}^K |E_{n_\ell} f(x) - E_{n_{\ell-1}} f(x)|^2\right)^{1/2} = \infty$$

almost everywhere.

If we let $S_n[f]$ denote the partial summation operator with respect to the Haar system, then it easily follows that $E_k f(x) = S_{n_{k+1}}[f](x) - S_{n_k}[f](x)$ for some sequence $\{n_k\}$. Therefore, there exists $f \in L^\infty(\mathbb{T})$ such that $||f||_{V^2}(x) = \infty$ for almost every $x \in \mathbb{T}$, where the operator V^2 is associated to the Haar system. For future use, let us define $\{b_n\}$ to be the Haar coefficients of the function f, that is

$$b_n = \langle f(x), \mathcal{H}_n(x) \rangle \,. \tag{4.11}$$

We will also need a theorem of Olevskii (see [54] Chapter 3), which requires that we introduce some additional notation. Let $\{g_n\}$ and $\{f_n\}$ be two sequences of real-valued measurable functions on $\mathbb{T}$. We say that they are weakly isomorphic if for each $n \in \mathbb{N}$ there exists an invertible measure-preserving mapping $T_n : \mathbb{T} \to \mathbb{T}$ that is one-to-one on a set of full measure and satisfies

$$f_k(T_n x) = g_k(x)$$

for all $1 \leq k \leq n$.

Theorem 55. (Olevskii) Let $\{\phi_n\}_{n=1}^\infty$ be a complete real-valued orthonormal system. There exists an orthonormal system $\{H_k\}_{k=1}^\infty$ that is weakly isomorphic to the Haar system, and a sequence $\{n_k\}_{k=1}^\infty$ such that

$$\left|\left| \sum_{i=n_k+1}^{n_{k+1}} \langle H_j, \phi_i \rangle \, \phi_i(x) \right|\right|_{L^2} \leq 2^{-k-j}$$

whenever $j \neq k$.

We now set $\tilde{f}(x) := \sum_{n=1}^{\infty} b_n H_n(x)$, for b_n defined in (4.11). Using the fact that the (finite) partial sums of the series defining $\tilde{f}(x)$ are weakly isomorphic to the partial sums of the Haar expansion of f, it follows that the partial sums of the function $\tilde{f}$ are uniformly bounded, hence $\tilde{f} \in L^{\infty}(\mathbb{T})$.

Lemma 56. For $\tilde{f}$ defined as above, we set $c_n := \left\langle \tilde{f}, \phi_n \right\rangle$. It follows that

$$\sum_{n=n_k+1}^{n_{k+1}} c_n \phi_n(x) = b_k H_k(x) + e_k(x),$$

where $\sum_k |e_k(x)| < \infty$ for almost every x.

Proof. Since $\tilde{f}(x) = \sum_{j=1}^{\infty} b_j H_j(x)$, we have

$$\sum_{n_k+1}^{n_{k+1}} c_n \phi_n(x) = \sum_{n=n_k+1}^{n_{k+1}} \left\langle \sum_{j=1}^{\infty} b_j H_j(x), \phi_n(x) \right\rangle \phi_n(x)$$

$$= \sum_{n=n_k+1}^{n_{k+1}} b_k \left\langle H_k(x), \phi_n(x) \right\rangle \phi_n(x) + \sum_{n=n_k+1}^{n_{k+1}} \left\langle \sum_{j \neq k} b_j H_j(x), \phi_n(x) \right\rangle \phi_n(x).$$

By applying the triangle inequality, we obtain:

$$\left|\left| b_k H_k(x) - \sum_{n_k+1}^{n_{k+1}} c_n \phi_n(x) \right|\right|_{L^2} \leq |b_k| \left|\left| \sum_{n \notin [n_k+1, n_{k+1}]} \left\langle H_k(x), \phi_n(x) \right\rangle \phi_n(x) \right|\right|_{L^2}$$

$$+ \sum_{j \neq k} |b_j| \left|\left| \sum_{n=n_k+1}^{n_{k+1}} \left\langle H_j(x), \phi_n(x) \right\rangle \phi_n(x) \right|\right|_{L^2}.$$

Now applying Theorem 55, we have that

$$\left|\left| b_k H_k(x) - \sum_{n_k+1}^{n_{k+1}} c_n \phi_n(x) \right|\right|_{L^2} \ll 2^{-k} \left(|b_k| \sum_{j \neq k} 2^{-j} + \sum_{j \neq k} |b_j| 2^{-j} \right) \ll 2^{-k} ||\tilde{f}||_{L^2}.$$

The last bound follows from the fact that $|b_j| \leq ||\tilde{f}||_{L^2} = (\sum_{i=1}^{\infty} b_i^2)^{1/2}$ for all j.

Denoting the expression on the inside of the norm on the left as $e_k(x)$, we see that $\left|\left| \sum_{k=1}^{\infty} |e_k| \right|\right|_{L^2} \ll ||\tilde{f}||_{L^2}$ and hence $\sum_{k=1}^{\infty} |e_k(x)|$ is finite for almost every $x \in \mathbb{T}$.

□

We now prove Theorem 42. We let V_ϕ and V_H denote the variation operators associated to the systems $\{\phi_n\}$ and $\{H_n\}$ respectively. Moreover, we let V^2 be the variation operator associated to the partial sums of the absolutely convergent function $E(x) = \sum_{k=1}^{\infty} e_k(x)$. We have, for almost every $x \in \mathbb{T}$,

$$||E||_{V^2}(x) \leq \sum_{k=1}^{\infty} |e_k(x)| < \infty.$$

It follows that

$$||\tilde{f}||_{L^2(V_H^2)} = \left|\left| \sum_{k=1}^{\infty} b_k H_k \right|\right|_{L^2(V_H^2)} \leq ||\tilde{f}||_{L^2(V_\phi^2)} - ||E||_{L^2(V^2)}.$$

Since the first quantity in this expression is infinite almost everywhere, and the third quantity is finite almost everywhere, it must hold that $||\tilde{f}||_{L^2(V_\phi^2)}$ is infinite almost everywhere. This completes the proof of the theorem.

Our proof of Theorem 42 was purely qualitative, a feature we inherit from Theorem 55, which relies on the Riemann-Lebesgue lemma. Next we show that it is impossible to obtain a quantitative lower bound on the growth of the variation in Theorem 42.

Remark 57. One could obtain the conclusion of Theorem 42 for functions in more restrictive classes. Combining the above argument with known perturbation techniques, one can show that the f in the statement of the theorem can be taken to be continuous. The proof of this relies on the fact that one already has an example in L^∞ (an example in L^2 is not sufficient). See [54] p.67 and the associated references for details. Additionally, one can show that for any nonconstant function f, there exists an invertible measure preserving transformation of $T : \mathbb{T} \to \mathbb{T}$ such that the conclusion holds for $g(x) = f(T(x))$. See [54] p.69 and the related references for details. From this, we see that one cannot hope to prove that V^2 is bounded on L^2 even in "restricted weak type" form, at least not for complete systems. Since the details of these arguments are not essential to our current investigation, and are essentially a combination of the above argument and the ideas of the cited papers, we omit them.

Theorem 58. Let $w(\cdot)$ denote a positive real-valued function monotonically increasing to infinity. Then there exists a complete orthonormal system $\{\phi_n\}_{n=1}^\infty$ such that for all sufficiently large $N \in \mathbb{N}$,

$$||f||_{L^2(V^2)} \ll w(N) \left(\sum_{n=1}^{N} |a_n|^2 \right)^{\frac{1}{2}}.$$

for all f of the form $f(x) = \sum_{n=1}^{N} a_n \phi_n(x)$.

Proof. Our example will be a rearrangement of the Haar system. We let $\Psi = \{\psi_n(x)\}_{n=1}^\infty$ be a subsequence of the Haar system with disjoint supports. We let $\{\rho_n(x)\}_{n=1}^\infty$ denote the subsequence of the Haar system consisting of

all the elements of the Haar system that are not included in Ψ. We now form a complete orthonormal system $\{\phi_n\}$ by sparsely inserting elements of the sequence $\{\rho_n(x)\}_{n=1}^{\infty}$ into the sequence $\{\psi_n(x)\}_{n=1}^{\infty}$, maintaining the relative ordering of each sequence. Clearly we may do this so that the first N elements of the system $\{\phi_n\}$ have at most $w(n)$ elements from the ρ's. We thus may partition the indices $[N]$ of the system $\{\phi_n\}_{n=1}^{N}$ into two classes. We let S be the subset of indices n for which $\phi_n = \rho_m$ for some m and $S^c := [N] \setminus S$. We note that for $n \in S^c$, ϕ_n is an element of the subsequence Ψ, and so all of these have disjoint supports.

We then have:

$$\left|\left|\sum_{n\in S} a_n\phi_n + \sum_{n\in S^c} a_n\phi_n\right|\right|_{L^2(V^2)} \leq \left|\left|\sum_{n\in S} a_n\phi_n\right|\right|_{L^2(V^2)} + \left|\left|\sum_{m\in S^c} a_m\phi_m\right|\right|_{L^2(V^2)}$$
$$\ll \ln(w(n))||f||_{L^2} + ||f||_{L^2} \ll \ln(w(n))||f||_{L^2} \ll w(n)||f||_{L^2}.$$

Here, we have employed the triangle inequality, Lemma 50, and the fact that $\{\phi_n\}_{n\in S^c}$ have disjoint supports.

□

Lastly, we show that if a system is uniformly bounded, then an quantitative lower bound on the growth of the V^2 operator is available, even without assuming completeness.

Theorem 43. Let $\{\phi_n\}_{n=1}^{N}$ be an ONS uniformly bounded by M. Then there exists a function of the form $f = \sum_{n=1}^{N} a_n\phi_n(x)$ such that

$$||S[f]||_{L^2(V^2)} \gg_M \sqrt{\ln\ln(N)}||f||_{L^2}$$

In light of Theorem 46, this is best possible.

To prove this, we will rely on the following lemma:

Lemma 59. We let $c_1, \ldots, c_N$ denote real numbers, all $\geq \delta$ for some constant $\delta > 0$. We let $X_1, \ldots, X_N$ denote independent Gaussian random variables, each with mean 0 and variance 1. Then

$$\mathbb{E}\left[\left|\left|\sum_{n=1}^{N} c_n X_n\right|\right|_{V^2}\right] \gg \delta\sqrt{N \ln\ln(N)}.$$

Proof. We essentially follow the proof of Theorem 2.1 in [58] (pp. 1373-1375), with minor modifications. We let $\Phi(x)$ denote the standard normal distribution function. By Lemma 2.1 of [58] (p. 1373), we have that

$$1 - \Phi(x) \geq (1/12)exp(-3x^2/4) \text{ for } x \geq 1. \tag{4.12}$$

We define $S_k = \sum_{n=1}^{k} c_n X_n$ and we set $K := 25$. We also set

$$\ell := \ell(N) := \left\lfloor \frac{\ln N}{4 \ln K} \right\rfloor \text{ and } m := m(N) := \left\lfloor \frac{\ln N}{2 \ln K} \right\rfloor.$$

We let $Lx := \max\{1, \ln x\}$.

For each $\omega \in \Omega$ (where Ω denotes the probability space), we define $E_N(\omega)$ to be the subset of values $t \in \{1, 2, \ldots, N - \sqrt{N}\}$ such that, for some $\ell \leq j \leq m$, $|S_{t+K^j}(\omega) - S_t(\omega)| \geq \delta\sqrt{K^j LL(N)}/2$. Additionally, for each fixed t and j, we define the event

$$E_N^j(t) := \left\{\omega : |S_{t+K^j}(\omega) - S_{t+K^{j-1}}(\omega)| \geq \delta\sqrt{K^j LL(N)}\right\}.$$

Now, $S_{t+K^j} - S_{t+K^{j-1}}$ is distributed as a Gaussian random variable with mean 0 and variance equal to

$$\sigma^2 := Var[S_{t+K^j} - S_{t+K^{j-1}}] = \sum_{n=t+K^{j-1}+1}^{t+K^j} c_n^2.$$

For any $\lambda \in \mathbb{R}$,

$$\mathbb{P}\left[S_{t+K^j}(\omega) - S_{t+K^{j-1}} \geq \lambda\right] = 1 - \Phi\left(\frac{\lambda}{\sigma}\right).$$

We apply this with $\lambda := \delta\sqrt{K^j LL(N)}$, and since each $c_n \geq \delta$, we have:

$$\frac{\lambda}{\sigma} \leq \sqrt{\frac{K^j LL(N)}{K^j - K^{j-1}}}.$$

Therefore, using (4.12), we obtain:

$$\mathbb{P}[E_N^j(t)] = 1 - \Phi\left(\frac{\lambda}{\sigma}\right) \geq 1 - \Phi\left(\sqrt{\frac{K^j LL(N)}{K^j - K^{j-1}}}\right)$$

$$\geq \frac{1}{12} exp\left(-\frac{3}{4}\frac{K^j}{K^j - K^{j-1}} LL(N)\right).$$

This is $\geq \frac{1}{12} exp\left(-\frac{4}{5} LL(N)\right) = \frac{1}{12}(\ln(N))^{-4/5}$.

We observe that if $|S_{t+K^j}(\omega) - S_{t+K^{j-1}}(\omega)| \geq \delta\sqrt{K^j LL(N)}$ for some $\ell < j \leq m$, then either $|S_{t+K^j}(\omega) - S_t(\omega)| \geq \delta\sqrt{K^j LL(N)}/2$ or $|S_{t+K^{j-1}} - S_t| \geq \delta\sqrt{K^j LL(N)}/2 \geq \delta\sqrt{K^{j-1} LL(N)}/2$. Thus,

$$\omega \in \bigcup_{j=\ell+1}^{m} E_N^j(t) \Rightarrow t \in E_N(\omega).$$

Therefore, for any $t \in \{1, 2, \ldots, N - \lfloor\sqrt{N}\rfloor\}$, we have:

$$\mathbb{P}\left[\omega : t \in E_N(\omega)\right] \geq \mathbb{P}\left[\bigcup_{j=\ell+1}^{m} E_N^j(t)\right].$$

We note that for $j' \neq j$, $E_N^j(t)$ and $E_N^{j'}(t)$ depend on disjoint sets of the random variables X_i, and so are independent events. Therefore, letting $\overline{E}_N^j(t)$ denote the complement of $E_N^j(t)$, we have

$$\mathbb{P}\left[\bigcup_{j=\ell+1}^{m} E_N^j(t)\right] = 1 - \mathbb{P}\left[\bigcap_{j=\ell+1}^{m} \overline{E}_N^j(t)\right] = 1 - \prod_{j=\ell+1}^{m} \mathbb{P}[\overline{E}_N^j(t)].$$

By the above computations, this is

$$\geq 1 - exp\left(-(1/12)(m-\ell)(\ln N)^{-4/5}\right).$$

For sufficiently large N, we can bound this by:

$$> 1 - exp\left(-(\ln N)^{1/5}/(52 \ln K)\right) := 1 - p_N.$$

This shows that for each t, $\mathbb{P}\left[\omega : t \in E_N(\omega)\right] > 1 - p_N$. We can alternately express this as:

$$\int_\Omega 1_{E_N}(t) d\mathbb{P} > 1 - p_N,$$

where $1_{E_N}(t)$ denotes the function that is equal to 1 when $t \in E_N(\omega)$ and equal to 0 otherwise. We define the subset $\mathcal{S} \subseteq \Omega$ to be the set of $\omega \in \Omega$ such that $|E_N(\omega)| > (1 - \sqrt{p_N})(N - \sqrt{N})$. Then

$$\mathbb{P}[\mathcal{S}] > 1 - \sqrt{p_N}. \tag{4.13}$$

To see this, observe that

$$\int_\Omega \sum_{t=1}^{N-\sqrt{N}} 1_{E_N}(t) d\mathbb{P} = \sum_{t=1}^{N-\sqrt{N}} \int_\Omega 1_{E_N}(t) d\mathbb{P} > (N - \sqrt{N})(1 - p_N).$$

Now, if $\mathbb{P}[\mathcal{S}] \leq 1 - \sqrt{p_N}$ held, this would imply that the integral on the left hand side of the above is also

$$\leq \sqrt{p_N}\,(1-\sqrt{p_N})\left(N-\sqrt{N}\right)+(1-\sqrt{p_N})\left(N-\sqrt{N}\right) = \left(N-\sqrt{N}\right)(1-p_N)\,,$$

which is a contradiction.

We next use the following Vitali covering lemma:

Lemma 60. ([18], Lemma 3.15) Let $\mu(A)$ denote the Lebesgue measure of a set $A \subseteq \mathbb{R}$. Let $\mathcal{U}$ be a collection of open intervals in $\mathbb{R}$ with bounded union W. Then for any $\lambda < \mu(W)$, there is a finite, disjoint subcollection $\{V_1, V_2, \ldots, V_q\} \subseteq \mathcal{U}$ such that $\sum_{i=1}^{q} \mu(V_i) \geq \lambda/3$.

For sufficiently large N, (4.13) implies that with probability $> 1-\sqrt{p_N}$, for $\geq N' := \lfloor (1-\sqrt{p_N})(N-\sqrt{N}-1) \rfloor$ integers $t \in \{1, 2, \ldots, N-\sqrt{N}\}$ (we will call them $t_1, t_2, \ldots, t_{N'}$), we have corresponding values $j_1, \ldots, j_{N'}$ (all $\leq m$) such that $|S_{t_i+K^{j_i}} - S_{t_i}| \geq \delta\sqrt{K^{j_i} LL(N)}/2$ for each i from 1 to N'. We consider the collection $\mathcal{U}$ of the open intervals $(t_i, t_i + K^{j_i})$ for i from 1 to N'. We note that each $K^{j_i} > 1$. We fix some positive constant $\alpha < 1$. For N sufficiently large, we have $N' > \alpha N$. (Note that p_N approaches 0 as N goes to infinity). Therefore, the union of the intervals in $\mathcal{U}$ is a subset of $(0, N]$ with Lebesgue measure $\geq N' > \alpha N$.

Applying Lemma 60, we conclude that there is disjoint subcollection of these open intervals, denoted by $\{(t_i, t_i + K^{j_i})\}_{i \in Q}$, where $Q \subseteq [N']$, such that

$$\sum_{i \in Q} K^{j_i} \geq \alpha N/3.$$

The closures of the intervals in Q are non-overlapping except for possibly at their endpoints. Relabeling the t_i's for $i \in Q$ as $t_1, \ldots, t_q$ (where $q = |Q|$), we have $t_1 < t_1 + K^{j_1} \leq t_2 < t_2 + K^{j_2} \leq \cdots \leq t_q < t_q + K^{j_q} \leq N$. Then,

$$\sum_{i=1}^{q} \left(S_{t_i+K^{j_i}} - S_{t_i}\right)^2 \geq (1/4)\delta^2 \sum_{i=1}^{q} K^{j_i} LL(N) \geq (\alpha/12)\delta^2 N LL(N).$$

This implies that

$$\mathbb{P}\left[\left|\left|\sum_{n=1}^{n} c_n X_n\right|\right|_{V^2} \geq \delta\sqrt{(\alpha/12)N \ln\ln N}\right] > 1 - \sqrt{p_N},$$

for all sufficiently large N. Hence, by Markov's inequality,

$$\mathbb{E}\left[\left|\left|\sum_{n=1}^{N} c_n X_n\right|\right|_{V^2}\right] \geq \delta\sqrt{(\alpha/12)N \ln\ln N}(1 - \sqrt{p_N}) \gg \delta\sqrt{N \ln\ln N}.$$

□

We now prove Theorem 43. We begin by noting that for each n, $\int_{\mathbb{T}} \phi_n^2(x)dx = 1$ and $|\phi_n(x)| \leq M \ \forall x$ implies that there are positive constants $\epsilon, \delta > 0$ (depending on M) such that for some sets $U_n \subseteq \mathbb{T}$ each of measure $\geq \epsilon$, $|\phi_n(x)| \geq \delta$ for all $x \in U_n$. For each n, we let χ_n denote the characteristic function of the set U_n. We then have:

$$\int_{\mathbb{T}} \sum_{n=1}^{N} \chi_n(x)dx = \sum_{n=1}^{N} \int_T \chi_n(x)dx \geq N\epsilon. \tag{4.14}$$

We define $\epsilon' := \frac{\epsilon}{2}$. Then the function $\sum_{n=1}^{N} \chi_n(x)$ must be $\geq \epsilon' N$ on a set of measure $\geq \epsilon'$. To see this, note that $0 \leq \sum_{n=1}^{N} \chi_n(x) \leq N$ for all N. If this function is less than $\epsilon' N$ on a set of measure $> 1 - \epsilon'$, this would imply

$$\int_T \sum_{n=1}^{N} \chi_n(x)dx < \epsilon' N(1 - \epsilon') + \epsilon' N = (1 - \epsilon/4)N\epsilon,$$

contradicting (4.14). Thus, there is some set U of measure $\geq \epsilon'$ such that for every $x \in U$, $|\phi_n(x)| \geq \delta$ for at least $\epsilon' N$ values of n.

We let $X_1, \ldots, X_N$ denote independent Gaussian random variables with mean 0 and variance 1. We consider the quantity

$$\mathbb{E}\left[\left|\left|\{X_n \phi_n(x)\}_{n=1}^N\right|\right|_{L^2(V^2)}^2\right].$$

This can be written as:

$$\mathbb{E}\left[\int_{\mathbb{T}} \left|\left|\{X_n \phi_n(x)\}_{n=1}^N\right|\right|_{V^2}^2 dx\right] = \int_\Omega \int_{\mathbb{T}} \left|\left|\{X_n \phi_n(x)\}_{n=1}^N\right|\right|_{V^2}^2 dx d\mathbb{P}.$$

By Fubini's theorem, we may exchange the integrals to obtain

$$= \int_T \int_\Omega \left|\left|\{X_n \phi_n(x)\}_{n=1}^N\right|\right|_{V^2}^2 d\mathbb{P} dx.$$

Since the inner integral is a non-negative quantity, this is

$$\geq \int_U \mathbb{E}\left[\left|\left|\{X_n \phi_n(x)\}_{n=1}^N\right|\right|_{V^2}^2\right] dx.$$

We consider a fixed $x \in U$. By definition of U, we have $|\phi_n(x)| \geq \delta$ for at least $\epsilon' N$ values of n. We now define new independent Gaussian random variables $Y_1, \ldots, Y_{\widetilde{N}}$ for $\widetilde{N} \geq \epsilon' N$ as follows. We start from $n = 1$, and we define Y_1 to be the first partial sum $\sum_{n=1}^{n_1} \phi_n(x) X_n$ such that $\sum_{n=1}^{n_1} |\phi_n(x)| \geq \delta$. We then similarly define Y_2 to be $\sum_{n=n_1+1}^{n_2} \phi_n(x) X_n$ for the smallest n_2 such that $\sum_{n=n_1+1}^{n_2} |\phi_n(x)| \geq \delta$. We continue this process, defining the Y_i's to be disjoint sums of the $\phi_n(x) X_n$'s. Since $x \in U$, we will have $Y_1, \ldots, Y_{\widetilde{N}}$ for $\widetilde{N} \geq \epsilon' N$. Since the sum of independent Gaussians is distributed as a Gaussian

(with variance equal to the sum of the variances), each Y_i is distributed as an independent, mean zero Gaussian with variance $\geq \delta^2$. Thus, applying Lemma 59, we have for each $x \in U$:

$$\mathbb{E}\left[\left|\left|\{X_n\phi_n(x)\}_{n=1}^N\right|\right|_{V^2}^2\right] \geq \mathbb{E}\left[\left|\left|\{Y_i\}_{i=1}^{\widetilde{N}}\right|\right|_{V^2}^2\right] \geq \delta^2\widetilde{N}\ln\ln(\widetilde{N}) \gg \delta^2 N\ln\ln(N).$$

Therefore, we have

$$\mathbb{E}\left[\left|\left|\{X_n\phi_n(x)\}_{n=1}^N\right|\right|_{L^2(V^2)}^2\right] \gg \int_U \delta^2 N\ln\ln(N)dx \gg N\ln\ln N. \tag{4.15}$$

We note that the constants being subsumed by the $\gg$ notation above depend on M.

Now, we consider the contribution to this expectation from points ω in the probability space Ω such that $\sum_{n=1}^N X_n(\omega)^2$ is much larger than N. We will show this contribution is small. To do this, we will upper bound the quantity $\mathbb{P}\left[\sum_{n=1}^N X_n^2 \geq kN\right]$ for each positive integer $k \geq 2$. We rely on the following version of the Berry-Esseen theorem.

Lemma 61. ([55], p. 132) Let $Z_1, \ldots, Z_N$ be independent, mean zero random variables with $\mathbb{E}[|Z_n|^{2+\gamma}] < \infty$ for all n for some $0 < \gamma \leq 1$. Let $\sigma_n^2 := \mathbb{E}[Z_n^2]$ and $B_N := \sum_{n=1}^N \sigma_n^2$. Then, for all $x \in \mathbb{R}$:

$$\left|\mathbb{P}\left[B_N^{-\frac{1}{2}}\sum_{n=1}^N Z_n < x\right] - \Phi(x)\right| \leq \frac{A}{B_N^{1+\gamma/2}(1+|x|)^{2+\gamma}}\sum_{n=1}^N \mathbb{E}[|Z_n|^{2+\gamma}],$$

where A is a constant and $\Phi(x)$ denotes the standard normal distribution function.

Now, letting $X_1, \ldots, X_N$ denote the independent, mean zero, variance one Gaussians as above, we define $Z_1, \ldots, Z_N$ by $Z_n := X_n^2 - 1$. Then the Z_n's are independent, mean zero random variables. We note that $\mathbb{E}[Z_n^2] = \mathbb{E}[X_n^4] - 1 = 2$ for each n. Also,

$$\mathbb{E}[|Z_n|^3] = \mathbb{E}[|X_n^6 - 3X_n^4 + 3X_n^2 - 1|] \leq \mathbb{E}[X_n^6] + 3\mathbb{E}[X_n^4] + 3\mathbb{E}[X_n^2] + 1 = 28.$$

We will apply Lemma 61 for $Z_1, \ldots, Z_N$, with $\gamma := 1$ and $B_N = 2N$ (since $\sigma_n^2 = 2$ for each n). We observe:

$$\mathbb{P}\left[\sum_{n=1}^N X_n^2 \geq kN\right] = \mathbb{P}\left[\sum_{n=1}^N Z_n \geq (k-1)N\right]$$

$$= \mathbb{P}\left[B_N^{-\frac{1}{2}} \sum_{n=1}^N Z_n \geq 2^{-\frac{1}{2}}(k-1)N^{\frac{1}{2}}\right]$$

$$= 1 - \mathbb{P}\left[B_N^{-\frac{1}{2}} \sum_{n=1}^N Z_n < x\right] \leq 1 - \Phi(x) + \frac{A}{B_N^{3/2}(1+|x|)^3} \sum_{n=1}^N \mathbb{E}\left[|Z_n|^3\right],$$

where $x := 2^{-1/2}(k-1)N^{1/2}$.

Since $\mathbb{E}\left[|Z_n|^3\right]$ is a constant, this is

$$\ll \int_x^\infty e^{-\frac{y^2}{2}} dy + \frac{1}{N^{1/2}(1+|x|)^3}.$$

Using that $x = 2^{-1/2}(k-1)N^{1/2}$, we have

$$\frac{1}{N^{1/2}(1+|x|)^3} \ll \frac{1}{N^2(k-1)^3}. \tag{4.16}$$

Since $x \geq 1$ (recall that $k \geq 2$), we have

$$\int_x^\infty e^{-\frac{y^2}{2}} dy \leq \int_x^\infty y e^{-\frac{y^2}{2}} dy = e^{-\frac{x^2}{2}} = e^{-\frac{1}{4}N(k-1)^2}. \tag{4.17}$$

Combining (4.16) and (4.17), we see that

$$\mathbb{P}\left[\sum_{n=1}^{N} X_n^2 \geq kN\right] \ll \frac{1}{N^2(k-1)^3} + e^{-\frac{1}{4}N(k-1)^3},$$

for each positive integer $k \geq 2$.

Now, by Lemma 50, for each $\omega \in \Omega$ such that $kN \leq \sum_{n=1}^{N} X_n^2(\omega) < (k+1)N$, we have that the quantity $\left|\left|\{X_n\phi_n(x)\}_{n=1}^{N}\right|\right|_{L^2(V^2)}^2$ evaluated at ω is $\ll (k+1)\ln^2(N)N$. Thus, the contribution to the expectation bounded in (4.15) coming from such points ω for all $k \geq 2$ is upper bounded as:

$$\ll \sum_{k=2}^{\infty}(k+1)\ln^2(N)N\left(e^{-\frac{1}{4}N(k-1)^2} + \frac{1}{N^2(k-1)^3}\right)$$

$$= \ln^2(N)Ne^{-\frac{1}{4}N}\sum_{k=2}^{\infty}(k+1)\left(e^{-\frac{1}{4}N}\right)^{k^2-2k} + \frac{\ln^2(N)}{N}\sum_{k=2}^{\infty}\frac{k+1}{(k-1)^3}.$$

Both of these sums are convergent, and it is easy to see that this quantity is $o(N\ln\ln N)$.

Therefore, by (4.15) and the above bounds, we have proven that there exists some point $\omega \in \Omega$ such that when we define $a_n := X_n(\omega)$ and define $f(x) = \sum_{n=1}^{N} a_n\phi_n(x)$, we have

$$||S[f]||_{L^2(V^2)} \gg_M \sqrt{\ln\ln(N)}||f||_{L^2}.$$

Here, we have used that we can choose ω so that $||S[f]||_{L^2(V^2)}^2 \gg_M N\ln\ln(N)$ and $||f||_{L^2}^2 = \sum_{n=1}^{N} a_n^2 \leq 2N$ simultaneously.

4.5 Systems of Bounded Independent Random Variables

In this section, we prove the following theorem:

Theorem 46. Let $\{X_i\}_{i=1}^N$ be a sequence of mean zero independent random variables such that $|X_i| \leq C$ and $\mathbb{E}\left[|X_i|^2\right] = 1$ for all $i \in [N]$. Then

$$\mathbb{E}\left[\left|\left|\{a_i X_i\}_{i=1}^N\right|\right|_{V^2}\right] \ll_C \sqrt{\ln\ln(N)} \left(\sum_{i=1}^N a_i^2\right)^{1/2}.$$

We will require the following lemmas. The first is a form of Hoeffding's inequality [26].

Lemma 62. Let $\{X_i\}$ be independent random variables such that $\mathbb{P}[X_i \in [a_i, b_i]] = 1$. Then

$$\mathbb{P}\left[|S_n - \mathbb{E}\left[S_n\right]| \geq t\right] \leq 2\exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right)$$

where $S_n = \sum_{i=1}^n X_i$.

Lemma 63. (Etemadi's Inequality). (See Theorem 1 in [17].) Let $X_1, X_2, \ldots, X_n$ denote independent random variables and let $a > 0$. Let $S_\ell := X_1 + \cdots + X_\ell$ denote the partial sum. Then

$$\mathbb{P}[\max_{1\leq \ell \leq n} |S_\ell| \geq 3a] \leq 3 \max_{1\leq \ell \leq n} \mathbb{P}[|S_\ell| \geq a].$$

Lemma 64. (Rosenthal's Inequality). (See Theorem 3 in [61].) Let $2 < p < \infty$. Then there exists a constant K_p depending only on p, so that if $X_1, \ldots, X_n$ are independent random variables with $\mathbb{E}[X_i] = 0$ for all i and $\mathbb{E}[|X_i|^p] < \infty$

for all i, then:

$$(\mathbb{E}[|S_n|^p])^{1/p} \leq K_p \max\left\{\left(\sum_{i=1}^n \mathbb{E}[|X_i|^p]\right)^{1/p}, \left(\sum_{i=1}^n \mathbb{E}[|X_i|^2]\right)^{1/2}\right\}.$$

We also use the following consequence of Doob's inequality. For an interval $I \subseteq [n]$, we define $S_I := \sum_{i \in I} X_i$. We also define

$$\tilde{S}_n := \max_{I \subseteq [n]} |S_I|.$$

We then have:

Lemma 65. For $p > 1$ and independent random variables $X_1, \ldots, X_n$ with $\mathbb{E}[X_i] = 0$ for all i,

$$\mathbb{E}\left[|\tilde{S}_n|^p\right] \leq 2^p \mathbb{E}\left[\max_{1 \leq \ell \leq n} \left|\sum_{i=1}^{\ell} X_i\right|^p\right] \leq 2^p \left(\frac{p}{p-1}\right)^p \mathbb{E}\left[|S_n|^p\right].$$

Proof. The first inequality is a consequence of the following observation. For a subinterval $I \subseteq [n]$, we let I_0 be the subinterval that starts at 1 and ends just before I, and we let I_1 be the interval $I_0 \cup I$. Then I_0 and I_1 are both intervals starting at 1, and $S_{I_0} + S_I = S_{I_1}$. Therefore, $\max\{|S_{I_0}|, |S_{I_1}|\} \geq \frac{1}{2}|S_I|$. The second inequality follows from Theorem 3.4 on p. 317 in [12]. □

We begin by decomposing $[N]$ into a family of subintervals according to a concept of mass defined with respect to the a_i values. We define the *mass* of a subinterval $I \subseteq [N]$ as $M(I) := \sum_{n \in I} a_n^2$. By normalization, we may assume that $M([N]) = 1$. We define $I_{0,1} := [N]$ and we iteratively define $I_{k,s}$, for $1 \leq s \leq 2^k$, as follows. Assuming we have already defined $I_{k-1,s}$ for all

$1 \leq s \leq 2^{k-1}$, we will define $I_{k,2s-1}$ and $I_{k,2s}$, which are subintervals of $I_{k-1,s}$. $I_{k,2s-1}$ begins at the left endpoint of $I_{k-1,s}$ and extends to the right as far as possible while covering strictly less than half the mass of $I_{k-1,s}$, while $I_{k,2s}$ ends at the right endpoint of $I_{k-1,s}$ and extends to the left as far as possible while covering at most half the mass of $I_{k-1,s}$. More formally, we define $I_{k,2s-1}$ as the maximal subinterval of $I_{k-1,s}$ which contains the left endpoint of $I_{k-1,s}$ and satisfies $M(I_{k,2s-1}) < \frac{1}{2}M(I_{k,s})$. We also define $I_{k,2s}$ as the maximal subinterval of $I_{k-1,s}$ which contains the right endpoint of $I_{k-1,s}$ and satisfies $M(I_{k,2s}) \leq \frac{1}{2}M(I_{k,s})$. We note that these subintervals are disjoint. We may express $I_{k-1,s} = I_{k,2s-1} \bigcup I_{k,2s} \bigcup i_{k,s}$, where $i_{k,s} \in I_{k-1,s}$. In other words, $i_{k,s}$ denotes the single element which lies between $I_{k,2s-1}$ and $I_{k,2s}$ (note that such a point always exists because we have required that $I_{k,2s-1}$ contains strictly less than half of the mass of the interval). Here it is acceptable, and in many instances necessary, for some choices of the intervals in this decomposition to be empty. By construction we have that

$$M(I_{k,s}) \leq 2^{-k}. \tag{4.18}$$

We call an interval $J \subseteq [N]$ admissible if it is an element of the decomposition given above. We denote the collection of admissible intervals by $\mathcal{A}$. We additionally refer to the subset $\{I_{k,s} | 1 \leq s \leq 2^k\}$ of $\mathcal{A}$ as the admissible intervals on level k and the subset $\{i_{k,s} | 1 \leq s \leq 2^k\}$ as the admissible points on level k. We note that every point in $[N]$ is an admissible point on some level. (Eventually, we have subdivided all intervals down to being single elements.)

We consider an arbitrary interval $J \subseteq [N]$. We would like to approximate J by an admissible interval $\tilde{J}$ such that $J \subseteq \tilde{J}$ and $M(\tilde{J}) \leq cM(J)$, for some constant c. This may be impossible, however, since J could span the boundary between adjacent admissible intervals for all comparable masses. To address this, we will instead approximate J by the union of two admissible intervals and one point.

Lemma 66. For every $J \subseteq [N]$, $(J \neq \emptyset)$ there exist $\tilde{J}_\ell, \tilde{J}_r \in \mathcal{A}$ and $i_J \in [N]$ such that $\tilde{J} := \tilde{J}_\ell \cup i_J \cup \tilde{J}_r$ is an interval (i.e. J_ℓ, i_J, J_ℓ are adjacent), $J \subseteq \tilde{J}$, and $M(\tilde{J}) \leq 2M(J)$.

Proof. We consider the minimal value k such that J contains an admissible point on level k. We note that this point is unique, and we define i_J to be equal to it. To see why a unique such point exists, first note that if J contained at least two admissible points on level k, then it would also contain an admissible point between them on level $k-1$. Now we consider the subinterval J_ℓ consisting of elements of J that lie to the left of i_j. Since the rightmost endpoint of this subinterval is at rightmost endpoint of an admissible interval on level k, it is also a rightmost endpoint of some admissible interval on every level $> k$. We define $\tilde{J}_\ell$ to be the admissible interval with this right endpoint on the highest level k_ℓ such that $J_\ell \subseteq \tilde{J}_\ell$. We note that the admissible interval with this right endpoint on level k contains J, so such an interval $\tilde{J}_\ell$ must exist, and $k_\ell \geq k$.

We claim that $M(\tilde{J}_\ell) \leq 2M(J_\ell)$. To prove this, we consider the admis-

sible interval $\tilde{J}'$ on level $k_\ell + 1$ with this same right endpoint. By maximality of k_ℓ, we must have that J isn't contained in $\tilde{J}'$. This implies that J must contain the admissible point on level $k_\ell+1$ that occurs when $\tilde{J}_\ell$ is decomposed. Therefore, $M(J_\ell) \geq \frac{1}{2}M(\tilde{J}_\ell)$.

We define the subinterval J_r consisting of elements of J that lie to the right of i_j, and we can similarly find an admissible $\tilde{J}_r$ such that $J_r \subseteq \tilde{J}_r$ and $M(\tilde{J}_r) \leq 2M(J_r)$. We then have $J \subseteq \tilde{J} := \tilde{J}_\ell \cup i_J \cup \tilde{J}_r$ and $M(\tilde{J}) \leq 2M(J)$ follows from:

$$M(\tilde{J}) = M(\tilde{J}_\ell) + M(i_J) + M(\tilde{J}_r) \leq 2(M(J_\ell) + M(i_J) + M(J_r)) = 2M(J).$$

□

Defining $\tilde{J}_\ell$, $\tilde{J}_r$, and i_J with respect to J as in the lemma, we observe that:

$$|S_J|^2 \ll |\tilde{S}_{\tilde{J}_\ell}|^2 + |\tilde{S}_{\tilde{J}_r}|^2 + |S_{i_J}|^2. \tag{4.19}$$

Here, $|\tilde{S}_{\tilde{J}}|$ is the maximal partial sum over all subintervals contained in $\tilde{J}$. Also, if $\mathcal{P}$ is a partition of $[N]$, then the admissible intervals and points ($\tilde{J}_\ell$, $\tilde{J}_r$, and i_J) associated to an element J of the partition will only reoccur for a bounded number of elements of the partition (i.e. a particular admissible interval/point will only appear among $\tilde{J}_\ell, \tilde{J}_r, i_J$ for a constant number of $J \in \mathcal{P}$). This is because the J's in $\mathcal{P}$ are disjoint, so $i_J \in J$ for only one $J \in \mathcal{P}$, and $M(J \cap \tilde{J}_\ell) \geq \frac{1}{2}\tilde{J}_\ell$ implies $\tilde{J}_\ell$ can appear for at most two J's in $\mathcal{P}$.

Now we will prove Theorem 46. We let Ω denote the probability space for $X_1, \ldots, X_N$ (each ω in Ω is associated to a sequence of N real numbers).

For each $\omega \in \Omega$, we let $\mathcal{P}_\omega$ denote a maximizing partition. We define $\mathcal{P}_{\omega,\ell}$ (resp. $\mathcal{P}_{\omega,r}$) to be the set of $\tilde{J}_\ell$ (resp. $\tilde{J}_r$) associated to $J \in \mathcal{P}_\omega$. We note that the same interval could appear as $\tilde{J}_\ell$ or $\tilde{J}_r$ for up to two different J's in $\mathcal{P}_\omega$.

We fix a large constant B which will be specified later. Now we split each set $\mathcal{P}_{\omega,\text{side}}$ (here side $\in \{\ell, r\}$) into two disjoint subsets $\mathcal{P}^{\text{good}}_{\omega,\text{side}}$ and $\mathcal{P}^{\text{bad}}_{\omega,\text{side}}$. We define $\mathcal{P}^{\text{good}}_{\omega,\text{side}}$ to be the set of $\tilde{J} \in \mathcal{P}_{\omega,\text{side}}$ such that

$$\left|\tilde{S}_{\tilde{J}}\right|^2 \leq BM(\tilde{J}) \ln\ln(N). \tag{4.20}$$

We then define $\mathcal{P}^{\text{bad}}_{\omega,\text{side}}$ to be the complement of $\mathcal{P}^{\text{good}}_{\omega,\text{side}}$ inside $\mathcal{P}_{\omega,\text{side}}$.

Our objective is to prove the estimate

$$\mathbb{E}\left[\sum_{J\in\mathcal{P}_\omega} |S_J|^2\right] \ll \ln\ln(N).$$

Using (4.19), we upper bound the left side as follows:

$$\mathbb{E}\left[\sum_{J\in\mathcal{P}_\omega} |S_J|^2\right] \ll \mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{good}}_{\omega,l}} |\tilde{S}_{\tilde{J}}|^2\right] + \mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{good}}_{\omega,r}} |\tilde{S}_{\tilde{J}}|^2\right]$$

$$+\mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad}}_{\omega,l}} |\tilde{S}_{\tilde{J}}|^2\right] + \mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad}}_{\omega,r}} |\tilde{S}_{\tilde{J}}|^2\right] + \mathbb{E}\left[\sum_{J\in\mathcal{P}_\omega} |S_{i_J}|^2\right].$$

We observe that $\sum_{\tilde{J}\in\mathcal{P}^{\text{good}}_{\omega,\text{side}}} |\tilde{S}_{\tilde{J}}|^2 \ll \left(\sum_{\tilde{J}\in\mathcal{P}_{\omega,\text{side}}} M(\tilde{J})\right) \ln\ln(N) \ll \ln\ln(N)$. This holds because $\sum_{J\in\mathcal{P}} M(J) = 1$, and the total mass of the intervals $\tilde{J}_\ell, \tilde{J}_r, i_J$ used to cover each J is at most $2M(J)$, thus $\sum_{\tilde{J}\in\mathcal{P}_{\omega,\text{side}}} M(\tilde{J}) \leq 2$. This shows that the terms involving the good admissible intervals are easily

controlled. The last term is also easily controlled as follows

$$\mathbb{E}\left[\sum_{J\in\mathcal{P}_\omega}|S_{i_J}|^2\right]\ll\mathbb{E}\left[\sum_{n\in[N]}|a_nX_n|^2\right]\ll 1.$$

It remains to control the terms involving the bad admissible intervals. The argument is essentially the same for both the sums over $\mathcal{P}^{\text{bad}}_{\omega,l}$ and $\mathcal{P}^{\text{bad}}_{\omega,r}$, so we will work with the quantity $\mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad}}_{\omega,\text{side}}}|\tilde{S}_{\tilde{J}}|^2\right]$ in what follows.

We now partition $\mathcal{P}^{\text{bad}}_{\omega,\text{side}}$ into two disjoint sets $\mathcal{P}^{\text{bad},1}_{\omega,\text{side}}$ and $\mathcal{P}^{\text{bad},2}_{\omega,\text{side}}$. The set $\mathcal{P}^{\text{bad},1}_{\omega,\text{side}}$ consists of intervals $I_{k,s}\in\mathcal{P}^{\text{bad}}_{\omega,\text{side}}$ such that $|I_{k,s}|\leq 2^{-k/2}N$ and $\mathcal{P}^{\text{bad},2}_{\omega,\text{side}}$ contains the complement set. For each k, we define $T_k\subseteq\{I_{k,s}:1\leq s\leq 2^k\}$ as the collection of all intervals $I_{k,s}$ satisfying $|I_{k,s}|\geq 2^{-k/2}N$. Clearly, $|T_k|\leq 2^{k/2}$ for each k. We then have:

$$\mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad},2}_{\omega,\text{side}}}|\tilde{S}_{\tilde{J}}|^2\right]\ll\mathbb{E}\left[\sum_{k=1}^{\infty}\sum_{\tilde{J}\in T_k}|\tilde{S}_{\tilde{J}}|^2\right]=\sum_{k=1}^{\infty}\sum_{\tilde{J}\in T_k}\mathbb{E}\left[|\tilde{S}_{\tilde{J}}|^2\right].$$

Using (4.18) and the fact that $\mathbb{E}\left[|\tilde{S}_{\tilde{J}}|^2\right]\ll\mathbb{E}\left[|S_{\tilde{J}}|^2\right]$ (by Lemma 65), we have

$$\sum_{k=1}^{\infty}\sum_{\tilde{J}\in T_k}\mathbb{E}\left[|\tilde{S}_{\tilde{J}}|^2\right]\ll\sum_{k=1}^{\infty}\sum_{\tilde{J}\in T_k}\mathbb{E}\left[|S_{\tilde{J}}|^2\right]\ll\sum_{k=1}^{\infty}2^{k/2}2^{-k}\ll 1.$$

It now suffices to bound the more difficult term $\mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad},1}_{\omega,\text{side}}}|\tilde{S}_{\tilde{J}}|^2\right]$.

Now $|I_{k,s}|\leq 2^{-k/2}N$ if $I_{k,s}\in\mathcal{P}^{\text{bad},1}_{\omega,\text{side}}$. For a fixed interval J, we let $B(J)\subseteq\Omega$ denote the event that the $|\tilde{S}_J(\omega)|^2$ is bad. In other words, $\omega\in B(J)$

if $\left|\tilde{S}_J(\omega)\right|^2 \geq BM(J)\ln\ln(N)$. We let T_k^c denote the complement of T_k. We now have that

$$\mathbb{E}\left[\sum_{\tilde{J}\in\mathcal{P}^{\text{bad},1}_{\omega,\text{side}}} |\tilde{S}_{\tilde{J}}|^2\right] \ll \sum_{k=1}^{2\ln(N)} \sum_{\tilde{J}\in T_k^c} \mathbb{E}\left[|1_{B(\tilde{J})}\tilde{S}_{\tilde{J}}|^2\right].$$

Here we have restricted the the summation of k to the range $1 \leq k \leq 2\ln(N)$ using the fact that $1 \leq |I_{k,s}| \leq 2^{-k/2}N$ implies $k \leq 2\ln(N)$.

We let $\gamma > 0$ denote a positive value to be specified later. Letting $2p := 2+\gamma$ and applying Lemma 64 (Rosenthal's inequality) we have that

$$\left(\mathbb{E}\left[|S_{\tilde{J}}|^{2p}\right]\right)^{1/p} = \left(\mathbb{E}\left[|S_{\tilde{J}}|^{2+\gamma}\right]\right)^{\frac{2}{2+\gamma}} \ll \left(\mathbb{E}\left[\left|\sum_{n\in\tilde{J}} a_n X_n\right|^{2+\gamma}\right]\right)^{\frac{2}{2+\gamma}}$$

$$\ll \max\left\{\left(\sum_{n\in\tilde{J}} |a_n|^{2+\gamma}\mathbb{E}\left[|X_i|^{2+\gamma}\right]\right)^{\frac{2}{2+\gamma}}, \left(\sum_{n\in\tilde{J}} |a_n|^2\right)\right\} \ll M(\tilde{J}). \quad (4.21)$$

The last inequality follows from the fact that the ℓ^2 norm is greater than the $\ell^{2+\gamma}$ norm and $\mathbb{E}\left[|X_i|^{2+\gamma}\right] \leq C^{2+\gamma}$.

We let $s := |\tilde{J}|$, and we let $S_{\tilde{J},\ell}$ denote the sum of $a_i X_i$ for the first ℓ indices i in $\tilde{J}$. By definition of the event $B(\tilde{J})$, we have:

$$\mathbb{E}\left[1_{B(\tilde{J})}\right] = \mathbb{P}\left[\left|\tilde{S}_{\tilde{J}}\right|^2 \geq BM(\tilde{J})\ln\ln(N)\right] \leq \mathbb{P}\left[\max_{1\leq\ell\leq s}\left|S_{\tilde{J},\ell}\right|^2 \geq \frac{B}{2}M(\tilde{J})\ln\ln(N)\right].$$

By Lemma 63, this is

$$\ll \max_{1\leq\ell\leq s} \mathbb{P}\left[\left|S_{\tilde{J},\ell}\right|^2 \geq \frac{B}{6}M(\tilde{J})\ln\ln(N)\right].$$

By Lemma 62, this is:

$$\ll \exp\left(-\frac{BM(\tilde{J})\ln\ln(N)}{3C^2M(\tilde{J})}\right) = \exp\left(-\frac{B\ln\ln(N)}{3C^2}\right).$$

By setting the value of B to be sufficiently large with respect to the constant C (i.e. $B > 12C^2$), we have:

$$\mathbb{E}\left[1_{B(\tilde{J})}\right] \ll \ln^{-4}(N). \tag{4.22}$$

We now define q as a function of p so that $\frac{1}{p} + \frac{1}{q} = 1$, i.e. $q = \frac{p}{p-1}$. We then set γ such that

$$\left(\mathbb{E}\left[1_{B(\tilde{J})}\right]\right)^{1/q} \ll \ln^{-2}(N) \tag{4.23}$$

for all $\tilde{J}$. (Recall that $p := \frac{2+\gamma}{2}$.) We now apply Hölder's inequality with p and q to obtain:

$$\sum_{k=1}^{2\ln(N)} \sum_{\tilde{J}\in T_k^c} \mathbb{E}\left[\left|1_{B(\tilde{J})}\tilde{S}_{\tilde{J}}^2\right|\right] \leq \sum_{k=1}^{2\ln(N)} \sum_{\tilde{J}\in T_k^c} \left(\mathbb{E}\left[\left|1_{B(\tilde{J})}\right|^q\right]\right)^{\frac{1}{q}} \left(\mathbb{E}\left[\left|\tilde{S}_{\tilde{J}}\right|^{2p}\right]\right)^{\frac{1}{p}}.$$

Using (4.21), (4.23) and Lemma 65, we see this is:

$$\ll \sum_{k=1}^{2\ln(N)} \sum_{\tilde{J}\in T_k^c} \ln^{-2}(N)M(\tilde{J}) \ll \sum_{k=1}^{2\ln(N)} \ln^{-2}(N) \ll \frac{1}{\ln(N)}.$$

This completes the proof.

4.6 Random Permutations

In this section, we will use probabilistic techniques to prove the following theorem:

Theorem 44. Let $\{\phi_n\}_{n=1}^N$ be an orthonormal system such that $|\phi_n(x)| = 1$ for all n and all $x \in \mathbb{T}$, and $\{a_n\}_{n=1}^N$ a choice of (complex) coefficients. Then there exists a permutation $\pi : [N] \to [N]$ such that

$$\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}\}_{n=1}^N\right|\right|_{L^2(V^2)} \ll \sqrt{\ln\ln(N)}\left(\sum_{n=1}^N |a_n|^2\right)^{1/2}$$

Proof. We assume without loss of generality that $\sum_{n=1}^N |a_n|^2 = 1$. Then, for each a_n, there exists some non-negative integer j such that $2^{-j-1} < |a_n|^2 \leq 2^{-j}$. For each fixed j, we let A_j denote the set of $n \in [N]$ such that $2^{-j-1} < |a_n|^2 \leq 2^{-j}$. We define $A^* \subseteq [N]$ as $A^* := \bigcup_{j=\lceil 2\ln N\rceil}^{\infty} A_j$. We also define

$$b_n = \begin{cases} a_n, & n \in A^* \\ 0, & n \notin A^*. \end{cases}$$

We then observe, for any permutation $\pi : [N] \to [N]$ and any $x \in \mathbb{T}$,

$$\left|\left|\{b_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^N\right|\right|_{V^2} \ll \sum_{n=1}^N |b_n\phi_n(x)| \ll \frac{1}{N}\cdot N \ll 1.$$

Applying the triangle inequality for the $||\cdot||_{V^2}$ norm, this allows us to ignore the contribution of all terms a_n where $n \in A^*$.

We consider the class of permutations $\pi : [N] \to [N]$ such that $\pi^{-1}(A_j)$ is an interval for each j. In other words, these are permutations which group the elements of each A_j together. We allow arbitrary orderings within each group and an arbitrary ordering of the groups. For a fixed permutation π, we let B_j denote the preimage of A_j under π (so B_j is an interval). We will refer to the intervals B_j as "blocks". From this point onward, we will only consider permutations belonging to this class, and we will only consider the contribution

of terms for A_1 up to $A_{\lfloor 2\ln(N)\rfloor}$. We let $N' := |A_1| + \cdots + |A_{\lfloor 2\ln(N)\rfloor}|$. For notational convenience, we assume that π maps $[N']$ bijectively to $\bigcup_{i=1}^{\lfloor 2\ln(N)\rfloor} A_j$. (This is without loss of generality, since we have seen that we can treat the set A^* separately.)

For each fixed permutation $\pi : [N] \to [N]$ in this class and each fixed $x \in \mathbb{T}$, we consider the quantity

$$\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V^2}^2 = \sum_{I\in\mathcal{P}} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2, \tag{4.24}$$

where $\mathcal{P}$ denotes the maximizing partition of $[N']$.

We now define two additional operators, V_L^2 and V_S^2. The value of $\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_L^2}^2$ is defined as

$$\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_L^2}^2 := \sum_{I\in\mathcal{P}_L} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2,$$

where $\mathcal{P}_L$ is the maximizing partition among the subset of partitions of $[N']$ that use only intervals which are unions of the B_j's.

The value of $\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_S^2}^2$ is defined as

$$\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_S^2}^2 := \sum_{I\in\mathcal{P}_S} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2,$$

where $\mathcal{P}_S$ is the maximizing partition among the subset of partitions of $[N']$ that use only intervals I that are contained in some B_j. This can be alternatively described as taking that maximizing partition of each B_j and then taking a union of these to form $\mathcal{P}_S$.

We now claim:

$$\left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V^2}^2 \ll \left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_L^2}^2 + \left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_S^2}^2. \tag{4.25}$$

To see this, consider the maximizing partition $\mathcal{P}$ in (4.24). Each $I \in \mathcal{P}$ can be expressed as the union of three disjoint intervals, I_{S_ℓ}, I_L, and I_{S_r}, where I_{S_ℓ} and I_{S_r} are each contained in some B_i, and I_L is a union of B_i's. More precisely, I_L is the union of all the intervals B_j that are contained in I, I_{S_ℓ} goes from the left endpoint of I until the left endpoint of I_L, and I_{S_r} goes from the right endpoint of I_L until the right endpoint of I. By construction, each of I_{S_ℓ} and I_{S_r} is contained in some B_j. (Some of I_L, I_{S_r}, I_{S_ℓ} may be empty.) Thus,

$$\left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2 \ll \left|\sum_{n\in I_L} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2 + \left|\sum_{n\in I_{S_\ell}} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2 + \left|\sum_{n\in I_{S_r}} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2.$$

Now, if we consider the set of intervals I_L corresponding to $I \in \mathcal{P}$, we get a disjoint set of intervals that can occur as part of a partition considered by the operator V_L^2. Similarly, if we consider the set of intervals I_{S_ℓ}, I_{S_r} corresponding to $I \in \mathcal{P}$, we get a disjoint set of intervals that can occur as part of a partition considered by the operator V_S^2. Therefore,

$$\sum_{I\in\mathcal{P}} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2 \ll \sum_{I\in\mathcal{P}_L} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2 + \sum_{I\in\mathcal{P}_S} \left|\sum_{n\in I} a_{\pi(n)}\phi_{\pi(n)}(x)\right|^2.$$

The inequality (4.25) then follows.

We first bound the contribution of the V_L^2 operator. For each B_j, we define the function $f_j : \mathbb{T} \to \mathbb{C}$ as:

$$f_j(x) := \sum_{n \in B_j} a_{\pi(n)} \phi_{\pi(n)}(x). \tag{4.26}$$

Since the sets B_j are disjoint, we note that the functions f_j are orthogonal to each other, but they may not be uniformly bounded. We need to show that there exists a permutation $\sigma : [\lfloor 2\ln(N) \rfloor] \to [\lfloor 2\ln(N) \rfloor]$ of the f_j values such that

$$\left|\left| \{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N) \rfloor} \right|\right|_{L^2(V^2)} \ll \sqrt{\ln\ln(N)} \left(\sum_{n=1}^{N} |a_n|^2 \right)^{1/2}. \tag{4.27}$$

This would imply that there is some ordering of the blocks for which the contribution of the V_L^2 operator is suitably bounded.

To show (4.27), we will use the following inequality of Garsia for real numbers:

Lemma 67. (See Theorem 3.6.15 in [22].) Let $x_1, \ldots, x_M \in \mathbb{R}$. We consider choosing a permutation ψ of $[M]$ uniformly at random. Then:

$$\mathbb{E}\left[\max_{1 \le k \le M} \left(x_{\psi(1)} + \cdots + x_{\psi(k)} \right)^2 \right] \ll \left(\sum_{k=1}^{M} x_k \right)^2 + \sum_{k=1}^{M} x_k^2.$$

We derive the following corollary:

Corollary 68. Let $x_1, \ldots, x_M \in \mathbb{R}$. Let L be a positive integer, $1 \le L \le M$. Let $\mathcal{P}$ denote the partition of $[M]$ into intervals of size L (starting with $[L]$),

except that the last interval may be of smaller size (when L does not divide M). We consider choosing a permutation ψ of $[M]$ uniformly at random. Then:

$$\mathbb{E}\left[\sum_{I\in\mathcal{P}}\max_{I'\subseteq I}\left(\sum_{j\in I'}x_{\psi(j)}\right)^2\right] \ll \binom{M-1}{L-1}^{-1}\left(\sum_{\substack{S\subseteq[M]\\|S|=L}}\left(\sum_{j\in S}x_j\right)^2+\sum_{j\in S}x_j^2\right).$$

We note here that S ranges over all subsets of $[M]$ of size L.

Proof. By linearity of expectation, we first observe:

$$\mathbb{E}\left[\sum_{I\in\mathcal{P}}\max_{I'\subseteq I}\left(\sum_{j\in I'}x_{\psi(j)}\right)^2\right] = \sum_{I\in\mathcal{P}}\mathbb{E}\left[\max_{I'\subseteq I}\left(\sum_{j\in I'}x_{\psi(j)}\right)^2\right].$$

This quantity is then

$$\ll \frac{M}{L}\,\mathbb{E}\left[\max_{I'\subset I}\left(\sum_{j\in I'}x_{\psi(j)}\right)^2\right],$$

where I is any fixed interval of size L (without loss of generality, we may take I to be $[L]$).

For any subset $S\subseteq[M]$ of size L, the probability that ψ maps I to S is $\binom{M}{L}^{-1}$. Conditioned on this event, the action of ψ on I acts as random permutation of the values x_j for $j\in S$. Applying Lemma 67, we then have the expectation (still conditioned on ψ mapping I to S) is $\ll \left(\sum_{j\in S}x_j\right)^2 + \sum_{j\in S}x_j^2$. (Note that the maximum over all subintervals I' of I is bounded by a constant times the maximum over subintervals starting at the left endpoint

of I, as in the lemma.) Thus,

$$\mathbb{E}\left[\max_{I'\subset I}\left(\sum_{j\in I'} x_{\psi(j)}\right)^2\right] \ll \binom{M}{L}^{-1}\sum_{\substack{S\subseteq[M]\\|S|=L}}\left(\left(\sum_{j\in S} x_j\right)^2+\sum_{j\in S} x_j^2\right).$$

Since $\frac{M}{L}\binom{M}{L}^{-1} = \binom{M-1}{L-1}^{-1}$, the corollary follows. □

We now decompose $[\lfloor 2\ln(N)\rfloor]$ into a family of dyadic intervals. More precisely, we consider all dyadic intervals of the form

$$((c-1)2^\ell, c2^\ell],\ \ell\in\{0,1,\dots,\lceil\ln(2\ln N)\rceil\},\ c\in\left\{1,\dots,2^{\lceil\ln\ln(N)+\ln 2\rceil-\ell}\right\}$$

(Some of these intervals may go beyond $M := \lfloor 2\ln(N)\rfloor$. For these, we consider their intersection with $[M]$.) The exponent ℓ of an interval here defines its "level". In other words, we say an interval $((c-1)2^\ell, c2^\ell]$ is on level ℓ. We let $\mathcal{F}$ denote the set of all intervals of this form.

We then have that for *any* interval $I'\subseteq[M]$, there are (at most) two adjacent intervals $I_l, I_r\in\mathcal{F}$ such that $I'\subseteq I_l\cup I_r$, and $|I_l\cup I_r|\le 4|I'|$ (when only one interval is needed, one of I_l, I_r can be substituted by $\emptyset$). To see this, consider the smallest positive integer k such that $|I'|<2^k$. Then either I' is contained in some dyadic interval of length 2^k, or it contains exactly one right endpoint of such an interval. We then take I_l to the be interval on level k with this right endpoint, and take I_r to be the next interval (with this as its open left endpoint).

This implies the following upper bound for each permutation σ and

each $x \in \mathbb{T}$:

$$\left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2 \ll \sum_{I\in\mathcal{F}} \max_{I'\subseteq I} \left|\sum_{j\in I'} f_{\sigma(j)}(x)\right|^2. \tag{4.28}$$

This holds because for each interval J in the maximizing partition, $J \subseteq I_l \cup I_r$ for some $I_r, I_l \in \mathcal{F}$ with $|I| < 4|I_l \cup I_r|$. Each $I \in \mathcal{F}$ will correspond to at most a constant number of J's (it can only be I_l for one J when I_r is non-empty, I_r for one J when I_l is non-empty, and it can contain at most 3 corresponding J's), and this constant factor is absorbed by the $\ll$ notation.

We consider choosing σ uniformly at random. We observe by Fubini's theorem:

$$\mathbb{E}\left[\int_{\mathbb{T}} \left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2 dx\right] = \int_{\mathbb{T}} \mathbb{E}\left[\left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2\right] dx.$$

Using the triangle inequality for the $||\cdot||_{V^2}$ norm and linearity of expectation, we can split each $f_j(x)$ into real and imaginary parts, $f_j(x) = f_j^r(x) + if_j^i(x)$, where f_j^r and f_j^i are both real valued. We then have:

$$\ll \int_{\mathbb{T}} \mathbb{E}\left[\left|\left|\{f_{\sigma(j)}^r(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2\right] dx + \int_{\mathbb{T}} \mathbb{E}\left[\left|\left|\{f_{\sigma(j)}^i(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2\right] dx.$$

For each ℓ from 0 to $\lceil \ln(2\ln N)\rceil$, we let $\mathcal{F}_\ell$ denote the intervals in $\mathcal{F}$ on level ℓ. On each level, these intervals are disjoint. Applying (4.28) to the quantity above for f^r (the argument for f^i is identical), we can express the result as:

$$\int_{\mathbb{T}} \mathbb{E}\left[\left|\left|\{f_{\sigma(j)}^r(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2\right] dx \ll \int_{\mathbb{T}} \mathbb{E}\left[\sum_{\ell=0}^{\lceil \ln(2\ln N)\rceil} \sum_{I\in\mathcal{F}_\ell} \max_{I'\subseteq I} \left|\sum_{j\in I'} f_{\sigma(j)}^r(x)\right|^2\right] dx.$$

By linearity of expectation, this is:

$$= \int_{\mathbb{T}} \sum_{\ell=0}^{\lceil \ln(2\ln N)\rceil} \mathbb{E}\left[\sum_{I\in\mathcal{F}_\ell} \max_{I'\subseteq I} \left|\sum_{j\in I'} f^r_{\sigma(j)}(x)\right|^2\right] dx.$$

Now, for each ℓ, we apply Corollary 68 to the dyadic intervals on level ℓ. As a result, we see that the above quantity is

$$\ll \sum_{\ell=0}^{\lceil \ln(2\ln N)\rceil} \binom{\lfloor 2\ln(N)\rfloor - 1}{2^\ell - 1}^{-1} \times$$

$$\sum_{\substack{S\subseteq[\lfloor 2\ln(N)\rfloor]\\ |S|=2^\ell}} \left(\int_{\mathbb{T}} \left(\sum_{j\in S} f^r_j(x)\right)^2 dx + \sum_{j\in S}\int_{\mathbb{T}} f^r_j(x)^2 dx\right). \tag{4.29}$$

Combining this with the same result for the imaginary parts, we have:

$$\int_{\mathbb{T}} \mathbb{E}\left[\left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2\right] dx \ll \sum_{\ell=0}^{\lceil \ln(2\ln N)\rceil} \binom{\lfloor 2\ln(N)\rfloor - 1}{2^\ell - 1}^{-1} \times$$

$$\sum_{\substack{S\subseteq[\lfloor 2\ln(N)\rfloor]\\ |S|=2^\ell}} \left(\int_{\mathbb{T}} \left(\sum_{j\in S} f^r_j(x)\right)^2 + \left(\sum_{j\in S} f^i_j(x)\right)^2 dx + \sum_{j\in S}\int_{\mathbb{T}} f^r_j(x)^2 + f^i_j(x)^2 dx\right) \tag{4.30}$$

We consider the quantity

$$\int_{\mathbb{T}} \left(\sum_{j\in S} f^r_j(x)\right)^2 + \left(\sum_{j\in S} f^i_j(x)\right)^2 dx = \int_{\mathbb{T}} \sum_{j,j'\in S} f^r_j(x) f^r_{j'}(x) + f^i_j(x) f^i_{j'}(x) dx.$$

When $j \neq j'$,

$$\int_{\mathbb{T}} f^r_j(x) f^r_{j'}(x) + f^i_j(x) f^i_{j'}(x) dx = 0,$$

since f_j and $f_{j'}$ are orthogonal, and this is the real part of $\int_{\mathbb{T}} f_j(x)\overline{f_{j'}(x)}dx$. Thus,

$$\int_{\mathbb{T}} \left(\sum_{j\in S} f_j^r(x)\right)^2 + \left(\sum_{j\in S} f_j^i(x)\right)^2 dx \ll \sum_{j\in S}\int_{\mathbb{T}} f_j^r(x)^2 + f_j^i(x)^2 dx.$$

We then have:

$$\mathbb{E}\left[\int_{\mathbb{T}} \left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2 dx\right]$$

$$\ll \sum_{\ell=0}^{\lceil \ln(2\ln N)\rceil} \binom{\lfloor 2\ln(N)\rfloor - 1}{2^\ell - 1}^{-1} \sum_{\substack{S\subseteq[\lfloor 2\ln(N)\rfloor] \\ |S|=2^\ell}} \sum_{j\in S}\int_{\mathbb{T}} |f_j(x)|^2 dx.$$

By Parseval's identity, $\int_{\mathbb{T}} |f_j(x)|^2 dx = \sum_{n\in A_j} |a_n|^2$. Since each j occurs in exactly $\binom{\lfloor 2\ln(N)\rfloor - 1}{2^\ell - 1}$ sets of size 2^ℓ for each ℓ, the above quantity is:

$$\ll \ln\ln(N)\sum_{n=1}^{N} |a_n|^2.$$

This implies that there exists some permutation σ such that

$$\int_{\mathbb{T}} \left|\left|\{f_{\sigma(j)}(x)\}_{j=1}^{\lfloor 2\ln(N)\rfloor}\right|\right|_{V^2}^2 dx \ll \ln\ln(N)\sum_{n=1}^{N} |a_n|^2.$$

Taking a square root of both sides of this establishes (4.27), as desired. This concludes our analysis of the V_L^2 operator.

We now bound the contribution of the V_S^2 operator.

Lemma 69. For some π in our class of permutations,

$$\int_{\mathbb{T}} \left|\left|\{a_{\pi(n)}\phi_{\pi(n)}(x)\}_{n=1}^{N'}\right|\right|_{V_S^2}^2 dx \ll \ln\ln(N)\sum_{n=1}^{N} |a_n|^2.$$

Proof. We first observe that it suffices to prove the following inequality for each A_j. We let Π_j denote the set of permutations of A_j, i.e. each $\pi_j \in \Pi_j$ is a bijective map from $[|A_j|] \to A_j$. We consider choosing such a permutation uniformly at random. Then if we have

$$\mathop{\mathbb{E}}_{\pi_j \in \Pi_j} \left[\int_{\mathbb{T}} \left|\left| \{a_{\pi_j(n)} \phi_{\pi_j(n)}(x)\}_{n=1}^{|A_j|} \right|\right|_{V^2}^2 dx \right] \ll \ln\ln(N) \sum_{n \in A_j} |a_n|^2 \tag{4.31}$$

for each j, this means that there exists a permutation π_j of each A_j satisfying

$$\int_{\mathbb{T}} \left|\left| \{a_{\pi_j(n)} \phi_{\pi_j(n)}(x)\}_{n=1}^{|A_j|} \right|\right|_{V^2}^2 dx \ll \ln\ln(N) \sum_{n \in A_j} |a_n|^2,$$

and these permutations can be put together to form a permutation π as required for Lemma 69. We note that it does not matter how we concatenate the π_j's: by definition of the V_S^2 operator, it only matters how each A_j is permutated, not the order the A_j's are placed in.

We now fix a j and we will prove (4.31). By Fubini's theorem, we can interchange the order of the integral and the expectation and instead work with the quantity

$$\int_{\mathbb{T}} \mathop{\mathbb{E}}_{\pi_j \in \Pi_j} \left[\left|\left| \{a_{\pi_j(n)} \phi_{\pi_j(n)}(x)\}_{n=1}^{|A_j|} \right|\right|_{V^2}^2 \right] dx.$$

For each fixed x, we define the set of complex numbers $\mathcal{C}$ to be the set of values $a_n \phi_n(x)$ for $n \in A_j$. Then, these complex numbers $c \in \mathcal{C}$ all satisfy $2^{-j-1} < |c|^2 \leq 2^{-j}$ (recall that $|\phi_n(x)| = 1$). We let $N_j := |A_j|$, and we let random variables $Z_1, \ldots, Z_{N_j}$ denote random samples from $\mathcal{C}$ taken *without*

replacement. We then see that it suffices to show:

$$\mathbb{E}\left[\left|\left|\{Z_n\}_{n=1}^{N_j}\right|\right|_{V^2}^2\right] \ll \ln\ln(N)\sum_{c\in\mathcal{C}}|c|^2 + \left|\sum_{c\in\mathcal{C}} c\right|^2. \tag{4.32}$$

To show this, we will need the following lemma:

Lemma 70. Let $X_1, \ldots, X_{N_j}$ denote uniformly random samples from $\mathcal{C}$ **with** replacement. For each k from 1 to N_j, we let $S_k := \sum_{i=1}^{k} X_i$. For a subinterval $I \subseteq [N_j]$, we let $S_I := \sum_{i\in I} X_i$. Then for any k and any $p > 2$:

$$\mathbb{E}\left[\max_{I\subseteq[k]} |S_I - \mathbb{E}[S_I]|^p\right] \ll C^p k^{\frac{p}{2}} p^{\frac{p}{2}} 2^{-jp/2},$$

where C is a positive constant.

Proof. We rely on Hoeffding's inequality [26], which implies that

$$\mathbb{P}\left[\max_{I\subseteq[k]} |Re[S_I] - \mathbb{E}[Re[S_I]]| > t\right] \ll exp\left(\frac{-ct^2}{k2^{-j}}\right), \tag{4.33}$$

for some positive constant c, where $Re[S_I]$ denotes the real part of S_I. (More precisely, Hoeffding's inequality is applied with the maximum over S_m for $1 \leq m \leq k$. However, moving to a maximum over arbitrary subintervals only results in a change of the constant c.) The same holds analogously for the imaginary part of S_I.

We note that

$$\mathbb{E}\left[\max_{I\subseteq[k]} |Re[S_I] - \mathbb{E}[Re[S_I]]|^p\right] =$$

$$p\int_0^\infty t^{p-1}\mathbb{P}\left[\max_{I\subseteq[k]} |Re[S_I] - \mathbb{E}[Re[S_I]]| > t\right] dt. \tag{4.34}$$

Applying (4.33), this is

$$\ll p \int_0^\infty t^{p-1} exp\left(\frac{-ct^2}{k2^{-j}}\right) dt.$$

We now perform the change of variable $t = \lambda^{\frac{1}{p}}$, so $dt = \frac{1}{p}\lambda^{\frac{1}{p}-1}d\lambda$. We obtain:

$$= \int_0^\infty exp\left(\frac{-c\lambda^{2/p}}{k2^{-j}}\right) d\lambda.$$

We recall that $\Gamma(z) := \int_0^\infty t^{z-1}e^{-t}dt$. Performing the change of variable $t = s^{\frac{2}{p}}$, we have

$$\Gamma(z) := \frac{2}{p}\int_0^\infty s^{\frac{2}{p}-1}s^{\frac{2}{p}(z-1)}e^{-s^{2/p}}ds = \frac{2}{p}\int_0^\infty s^{\frac{2}{p}z-1}e^{-s^{2/p}}ds.$$

We now see that

$$\int_0^\infty e^{-t^{\frac{2}{p}}}dt = \frac{p}{2}\,\Gamma\left(\frac{p}{2}\right).$$

We then set $s := \left(\frac{c}{k2^{-j}}\right)^{p/2}\lambda$, and we have:

$$\int_0^\infty exp\left(\frac{-c\lambda^{2/p}}{k2^{-j}}\right) d\lambda = \left(\frac{c}{k2^{-j}}\right)^{-p/2}\int_0^\infty e^{-s^{\frac{2}{p}}}ds = \left(\frac{c}{k2^{-j}}\right)^{-p/2}\frac{p}{2}\,\Gamma\left(\frac{p}{2}\right).$$

This yields

$$\mathbb{E}\left[\max_{I\subseteq[k]}|Re[S_I] - \mathbb{E}[Re[S_I]]|^p\right] \ll \frac{p}{2}k^{p/2}c^{-p/2}2^{-jp/2}\,\Gamma\left(\frac{p}{2}\right).$$

By Sterling's formula, $\Gamma(z) \ll \sqrt{\frac{2\pi}{z}}\left(\frac{z}{e}\right)^z$. Thus, $\Gamma\left(\frac{p}{2}\right) \ll \sqrt{\frac{4\pi}{p}}\left(\frac{p}{2e}\right)^{\frac{p}{2}}$. By arguing analogously for the imaginary parts, we obtain:

$$\mathbb{E}\left[\max_{I\subseteq[k]}|S_I - \mathbb{E}[S_I]|^p\right] \ll C^p k^{\frac{p}{2}}p^{\frac{p}{2}}2^{-jp/2},$$

where C is a positive constant. □

Using the above lemma, we estimate $\mathbb{E}\left[\left|\left|\{Z_n\}_{n=1}^{N_j}\right|\right|_{V^2}^2\right]$ as follows. We let $N_j' = 2^m$ be the smallest power of 2 which is $\geq N_j$. We then decompose $[N_j']$ into a family of dyadic intervals. More precisely, we define $\mathcal{F}$ to be the family of intervals of the form

$$((d-1)2^\ell, d2^\ell],\ \ell \in \{0,1,\ldots,m\},\ d \in \{1,\ldots,2^{m-\ell}\}.$$

Now, for any interval I', there are (at most) two intervals $I_l, I_r \in \mathcal{F}$ such that $I' \subseteq I_l \cup I_r$ and $|I_l \cup I_r| < 4|I'|$. Moreover, for any partition $\mathcal{P}$ of $[N_j]$, the number of times an $I \in \mathcal{F}$ is associated to an $I' \in \mathcal{P}$ is upper bounded by a constant. (This is as we have argued previously.)

We let Ω denote our probability space ($\omega \in \Omega$ corresponds to a specified value for each Z_n). Now, for a fixed $\omega \in \Omega$, we say an interval $I \subseteq \mathcal{F}$ is *good* if:

$$\max_{I' \subseteq I} |S_{I'} - \mathbb{E}[S_{I'}]|^2 \leq D2^{-j}|I| \ln\ln(N),$$

where D is a positive constant whose value we will specify later. Otherwise, we say I is *bad*. We let $\mathcal{P}$ denote the maximal partition (which depends on ω). For each interval $I' \in \mathcal{P}$, we have (at most two) covering intervals $I_r, I_l \in \mathcal{F}$. We let $\mathcal{F}_\mathcal{P}$ denote the set of intervals in $\mathcal{F}$ which correspond to intervals in $\mathcal{P}$ (each $I \in \mathcal{F}$ corresponds to at most a constant number of intervals $I' \in \mathcal{P}$). We have:

$$\sum_{I' \in \mathcal{P}} \left|\sum_{n \in I} Z_n\right|^2 \ll \sum_{I \in \mathcal{F}_\mathcal{P}} \max_{I' \subseteq I} \left|\sum_{n \in I'} Z_n\right|^2.$$

We observe that

$$\sum_{\substack{I\in\mathcal{F}_{\mathcal{P}}\\ I \text{ is good}}} \max_{I'\subseteq I}\left|\sum_{n\in I'} Z_n\right|^2 \ll \left|\sum_{c\in\mathcal{C}} c\right|^2 + D2^{-j}N_j \ln\ln(N) \ll \ln\ln(N)\sum_{c\in\mathcal{C}}|c|^2 + \left|\sum_{c\in\mathcal{C}} c\right|^2,$$

since each $|c|^2$ is between 2^{-j-1} and 2^{-j}, and $|\mathcal{C}| = N_j$. To see this, note that for each I', $|S_{I'}|^2 \ll |S_{I'} - \mathbb{E}[S_{I'}]|^2 + |\mathbb{E}[S_{I'}]|^2$, and $|\mathbb{E}[S_{I'}]|^2 = \left|\frac{|I'|}{N_j}\sum_{c\in\mathcal{C}} c\right|^2$.

It only remains to bound the contribution of the intervals that are not good. For this, we first prove the following lemma. For each interval $I \in \mathcal{F}$, we let $B(I)$ denote the event that I is *bad* (i.e. not good), and we let $1_{B(I)}$ denote its indicator function.

Lemma 71. For each $I \in \mathcal{F}$,

$$\mathbb{P}\left[1_{B(I)}\right] \ll \frac{1}{\ln(N)^4},$$

when D is chosen to be a sufficiently large constant.

Proof. By Chebyshev's inequality, for any $p > 2$ we have

$$\mathbb{P}\left[1_{B(I)}\right] =$$
$$\mathbb{P}\left[\max_{I'\subseteq I}|S_{I'} - \mathbb{E}[S_{I'}]|^2 > D2^{-j}|I|\ln\ln(N)\right] \ll \frac{\mathbb{E}\left[\max_{I'\subseteq I}|S_{I'} - \mathbb{E}[S_{I'}]|^p\right]}{(D2^{-j}|I|\ln\ln(N))^{p/2}}. \tag{4.35}$$

We now rely on the following result of Rosén [59].

Lemma 72. (Theorem 4 in [59]) Let $X_1, \ldots, X_k$ be samples drawn from a finite set of real numbers with replacement, and let $Z_1, \ldots, Z_k$ be samples

drawn without replacement. Let $1 \leq n_1 < n_2 < \cdots < n_m$. For every convex, monotone function $\phi : \mathbb{R} \to \mathbb{R}$, we have

$$\mathbb{E}\left[\max\left(\phi\left(\sum_{n=1}^{n_1} Z_n\right), \ldots, \phi\left(\sum_{n=1}^{n_m} Z_n\right)\right)\right]$$
$$\leq \mathbb{E}\left[\max\left(\phi\left(\sum_{n=1}^{n_1} X_n\right), \ldots, \phi\left(\sum_{n=1}^{n_m} X_n\right)\right)\right].$$

We want to apply this lemma to the function $f(x) := |x|^p$, but this is not monotone. Instead we define monotone, convex functions f_1, f_2 such that $|x|^p = f_1(x) + f_2(x)$, namely setting $f_1(x) = (-x)^p$ for $x < 0$ and equal to 0 otherwise, and $f_2(x) = x^p$ for $x > 0$ and equal to 0 otherwise. We note that $|x|^p \geq f_1(x), f_2(x)$ always holds.

Without loss of generality, we consider I equal to the interval of length $|I|$ starting at 1. Then, for some constant H, we have:

$$\mathbb{E}\left[\max_{I' \subseteq I} |S_{I'} - \mathbb{E}[S_{I'}]|^p\right] \ll H^p\, \mathbb{E}\left[\max_{1 \leq n \leq |I|} f_1\left(Re\left(S_n - \mathbb{E}[S_n]\right)\right)\right] +$$
$$\cdots + H^p\, \mathbb{E}\left[\max_{1 \leq n \leq |I|} f_2\left(Im\left(S_n - \mathbb{E}[S_n]\right)\right)\right].$$

Here, S_n denotes the partial sum of $Z_1 + Z_2 + \cdots + Z_n$, Re denotes the real part, Im denotes the imaginary part, and there are four terms in this sum: one for each combination of f_1, f_2 and real and imaginary parts.

We can apply Lemma 72 to each of these four terms to replace the samples $Z_1, \ldots, Z_{|I|}$ taken without replacement with samples $X_1, \ldots, X_{|I|}$ taken with replacement. Now applying Lemma 70, we have

$$\mathbb{P}\left[1_{B(I)}\right] \ll \frac{\tilde{H}^p |I|^{\frac{p}{2}} p^{\frac{p}{2}} 2^{-jp/2}}{\sqrt{D}^p (\ln\ln(N))^{\frac{p}{2}} |I|^{\frac{p}{2}} 2^{-jp/2}} = \left(\frac{\tilde{H}}{\sqrt{D}}\right)^p p^{\frac{p}{2}} (\ln\ln(N))^{-\frac{p}{2}},$$

for some constant $\tilde{H}$.

Now, setting $p := \ln\ln(N)/e$, this is:

$$= \left(\frac{\tilde{H}}{\sqrt{D}}\right)^{\frac{\ln\ln(N)}{e}} \ln(N)^{-\frac{1}{2e}}.$$

We can then set D large enough so that $\frac{\tilde{H}}{\sqrt{D}} < e^{-4e}$, and the lemma follows. $\square$

We observe that the contribution of the bad intervals is upper bounded by

$$\ll \sum_{I\in\mathcal{F}} \mathbb{E}\left[1_{B(I)} \max_{I'\subseteq I} |S_{I'}|^2\right]. \tag{4.36}$$

We next apply Hölder's inequality with q, r fixed to be constants such that $\frac{1}{r} + \frac{1}{q} = 1$ and $\frac{4}{q} > 2, r > 1$. We then have that the above quantity is:

$$\ll \sum_{I\in\mathcal{F}} \left(\mathbb{E}[1_{B(I)}]\right)^{\frac{1}{q}} \left(\mathbb{E}\left[\max_{I'\subseteq I} |S_{I'}|^{2r}\right]\right)^{\frac{1}{r}}.$$

By Lemma 71, we know that

$$\left(\mathbb{E}[1_{B(I)}]\right)^{\frac{1}{q}} \ll (\ln(N))^{-2}.$$

We also know that for each I', $|\mathbb{E}[S_{I'}]|^2 \ll \left(\frac{|I'|}{N_j}\right)^2 \left|\sum_{c\in\mathcal{C}} c\right|^2 \ll \frac{|I'|}{N_j}\left|\sum_{c\in\mathcal{C}} c\right|^2$. When we sum these up over all $\mathcal{I}\in\mathcal{F}$, we obtain $\ll \ln(N)\left|\sum_{c\in\mathcal{C}} c\right|^2$. Now multiplying by $\ln(N)^{-2}$, we obtain a contribution which is $o\left(\left|\sum_{c\in\mathcal{C}} c\right|^2\right)$. Thus, it only remains to bound

$$(\ln(N))^{-2} \sum_{I\in\mathcal{F}} \left(\mathbb{E}\left[\max_{I'\subseteq I} |S_{I'} - \mathbb{E}[S_{I'}]|^{2r}\right]\right)^{\frac{1}{r}}.$$

Similarly to our above arguments, we define convex, monotone functions $f_1, f_2 : \mathbb{R} \to \mathbb{R}$ such that $f_1(x) + f_2(x) = |x|^{2r}$. More precisely, we set $f_1(x) = (-x)^{2r}$ when $x < 0$ and equal to 0 otherwise, while we set $f_2(x) = x^{2r}$ when $x > 0$ and equal to 0 otherwise. Now, again applying Lemma 72, it suffices to bound e.g.

$$\sum_{I \in \mathcal{F}} \left(\mathbb{E} \left[\max_{1 \leq n \leq |I|} f_1(Re(S_n - \mathbb{E}[S_n])) \right] \right)^{\frac{1}{r}},$$

where S_n is now the partial sum $X_1 + \cdots + X_n$, where each X_k is a sample from $\mathcal{C}$ taken *with* replacement. (We must also bound the analogous quantities for other combinations of f_1, f_2 and Re, Im, but these will follow via the same argument.)

We now apply Lemma 65 to obtain that the above quantity is

$$\ll \sum_{I \in \mathcal{F}} \left(\mathbb{E} \left[\max_{1 \leq n \leq |I|} |Re(S_n - \mathbb{E}[S_n])|^{2r} \right] \right)^{\frac{1}{r}} \ll \sum_{I \in \mathcal{F}} \left(\mathbb{E}[|Re(S_I - \mathbb{E}[S_I])|^{2r}] \right)^{\frac{1}{r}}.$$

Next applying Lemma 64, we see that this is

$$\ll \sum_{I \in \mathcal{F}} \max \left\{ \left(\sum_{n=1}^{|I|} \mathbb{E}[|\tilde{X}_n|^{2r}] \right)^{\frac{1}{r}}, \sum_{n=1}^{|I|} \mathbb{E}[|\tilde{X}_n|^2] \right\},$$

where $\tilde{X}_n$ is defined to be an (independent, uniform) sample from $\mathcal{C}$ with replacement, recentered to be mean zero. In other words, $\tilde{X}_n = X_n - \mathbb{E}X_n$. Now, since $r > 1$, both of the quantities in this maximum are $\ll |I| 2^{-j}$. Hence, we have:

$$\ll \sum_{I \in \mathcal{F}} |I| 2^{-j} \ll \ln(N) \sum_{c \in \mathcal{C}} |c|^2.$$

Multiplying this by our bound $(\ln(N))^{-2}$ for the probability of each I being bad, we see that this is $o\left(\sum_{c\in\mathcal{C}}|c|^2\right)$. This completes the proof of Lemma 69.

□

Combining Lemma 69 with (4.27), we obtain Theorem 44.

□

4.7 Refinements of Theorem 40 for Certain Structured ONS

In this section, we briefly outline how Theorem 40 can be improved for more restrictive classes of ONS, using the methods employed in proving Theorem 46. We consider an ONS such that for f in the span of the system, we have $||f||_{L^p} \leq C_p||f||_{L^2}$ for $p > 2$, where C_p is a constant depending only on p. Such systems arise naturally, for example, as the restriction of the trigonometric system to certain arithmetic subsets ($\Lambda(p)$ sets). We will use the fact that a maximal form of this hypothesis can be obtained from a very general theorem of Christ and Kiselev [9].

Theorem 73. Let $\{\phi_n\}_{n=1}^{\infty}$ be an ONS such that for f in the span of the system, we have $||f||_{L^p} \leq C_p||f||_{L^2}$ for some $p > 2$. Then

$$||\mathcal{M}f||_{L^p} \ll_\delta C_p||f||_{L^2} \tag{4.37}$$

as long as $p > \delta > 2$.

This last condition implies that the implicit constant is uniform for large p. Using this and the arguments in the proof of Theorem 46, one can obtain the following:

Theorem 74. Let $\{\phi_n\}_{n=1}^{\infty}$ be a ONS such that if f is in the span of the system, then $||f||_{L^p} \ll C_p||f||_{L^2}$ for some $p > 2$. We then have that

$$||f||_{L^2(V^2)} \ll_p \ln^{1/p}(|A|)||f||_{L^2}.$$

where the coefficients of f are supported a finite index set A.

We briefly sketch the proof. We note that if $||\mathcal{M}f||_{L^2} \ll ||f||_{L^2}$ holds, then this theorem follows for $p = 2$. However, this is in general not true and by the sharpness of Theorem 40, the best one can hope for in the general case is a factor of $\ln(|A|)$ in place of $\ln^{1/2}(|A|)$. The proof follows the same setup as the proof of Theorem 46. We define a bad event for some interval J to be the event that $|\tilde{S}_J| \gg \ln^{1/p}(|A|)(M(J))^{1/2}$ (here $M(J)$ is defined to be the sum of a_n^2 over $n \in J$, where the a_n's are the coefficients of ϕ_n in the expansion of f). It is easy to see that the contribution from the good events are of an acceptable order and it suffices to bound the bad events. The argument is essentially the same as the proof of Theorem 46, with the exception that we use the following estimate:

$$\int_{\mathbb{T}} |1_{B(\tilde{J})}\tilde{S}_{\tilde{J}}|^2 \leq \left(\int_{\mathbb{T}} 1_{B(\tilde{J})}\right)^{1/(p/2)'} \left(\int_{\mathbb{T}} |\tilde{S}_{\tilde{J}}|^p\right)^{(2/p)}.$$

(Here, $(p/2)'$ denotes the conjugate exponent of $p/2$.)

We now estimate $\int_{\mathbb{T}} |\tilde{S}_{\tilde{J}}|^p \ll C_p^p \ \left(\int_{\mathbb{T}} |S_{\tilde{J}}|^2\right)^{p/2} \ll C_p^p \ (M(\tilde{J}))^{p/2}$. Hence $\left(\int_{\mathbb{T}} |\tilde{S}_{\tilde{J}}|^p\right)^{(2/p)} \ll C_p^2 M(\tilde{J})$. Next, by Chebyshev's inequality,

$$\int_{\mathbb{T}} 1_{B(\tilde{J})} \leq \frac{\int_{\mathbb{T}} |\tilde{S}_{\tilde{J}}|^p}{\left(\ln^{1/p}(|A|)(M(\tilde{J}))^{1/2}\right)^p} \leq \frac{C_p^p}{\ln(|A|)}.$$

Hence (using $1/(p/2)' = \frac{p-2}{p}$), we have $\left(\int_{\mathbb{T}} 1_{B(\tilde{J})}\right)^{(p-2)/p} \ll \frac{C_p^{p-2}}{\ln^{(p-2)/p}(|A|)}$. This yields

$$\int_{\mathbb{T}} |1_{B(J)}\tilde{S}_{\tilde{J}}|^2 \leq \left(\int_{\mathbb{T}} 1_{B(\tilde{J})}\right)^{1/(p/2)'} \left(\int_{\mathbb{T}} |\tilde{S}_{\tilde{J}}|^p\right)^{(2/p)} \ll \frac{C_p^p M(\tilde{J})}{\ln^{(p-2)/p}(|A|)}.$$

Now we sum this quantity over $\ln(|A|)$ levels, each with the sum of $M(\tilde{J})$ summing to 1. Hence the contribution from the bad events to the quantity we wish to estimate is $O(\ln^{2/p}(|A|))$. This is exactly the order we wish to show.

Finally, we observe that:

Theorem 75. Let $\{\phi_n\}_{n=1}^{\infty}$ be an ONS such that if f is in the span of the system, then $||f||_{L^p} \ll \sqrt{p}||f||_{L^2}$ (for all $p > 2$). Then

$$||f||_{L^2(V^2)} \ll \sqrt{\ln\ln(|A|)}||f||_{L^2},$$

where the coefficients of f are supported on the index set A.

This is proved using the same arguments sketched for the previous theorem, however now we have freedom to optimize over the choice of p we use. The optimum occurs with a choice of p about $ce^{-1}\ln\ln(N)$. Essentially

the same argument is given in detail in the proof of Theorem 44 for random permutations (see the proof of Lemma 71). Here it is important that the constants in the Christ-Kiselev theorem are uniformly bounded for large p.

The above theorem can be applied to systems formed by Sidon subsets of the trigonometric system, since the hypothesis of this theorem characterizes Sidon sets (when applied to subsets of the trigonometric system) by a theorem of Pisier [56] (see also [61]).

4.8 Variational Estimates for the V^p Operator

4.8.1 Notation

Let $\Gamma : \mathbb{R} \to \mathbb{R}^+$ be a convex symmetric function, increasing on $\mathbb{R}^+$ and tending to infinity at infinity such that $\Gamma(0) = 0$. Then the Orlicz space norm associated to Γ is defined as

$$||f||_\Gamma := \min \left\{ \lambda : \int_{\mathbb{T}} \Gamma \left(\frac{f(x)}{\lambda} \right) dx \leq 1 \right\}.$$

The fact that this norm satisfies the triangle inequality is an easy exercise using Jensen's inequality. We refer the reader to [35] for the general theory of these spaces. Following [4], we will be interested in $\Gamma := \Gamma_K$ defined as follows

$$\Gamma_K(t) := \begin{cases} |t|^{5/2}, & |t| \leq K \\ \frac{5}{4} K^{1/2} t^2 - \frac{1}{4} K^{5/2}, & |t| \geq K \end{cases}.$$

Later we will also use

$$\gamma_K(t) := \begin{cases} |t|^{1/2}, & |t| \leq K \\ K^{1/2}, & |t| \geq K \end{cases} .$$

We note that $t^2\gamma_K(t) \leq \Gamma_K(t)$ for all t. We state some other basic properties that we will need.

Lemma 76. Let $2 = p$. Then $||\cdot||_{\Gamma_K}$ is p-convex. That is, for any functions $f_1, \ldots, f_k$ from $\mathbb{T}$ to $\mathbb{R}$,

$$\left|\left|\left(\sum_{i=1}^k |f_i|^p\right)^{1/p}\right|\right|_{\Gamma_K} \leq \left(\sum_{i=1}^k ||f_i||_{\Gamma_K}^p\right)^{1/p} .$$

Proof. Let $\Gamma_{K,1/p}(t) := \Gamma_K(t^{1/p})$, which we observe is still convex (we have used that $p = 2$ here). Since $\Gamma_{K,1/p}(t)$ is convex, we can use it to form an Orlicz space norm. We observe that

$$\left|\left|\left(\sum_{i=1}^k |f_i|^p\right)^{1/p}\right|\right|_{\Gamma_K} = \min\left\{\lambda : \int_{\mathbb{T}} \Gamma_K\left(\frac{\left(\sum_{i=1}^k |f_i(x)|^p\right)^{1/p}}{\lambda}\right) dx \leq 1\right\}$$

$$= \min\left\{\lambda : \int_{\mathbb{T}} \Gamma_{K,1/p}\left(\frac{\sum_{i=1}^k |f_i(x)|^p}{\lambda^p}\right) dx \leq 1\right\} = \left|\left|\sum_{i=1}^k |f_i|^p\right|\right|_{\Gamma_{K,1/p}}^{1/p}$$

$$\leq \left(\sum_{i=1}^k |||f_i|^p||_{\Gamma_{K,1/p}}\right)^{1/p} = \left(\sum_{i=1}^k ||f_i||_{\Gamma_K}^p\right)^{1/p} .$$

The inequality here follows from the triangle inequality for $||\cdot||_{\Gamma_{K,1/p}}$. □

4.8.2 Proof of Theorem 47

We now prove:

Theorem 47. Let $p > 2$ and $\{\phi_n\}_{n=1}^N$ be an orthonormal system such that $||\phi_n||_{L^\infty} \leq C$ for all n. There exists a permutation $\pi : [N] \to [N]$ such that the orthonormal system $\{\psi_n := \phi_{\pi(n)}\}_{n=1}^N$ satisfies

$$||f||_{L^2(V^p)} \ll_{C,p} \ln\ln(N)||f||_{L^2} \tag{4.38}$$

for all $f = \sum_{n=1}^N a_n\psi_n(x)$.

Our starting point is the inequality (3.21) of [4]:

Theorem 77. Let $\{\phi_n\}_{n=1}^N$ be an orthonormal system with $||\phi_n||_{L^\infty} \leq C$ for all n. Then there exists a permutation $\pi : [N] \to [N]$ such that for all subintervals I of $[N]$ and all real values $a_1, \ldots, a_N$, the orthonormal system $\{\psi_n := \phi_{\pi(n)}\}_{n=1}^N$ satisfies:

$$\left|\left|\sum_{n\in I} a_n\psi_n\right|\right|_{\Gamma_{N/|I|}} \ll_C \ln^{3/4}(N)\left(\sum_{n\in[I]} a_n^2\right)^{1/2}. \tag{4.39}$$

We will need a variational form of this inequality. This is easily achieved using a Rademacher-Menshov argument.

Lemma 78. With the notation as above, we have that

$$\left|\left|||\{a_n\psi_n\}_{n\in I}||_{V^2}\right|\right|_{\Gamma_{N/|I|}} \ll_C \ln^{7/4}(N)\left(\sum_{n\in I} a_n^2\right)^{1/2} \tag{4.40}$$

for all $I \subseteq [N]$ and all real sequences $a_1, \ldots, a_N$.

Proof. As in section 4.3, we assume (without loss of generality) that $I = [2^\ell]$ for some ℓ and we define the intervals $I_{k,i} := (k2^i, (k+1)2^i]$ for $0 \leq i \leq \ell$ and $0 \leq k \leq 2^{\ell-i} - 1$. For each $J \subseteq I$, we can express J as a disjoint union of intervals $I_{k,i}$, where the union contains at most two intervals of each size. As in (4.7), we then observe for each $x \in \mathbb{T}$:

$$||\{a_n\psi_n\}_{n\in I}||_{V^2}(x) \ll \sum_{i=0}^{\ell} \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left(\sum_{n\in I_{k,i}} a_n\psi_n(x)\right)^2}.$$

By the triangle inequality for the Orlicz norm, we then have

$$\left|\left|\,||\{a_n\psi_n\}_{n\in I}||_{V^2}\,\right|\right|_{\Gamma_{N/|I|}} \ll \sum_{i=0}^{\ell} \left|\left| \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left(\sum_{n\in I_{k,i}} a_n\psi_n(x)\right)^2} \right|\right|_{\Gamma_{N/|I|}}.$$

Applying Lemma 76, this is

$$\leq \sum_{i=0}^{\ell} \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \left|\left| \sum_{n\in I_{k,i}} a_n\psi_n(x) \right|\right|^2_{\Gamma_{N/|I|}}}.$$

By Theorem 77, we obtain

$$\ll_C \ln^{3/4}(N) \sum_{i=0}^{\ell} \sqrt{\sum_{k=0}^{2^{\ell-i}-1} \sum_{n\in I_{k,i}} a_n^2} = \ln^{3/4}(N) \sum_{i=0}^{\ell} \sqrt{\sum_{n\in I} a_n^2} = \ln^{7/4}(N) \sqrt{\sum_{n\in I} a_n^2}.$$

□

We now prove Theorem 47. We assume (without loss of generality) that $\sum_{n=1}^{N} a_n^2 = 1$. As in Section 4.5, we consider decomposing $[N]$ into a family

of subintervals according to mass, defined with respect to the a_n's. We recall that the mass of an arbitrary subinterval I is defined to be $M(I) := \sum_{n \in I} a_n^2$. We define the intervals $I_{k,s}$ for $1 \leq s \leq 2^k$ and points $i_{k,s}$ as in Section 4.5. We refer to the intervals $I_{k,s}$ for $1 \leq s \leq 2^k$ as the admissible intervals on level k, and the points $i_{k,s}$ (as s ranges) as the admissible points on level k. We note that any interval $I \subseteq [N]$ can be expressed as a union of intervals of the form $I_{k,s}$ and points $i_{k,s}$, where there are at most two intervals and two points for each value of k (this follows analogously to the proof of Lemma 49). This decomposition is obtained by first taking the intervals $I_{k,s}$ and points $i_{k,s}$ contained in I with the smallest value of k. (There are at most 2 of each, otherwise I would contain an admissible interval or point for a smaller k value.) These "components" of I on level k form an interval, and when we remove this from I, we are left with a left part and a right part. Each part can then be decomposed as union of intervals $I_{k,s}$ and points $i_{k,s}$ for higher values of k, and each of the two unions contains at most one interval and one point on each level.

We let $\pi : [N] \to [N]$ be the permutation as in Lemma 78, and $\psi_n := \phi_{\pi(n)}$. We fix an $x \in \mathbb{T}$. The value of

$$\left|\left|\{a_n \psi_n(x)\}_{n=1}^N\right|\right|_{V^p}$$

is achieved by some partition $\mathcal{P}$ of $[N]$. Each $I \in \mathcal{P}$ can be expressed as a union of intervals of the form $I_{k,s}$ and points $i_{k,s}$, and we denote the set of these intervals and points by T_I and t_I respectively. We recall that each of T_I

and t_I will have at most two intervals or points (respectively) on each level. We also note that each admissible interval will appear in this union for at most one $I \in \mathcal{P}$.

We fix a positive constant c (depending on p) such that

$c > \max\{\frac{35}{4}\left(\frac{1}{2}-\frac{1}{p}\right)^{-1}, 9\}$ (this is possible because $p > 2$). We define $k^* := c\ln\ln(N)$ (more precisely, k^* is the nearest integer greater than $c\ln\ln(N)$). Now, for each $I \in \mathcal{P}$, all of the intervals in T_I and points in t_I on levels greater than k^* are contained in the two intervals I_{k^*,s_ℓ} and I_{k^*,s_r} on level k^*, where s_ℓ is one less than the s value for the leftmost interval $I_{k^*,s}$ in T_I, and s_r is one more than the s value for the rightmost interval $I_{k^*,s}$ in T_I. We will use k^* as a cutoff threshold: we handle the intervals and points at levels $\leq k^*$ directly and handle the intervals and points at levels $> k^*$ using the fact that they are contained in $I_{k^*,s_\ell}, I_{k^*,s_r}$. We define T_I' to be the subset of intervals in T_I on levels $\leq k^*$ and t_I' to be the subset of points in t_I on levels $\leq k^*$.

Now, $\left|\left|\{a_n\psi_n(x)\}_{n=1}^N\right|\right|_{V^p}$ is equal to:

$$\left(\sum_{I\in\mathcal{P}}\left(\sum_{n\in I}a_n\psi_n(x)\right)^p\right)^{1/p} =$$

$$\left(\sum_{I\in\mathcal{P}}\left(\sum_{J\in T_I'}\sum_{n\in J}a_n\psi_n(x)+\sum_{J\in T_I\setminus T_I'}\sum_{n\in J}a_n\psi_n(x)+\sum_{n\in t_I'}a_n\psi_n(x)+\sum_{n\in t_I\setminus t_I'}a_n\psi_n(x)\right)^p\right)^{1/p}.$$

Applying the triangle inequality for the ℓ_p-norm, this is:

$$\leq \left(\sum_{I\in\mathcal{P}}\left(\sum_{J\in T_I'}\sum_{n\in J} a_n\psi_n(x)\right)^p\right)^{1/p} + \left(\sum_{I\in\mathcal{P}}\left(\sum_{n\in t_I'} a_n\psi_n(x)\right)^p\right)^{1/p}$$
$$+ \left(\sum_{I\in\mathcal{P}}\left(\sum_{J\in T_I\setminus T_I'}\sum_{n\in J} a_n\psi_n(x) + \sum_{n\in t_I\setminus t_I'} a_n\psi_n(x)\right)^p\right)^{1/p} \tag{4.41}$$

We consider the second of these three terms. Since $p \geq 2$, we have

$$\left(\sum_{I\in\mathcal{P}}\left(\sum_{n\in t_I'} a_n\psi_n(x)\right)^p\right)^{1/p} \leq \left(\sum_{I\in\mathcal{P}}\left(\sum_{n\in t_I'} a_n\psi_n(x)\right)^2\right)^{1/2}.$$

For each $k \leq k^*$, we let ℓ_k denote the set of admissible points on level k. Since each t_I' contains at most 2 points in each ℓ_k, we can apply the triangle inequality to obtain

$$\left(\sum_{I\in\mathcal{P}}\left(\sum_{n\in t_I'} a_n\psi_n(x)\right)^2\right)^{1/2} \ll \sum_{k=0}^{k^*}\left(\sum_{n\in\ell_k}(a_n\psi_n(x))^2\right)^{1/2}.$$

Now, by the triangle inequality for the L^2 norm and the fact that $\int_{\mathbb{T}} a_n^2\psi_n^2(x)dx = a_n^2$ for all n, we have

$$\left\|\sum_{k=0}^{k^*}\left(\sum_{n\in\ell_k}(a_n\psi_n(x))^2\right)^{1/2}\right\|_{L^2} \ll_p \ln\ln(N).$$

To see this, recall that $\sum_{n=1}^N a_n^2 = 1$, so $\sum_{n\in\ell_k} a_n^2 \leq 1$ for each k, and $k^* \ll_p \ln\ln(N)$.

It remains to bound the first and third terms in (4.41). We consider the first term. For each k, we let $\mathcal{L}_k$ denote the set of admissible intervals $I_{k,s}$

as s ranges from 1 to 2^k (i.e. the admissible intervals on level k). Then, by triangle inequality for the ℓ^2 norm and the fact that $p \geq 2$,

$$\left(\sum_{I \in \mathcal{P}} \left(\sum_{J \in T_I'} \sum_{n \in J} a_n \psi_n(x) \right)^p \right)^{1/p} \leq \left(\sum_{I \in \mathcal{P}} \left(\sum_{J \in T_I'} \sum_{n \in J} a_n \psi_n(x) \right)^2 \right)^{1/2}$$

$$\leq \sum_{k=0}^{k^*} \left(\sum_{I \in \mathcal{P}} \left(\sum_{J \in T_I' \cap \mathcal{L}_k} \sum_{n \in J} a_n \psi_n(x) \right)^2 \right)^{1/2}$$

$$\leq \sum_{k=0}^{k^*} \left(\sum_{J \in \mathcal{L}_k} \left(\sum_{n \in J} a_n \psi_n(x) \right)^2 \right)^{1/2}.$$

Now, using the triangle inequality for the $||\cdot||_{L^2}$ norm, we have:

$$\left\| \sum_{k=0}^{k^*} \left(\sum_{J \in \mathcal{L}_k} \left(\sum_{n \in J} a_n \psi_n(x) \right)^2 \right)^{1/2} \right\|_{L^2} \leq \sum_{k=0}^{k^*} \left\| \left(\sum_{J \in \mathcal{L}_k} \left(\sum_{n \in J} a_n \psi_n(x) \right)^2 \right)^{1/2} \right\|_{L^2}$$

$$= \sum_{k=0}^{k^*} \left(\sum_{J \in \mathcal{L}_k} \int_{\mathbb{T}} \left(\sum_{n \in J} a_n \psi_n(x) \right)^2 dx \right)^{1/2}$$

$$= \sum_{k=0}^{k^*} \left(\sum_{J \in \mathcal{L}_k} M(J) \right)^{1/2} \ll_p \ln \ln(N),$$

since $\sum_{J \in \mathcal{L}_k} M(J) = 1$ for each k, and $k^* \ll_p \ln \ln(N)$.

We are thus left with the third term of (4.41). For each $I \in \mathcal{P}$, we consider the union of the intervals and points in $T_I \backslash T_I'$ and $t_I \backslash t_I'$. This can alternatively be described as a union of at most two intervals J_ℓ and J_r, where each of J_ℓ, J_r is a subinterval of $I_{k^*,s}$ for some s. To see this, recall that I is decomposed into a union of admissible intervals and points by taking the

admissible intervals and points contained in I for the earliest level where this set is non-empty. The remaining left and right parts of I are then decomposed separately. If the minimal k is $\leq k^*$, then J_ℓ is the union of the intervals/points in the decomposition of the left part that fall beyond level k^*, and J_r is the same for the right part. If the minimal k is $> k^*$, then in fact all of I is contained in some admissible interval on level k^*, and we can take J_ℓ to be this interval and J_r to be empty. We then rewrite the quantity we wish to bound as:

$$\left(\sum_{I \in \mathcal{P}} \left(\sum_{n \in J_\ell} a_n \psi_n(x) + \sum_{n \in J_r} a_n \psi_n(x) \right)^p \right)^{1/p}.$$

Applying the simple fact that $(a+b)^p \leq 2^p(a^p + b^p)$ for all non-negative real numbers a and b, we see this is

$$\ll \left(\sum_{I \in \mathcal{P}} \left(\sum_{n \in J_\ell} a_n \psi_n(x) \right)^p + \left(\sum_{n \in J_r} a_n \psi_n(x) \right)^p \right)^{1/p}.$$

Now we observe that we are summing the values $a_n \psi_n(x)$ over disjoint intervals, each of which is contained in $I_{k^*,s}$ for some s. Thus, this quantity is upper bounded by:

$$\leq \left(\sum_{1 \leq s \leq 2^{k^*}} \left|\left| \{a_n \psi_n(x)\}_{n \in I_{k^*,s}} \right|\right|_{V^p}^p \right)^{1/p}.$$

Therefore, it suffices to bound

$$\left|\left| \left(\sum_{1 \leq s \leq 2^{k^*}} \left|\left| \{a_n \psi_n(x)\}_{n \in I_{k^*,s}} \right|\right|_{V^p}^p \right)^{1/p} \right|\right|_{L^2}.$$

For each s from 1 to 2^{k^*}, we define disjoint sets G_s, B_s such that $G_s \cup B_s = \mathbb{T}$. We define G_s to be $x \in \mathbb{T}$ such that $||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p} \leq 2^{-c\ln\ln(N)/p}$ and B_s to be the complement. By two applications of the triangle inequality (first in the ℓ^p norm and then in the L^2 norm), we have

$$\left|\left|\left(\sum_{s=1}^{2^{k^*}} ||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p}^p\right)^{1/p}\right|\right|_{L^2} \ll \left|\left|\left(\sum_{s=1}^{2^{k^*}} 1_{G_s}||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p}^p\right)^{1/p}\right|\right|_{L^2}$$
$$+ \left|\left|\left(\sum_{s=1}^{2^{k^*}} 1_{B_s}||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p}^p\right)^{1/p}\right|\right|_{L^2}.$$

Using that $||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p}^p \ll 2^{-c\ln\ln(N)}$ for $x \in G_s$, we have that the first term is $O(1)$ (from the fact that there are at most $2^{c\ln\ln(N)}$ terms in the sum). We now estimate

$$\left|\left|\left(\sum_{s=1}^{2^{k^*}} 1_{B_s}(x)||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^p}^p\right)^{1/p}\right|\right|_{L^2}$$
$$\ll \left|\left|\left(\sum_{s=1}^{2^{k^*}} 1_{\tilde{B}_s}(x)||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2}^2\right)^{1/2}\right|\right|_{L^2}$$
$$\ll \left(\sum_{s=1}^{2^{k^*}} ||1_{\tilde{B}_s}(x)||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2}||_{L^2}^2\right)^{1/2}, \tag{4.42}$$

where $\tilde{B}_s$ is the set of $x \in \mathbb{T}$ such that $||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2} \geq 2^{-c\ln\ln(N)/p}$, and we have used the fact that $B_s \subseteq \tilde{B}_s$.

We now consider two cases. First, we consider the set S_{big} of s values where $|I_{k^*,s}| \geq N2^{-7\ln\ln(N)}$. Clearly, there can be at most $2^{7\ln\ln(N)}$ such intervals. Now we bound the contribution to (4.42) above from these big intervals as

$$\left(\sum_{s\in S_{\text{big}}}^{2^{k^*}} ||1_{\tilde{B}_s}(x)||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2}||_{L^2}^2\right)^{1/2}$$
$$\ll \left(\sum_{s\in S_{\text{big}}}^{2^{k^*}} ||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{L^2(V^2)}^2\right)^{1/2}.$$

Recalling that $||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{L^2(V^2)}^2 \ll \ln^2(N)2^{-c\ln\ln(N)}$ (from Lemma 50, since $M(I_{k^*,s}) \leq 2^{-k^*}$ for all s) and that there are at most $2^{7\ln\ln(N)}$ values of $s \in S_{\text{big}}$, we have that the above is

$$\ll \left(2^{7\ln\ln(N)}\ln^2(N)2^{-c\ln\ln(N)}\right)^{1/2} \ll 1.$$

Here we have used that $9 \leq c$. It now suffices to consider the values of s such that $|I_{k^*,s}| \leq N2^{-7\ln\ln(N)}$.

We define $\gamma_* = \gamma_{2^{7\ln\ln(N)}}$. For any real numbers $\epsilon > 0$, $\lambda > 1$, and $a \geq \epsilon$, we have $\frac{\gamma_*(\lambda^{-1}a)}{\gamma_*(\lambda^{-1}\epsilon)} \geq 1$. We set $\epsilon := 2^{-c\ln\ln(N)/p}$. Now, for all $x \in \tilde{B}_s$, we have:

$$\left|\left|\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}\right|\right|_{V^2}^2 \leq \left|\left|\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}\right|\right|_{V^2}^2 \frac{\gamma_*(\lambda^{-1}||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2})}{\gamma_*(\lambda^{-1}\epsilon)}. \tag{4.43}$$

We recall that $M(I_{k^*,s}) \leq 2^{-c\ln\ln(N)}$ for each s. Analogously to γ_*, we define $\Gamma_* := \Gamma_{2^{7\ln\ln(N)}}$. Now, for any $\lambda > 1$:

$$\int_{\tilde{B}_s} \left|\left|\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}\right|\right|_{V^p}^2 dx \leq \lambda^2 \int_{\tilde{B}_s} \gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1} \Gamma_*(\lambda^{-1}||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2})dx.$$

This follows from (4.43) and the definitions of γ_* and Γ_* (recall also that $t^2\gamma_*(t) \leq \Gamma_*(t)$ for all t).

Since $\frac{N}{|I_{k^*,s}|} \geq 2^{7\ln\ln(N)}$ and the value of $||\cdot||_{\Gamma_K}$ increases as K increases, we can apply Lemma 78 to obtain

$$\left|\left|\left|\{a_n\psi_n\}_{n\in I_{k^*,s}}||_{V^2}\right|\right|_{\Gamma_*} \leq D\ln^{7/4}(N)\left(\sum_{n\in I_{k^*,s}} a_n^2\right)^{1/2}$$

for all s such that $|I_{k^*,s}| \leq N2^{-\frac{7}{2}\ln\ln(N)}$, where D is some fixed constant (depending on C).

We see that for $\lambda := D\ln^{7/4}(N)2^{-\frac{c\ln\ln(N)}{2}}$, we have

$\int_{\mathbb{T}} \Gamma_*(\lambda^{-1}||\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}||_{V^2})dx \ll 1$. Therefore:

$$\int_{\tilde{B}_s} \left|\left|\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}\right|\right|_{V^p}^2 dx \ll \ln^{7/2}(N)2^{-c\ln\ln(N)}\gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1}. \tag{4.44}$$

We consider the quantity $\gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1}$. We observe:

$$\frac{\epsilon}{\lambda} = (D^{-1})2^{\ln\ln(N)(-c/p+c/2-7/4)}. \tag{4.45}$$

Now, if (4.45) is $\geq 2^{7\ln\ln(N)}$, we will have

$$\gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1} = 2^{-7/2\ln\ln(N)}.$$

If (4.45) is $< 2^{7\ln\ln(N)}$, we will have

$$\gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1} = D^{1/2}2^{\ln\ln(N)(7/8-c/4+c/2p)}.$$

We note that $\frac{7}{8} - \frac{c}{4} + \frac{c}{2p} \leq -\frac{7}{2}$, because $c\left(\frac{1}{2} - \frac{1}{p}\right) \geq \frac{35}{4}$. Thus, in either case,

$$\gamma_*\left(\frac{\epsilon}{\lambda}\right)^{-1} \ll_C 2^{-7/2\ln\ln(N)}.$$

Inserting this into (4.44), we find that

$$\int_{\tilde{B}_s} \left|\left|\{a_n\psi_n(x)\}_{n\in I_{k^*,s}}\right|\right|_{V^p}^2 dx \ll_C \ln^{7/2}(N)2^{-c\ln\ln(N)}2^{-7/2\ln\ln(N)} \ll_C 2^{-c\ln\ln(N)}.$$

Now to bound (4.42), we apply this to each of the $\leq 2^{c\ln\ln(N)}$ terms, yielding $O(1)$, completing the proof.

Chapter 5

Orthonormal Systems in Linear Spans

5.1 Introduction

Let $\mathbb{T}$ denote a probability space and $\Phi := \{\phi_n(x)\}_{n=1}^N$ an orthonormal system (ONS) of functions from $\mathbb{T}$ to $\mathbb{C}$. One is often interested, usually motivated by questions regarding almost everywhere convergence, in the behavior of the maximal function

$$\mathcal{M}f := \max_{\ell \leq N} \left| \sum_{n=1}^{\ell} a_n \phi_n \right|.$$

For an arbitrary ONS the Radamacher-Menchov theorem states that $||\mathcal{M}f||_{L^2} \ll \log(N)||f||_{L^2}$, where the $\log(N)$ factor is known to be sharp. One however can do much better for many classical systems, for instance one can replace $\log(N)$ with an absolute constant in the case of the trigonometric system (the Carleson-Hunt inequality). More recently, there has been interest in variational refinements of these maximal results. Define the r-th variation operator

$$\mathcal{V}^r f := \left(\max_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \left| \sum_{n \in I} a_n \phi_n \right|^r \right)^{1/r}$$

where $\mathcal{P}_N$ denotes the set of partitions of $[N]$ into subintervals. Clearly, $|\mathcal{M}f| \leq |\mathcal{V}^r f|$ for all $r < \infty$. In the case of trigonometric system it has been shown that $||\mathcal{V}^r f||_2 \ll ||f||_2$ for $r > 2$ [52], and $||\mathcal{V}^2 f||_2 \ll \sqrt{\log(N)}||f||_2$ [41], where the factor of $\sqrt{\log(N)}$ is optimal. This later inequality has some applications to sieve theory [38]. The factor of $\sqrt{\log(n)}$ is rather unfortunate, leading to inefficiencies in these applications. It is likely that this can be improved in cases where the Fourier support of f has arithmetic structure. This is a potential route towards for improving the estimates in [38]. Some results in this direction can be found in section 7 of [41].

In a different direction, it seems that the $\sqrt{\log(n)}$ might also be an eccentricity of the standard ordering of the trigonometric system. In [41] (see Chapter 3) we posed the problem:

Problem 79. Is there a permutation $\sigma : [N] \to [N]$ such that the reordering of the trigonometric system $\Phi := \{\phi_n = e(\sigma(n)x)\}$ (where $e(x) := e^{2\pi i x}$) satisfies

$$||\mathcal{V}^2 f||_2 \ll o(\sqrt{\log(N)})||f||_2?$$

In support of an an affirmative answer we proved that given a function $f = \sum_{n=1}^{N} a_n e(nx)$, there exists a permutation $\sigma : [N] \to [N]$ such that reordered trigonometric system satisfies $||\mathcal{V}^2 f||_2 \ll \sqrt{\log\log(N)}||f||_2$. There, we have allowed the permutation to depend on the function, while in the above problem we seek a permutation that works for all functions simultaneously.

In this paper we will consider a relaxation of this problem. For an ONS $\Phi := \{\phi_n(x)\}_{n=1}^{N}$ and $N \times N$ orthogonal matrix $O = \{o_{i,n}\}_{1 \leq i,n \leq N}$ we define a

new ONS, $\Psi := \{\psi_n(x)\}_{n=1}^N$. By

$$\psi_n(x) := \sum_{i=1}^N o_{i,n}\phi_n(x).$$

This new system will span the same space as the original system (and every such system can be obtained in this manner). Let us write $\Phi(O) := \Psi$.

Theorem 80. Given an ONS $\Phi := \{\phi_n(x)\}_{n=1}^N$ from $\mathbb{T}$ to $\mathbb{R}$ there exists an alternate ONS $\Phi(O)$ that spans the same space, and satisfies

$$||\mathcal{V}^2 f||_2 \ll \sqrt{\log\log(N)}||f||_2. \tag{5.1}$$

Indeed the conclusion holds for a generic $O \in \mathcal{O}(N)$ with large probability. If we take $\Phi := \{e(nx)\}_{n=1}^N$ then this produces an ONS of trigonometric polynomials (spanning the same space as the trigonometric system) with much smaller square variation than the trigonometric system. Strictly speaking, Theorem 80 is stated for real valued ONS, but the result for the trigonometric system can be obtained by splitting into real and imaginary parts. We note that Problem 79 asks for a similar conclusion where O is restricted to be a permutation matrix instead of just an orthogonal matrix.

Theorem 80 is sharp. Consider an ONS of independent, mean zero, variance 1 Gaussians, g_i. Notice that applying an orthogonal transform to this system leaves it metrically unchanged. On the other hand we have that $\max_{\pi\in\mathcal{P}_N}\sum_{I\in\pi}\left|\sum_{n\in I} g_n\right|^2 \sim 2N\log\log(N)$ (almost surely) from the variational law of the iterated logarithm [36].

Let us briefly outline the key idea in the proof of Theorem 80. In [41] we proved an estimate of the form (5.1) for system of bounded independent random variables (see Theorem 9). The key observation in that case is that for every f in the span of the system we have the sub-gaussian tail estimate $||f||_{\mathcal{G}} \leq ||f||_2$ (where $||\cdot||_{\mathcal{G}}$ is the Orlicz space associated to $e^{x^2} - 1$). This clearly can't hold in the setting of theorem 80, since any L^2 function can be in the span of the system. However, we will show that for a generic O the system will satisfy $||f||_{\mathcal{G}} \leq ||f||_2$ (with a controllable error) once the support of Fourier coefficients of f is small. More precisely we prove:

Proposition 81. For N fixed, let $\Phi = \{\phi_n(x)\}_{n=1}^N$ be an ONS. There exists an orthogonal matrix O such that the associated system $\Phi(O) = \{\psi_n\}_{n=1}^N$ satisfies the following property. For any $f = \sum a_n \psi_n$, letting m denote support$(\{a_n\})$, we have that the function defined by

$$f := \sum a_n \psi_n(x)$$

can be decomposed as $f := G + E$ where $||G||_{\mathcal{G}(c)} \ll ||f||_2$ for some universal constant $c > 0$ (see the next section for this notation) and $||E||_2 \ll \left(\frac{m}{N}\right)^{c'} ||f||_2$ for some universal constant $c' > 0$.

See Proposition 92 below, which gives a stronger maximal form of this statement. It seems likely that this decomposition may have other applications, and perhaps may have greater appeal than the main result itself. The techniques used here are based in part on those of [4] and [41].

5.2 Preliminaries

We need to define several different norms on the space of functions from $\mathbb{T}$ to $\mathbb{C}$. First, for a positive constant c let $||\cdot||_{\mathcal{G}(c)}$ denote the Orlicz spaces associated to the convex function $e^{cx^2}-1$. That is

$$||f||_{\mathcal{G}(c)} := \inf_{\lambda\in\mathbb{R}^+}\left\{\int e^{c|f/\lambda|^2}-1\leq 1\right\}.$$

When we write $||\cdot||_{\mathcal{G}}$ with the specification of c omitted, we mean $c=1$.

We next define the convex function

$$\Gamma_K(t) := \begin{cases} e^{t^2}-1, & |t|\leq K \\ e^{K^2}t^2+e^{K^2}(1-K^2)-1, & |t|\geq K \end{cases}$$

and denote the associated Orlitz norm $||\cdot||_{\Gamma_K}$. We then have

Lemma 82. When $K\geq 1$, for all t we have that

$$\Gamma_K(t)\leq e^{t^2}-1$$

$$\Gamma_K(t)\leq e^{K^2}t^2.$$

It follows that for $f:\mathbb{T}\to\mathbb{R}$ we have $||f||_{\Gamma_K}\leq||f||_{\mathcal{G}}$ and $||f||_{\Gamma_K}\leq e^{K^2/2}||f||_{L^2}$.

Proof. We first prove $\Gamma_K(t)\leq e^{t^2}-1$ for all t. For t such that $|t|\leq K$, this is clear since $\Gamma_K(t)=e^{t^2}-1$. We consider t such that $|t|\geq K$. Then $\Gamma_K(t)=e^{K^2}t^2+e^{K^2}(1-K^2)-1$, so we must show that $e^{K^2}t^2+e^{K^2}(1-K^2)\leq e^{t^2}$. We note that for all real $x\geq 0$, $1+x\leq e^x$. Applying this to the quantity $t^2-K^2+1>0$, we have:

$$e^{K^2}t^2+e^{K^2}(1-K^2)=e^{K^2}(t^2-K^2+1)\leq e^{K^2}e^{t^2-K^2}=e^{t^2},$$

as required.

We let f be a function from $\mathbb{T}$ to $\mathbb{R}$. For any fixed positive real number λ such that $\int e^{|f/\lambda|^2} - 1 \leq 1$ (i.e. $\lambda \geq ||f||_{\mathcal{G}}$), we have

$$\int \Gamma_K(f/\lambda) \leq \int e^{|f/\lambda|^2} - 1 \leq 1,$$

since $\Gamma_K(t) \leq e^{t^2} - 1$ for all t. This shows that $\lambda \geq ||f||_{\Gamma_K}$, hence $||f||_{\Gamma_K} \leq ||f||_{\mathcal{G}}$.

We next prove $\Gamma_K(t) \leq e^{K^2}t^2$. We first consider t such that $|t| \geq K$. In this case, $\Gamma_K(t) = e^{K^2}t^2 + e^{K^2}(1 - K^2) - 1$. Since $K \geq 1$, we see that $e^{K^2}(1 - K^2) < 0$, so $\Gamma_K(t) \leq e^{K^2}t^2$ follows. For t such that $|t| \leq K$, we have $\Gamma_K(t) = e^{t^2} - 1$, so we must show that $e^{t^2} - 1 \leq e^{K^2}t^2$ for $|t| \leq K$.

We consider $\frac{e^{t^2}-1}{t^2}$ as a function of t for $t \geq 0$. Its derivative is:

$$2\left(t^{-1}e^{t^2} - t^{-3}e^{t^2} + t^{-3}\right).$$

We observe that this is always non-negative. To see this, consider multiplying the quantity by t^3 to obtain $2(t^2e^{t^2} - e^{t^2} + 1)$. Non-negativity then follows from the inequality $1 + xe^x \geq e^x$ for all real $x \geq 0$. (This inequality can be proved by noting that $xe^x \geq \int_0^x e^u du$.) Hence $\frac{e^{t^2}-1}{t^2}$ is a non-decreasing function of t in the range $0 \leq t \leq K$, so it suffices to consider the value at $t = K$, which is $K^{-2}(e^{K^2} - 1)$. Since $K \geq 1$, this is $< e^{K^2}$, as required.

For $f : \mathbb{T} \to \mathbb{R}$, we consider $\lambda := e^{K^2/2}||f||_{L^2}$. Then

$$\int \Gamma_K(f/\lambda) \leq \int e^{K^2}\frac{f^2}{\lambda^2} = \frac{e^{K^2}}{\lambda^2}||f||_{L^2}^2 = 1,$$

since $\Gamma_K(t) \leq e^{K^2}t^2$. Thus, $||f||_{\Gamma_K} \leq e^{K^2/2}||f||_{L^2}$. □

Lemma 83. For any (measurable) $f : \mathbb{T} \to \mathbb{R}$, we can decompose $f = f_1 + f_2$ such that

$$||f_1||_{\mathcal{G}} \ll ||f||_{\Gamma_K} \text{ and}$$

$$||f_2||_{L^2} \ll e^{-cK^2}||f||_{\Gamma_K},$$

for some universal constant $c > 0$.

Proof. Given f, we define $\gamma := 2||f||_{\Gamma_K}$ to simplify our notation. We then set:

$$f_1 := f \cdot \mathbb{I}_{|\frac{f}{\gamma}| \leq K} \text{ and } f_2 := f \cdot \mathbb{I}_{|\frac{f}{\gamma}| \geq K},$$

where $\mathbb{I}_S$ for a set $S \subset \mathbb{T}$ denotes the indicator function for that set. By definition of $\gamma = 2||f||_{\Gamma_K} > ||f||_{\Gamma_K}$, we have that

$$\int \Gamma_K(f/\gamma) =$$

$$\int \left(e^{|f/\gamma|^2} - 1\right) \cdot \mathbb{I}_{|\frac{f}{\gamma}| \leq K} + \int \left(e^{K^2} f^2/\gamma^2 + e^{K^2}(1 - K^2) - 1\right) \cdot \mathbb{I}_{|\frac{f}{\gamma}| \geq K} \leq 1. \quad (5.2)$$

Since this is a sum of two non-negative quantities, this implies

$$\int \left(e^{|f/\gamma|^2} - 1\right) \cdot \mathbb{I}_{|\frac{f}{\gamma}| \leq K} \leq 1.$$

This is equivalent to:

$$\int e^{|f_1/\gamma|^2} - 1 \leq 1,$$

and so $||f_1||_{\mathcal{G}} \leq \gamma \ll ||f||_{\Gamma_K}$.

Again considering (5.2), we also have

$$\int \left(e^{K^2} f^2/\gamma^2 + e^{K^2}(1 - K^2) - 1\right) \cdot \mathbb{I}_{|\frac{f}{\gamma}| \geq K} \leq 1.$$

We let $\mu\left(\left|\frac{f}{\gamma}\right| \geq K\right)$ denote the measure of the set in $\mathbb{T}$ on which $|\frac{f}{\gamma}| \geq K$. We can then rewrite the above as:

$$\mu\left(\left|\frac{f}{\gamma}\right| \geq K\right)(e^{K^2}(1-K^2)-1) + \int e^{K^2} f_2^2/\gamma^2 \leq 1. \tag{5.3}$$

Now, since $\int \Gamma_K(f/\gamma) \leq 1$ and $\Gamma_K(f/\gamma) \geq e^{K^2}-1$ whenever $|f/\gamma| \geq K$, we must have

$$\mu\left(\left|\frac{f}{\gamma}\right| \geq K\right)(e^{K^2}-1) \leq 1.$$

Thus, $\mu\left(\left|\frac{f}{\gamma}\right| \geq K\right) \leq \frac{1}{e^{K^2}-1}$. Combining this with (5.3), we have

$$\int e^{K^2} f_2^2/\gamma^2 \leq 1 + \mu\left(\left|\frac{f}{\gamma}\right| \geq K\right)(e^{K^2}(K^2-1)+1) \ll K^2,$$

and hence

$$||f_2||_{L^2}^2 \ll K^2 e^{-K^2}\gamma^2,$$

implying that $||f_2||_{L^2} \ll e^{-cK^2}||f||_{\Gamma_K}$ for some universal constant $c > 0$.

□

5.3 Probabilistic Methods

In this section we establish the following result.

Proposition 84. For N fixed, let $\{\phi_n(x)\}_{n=1}^N$ be an ONS. Define for each $1 \leq m \leq N$ the function $\Gamma_* := \Gamma_{\sqrt{\frac{2}{5}\log\left(\frac{N}{m}\log(\frac{N}{m}+1)\right)}}$ (the dependence on m is implicit in this notation). There exists an orthogonal transformation $O = \{o_{i,n}\}_{1\leq i,n\leq N}$ such that the corresponding base change of $\{\phi_n\}_{n=1}^N$, that is

$$\psi_n(x) := \sum_{i=1}^N o_{i,n}\phi_n(x),$$

satisfies the following. For each m in the range $1 \leq m \leq N$,

$$\left|\left|\sum_{n=1}^{N} a_n \psi_n\right|\right|_{\Gamma_*} \ll \left(\sum_{n=1}^{N} a_n^2\right)^{1/2}$$

for all vectors $\mathbf{a} \in \mathbb{R}^N$ such that $\mathbf{support}(\mathbf{a}) \leq m$. (We use $\mathbf{support}(\mathbf{a})$ to denote the number of nonzero coordinates of $\mathbf{a}$.)

We start by establishing a weaker result. For a fixed m in the range $1 \leq m \leq N$, we let $\mathbb{S}_m \subset \mathbb{R}^N$ denote the subset of vectors $\mathbf{b}$ such that $||\mathbf{b}||_2 \leq 1$ and $\text{support}(\mathbf{b}) \leq m$. We then define

$$B(\mathcal{O}) := \sup_{\mathbf{a} \in \mathbb{S}_m} ||\sum_{n=1}^{N} a_n \psi_n||_{\Gamma_*}.$$

Note that both the set $\mathbb{S}_m$ and the function $\Gamma_* := \Gamma_{\sqrt{\frac{2}{5}\log\left(\frac{N}{m}\log(\frac{N}{m})\right)}}$ depend on m. Our first step will be to establish the following:

Proposition 85. For any $1 \leq m \leq N$ we have that

$$\mathbb{E}_{\mathcal{O}(N)} B(O) \ll 1.$$

This does not quite give Proposition 84, since there it is claimed that there exists an $O \in \mathcal{O}(N)$ that satisfies the conclusion above for all m simultaneously. This stronger claim, however, will be deduced later from the above statement using the concentration of measure phenomenon on the Orthogonal group.

We will need the following result. This is Lemma 5.5 from [4]. There it is attributed to [2]. The result is a concatenation of Lemma 1.10 and 1.12 in [2]. These were both previously known, and are due to [8] and [42], respectively.

Lemma 86. Let X and Y be Banach spaces and consider the operator

$$T_O := \sum_{i,j=1}^{N} o_{ij}(x_i^* \otimes y_i)$$

for $O := (o_{ij})_{1\leq i,j\leq N} \in O(N)$, and where $\{x_i^*\}_{i=1}^N$ (respectively $\{y_i\}_{j=1}^N$) are sequences in X^* (respectively Y). Then,

$$\int_{\emptyset(N)} ||T_O|| \leq$$

$$\frac{C\alpha(\{x_i^*\}_{i=1}^N)}{\sqrt{N}} \int \left|\left|\sum_{j=1}^{N} g_j(\omega)y_j\right|\right| d\omega + \frac{C\alpha(\{y_i\}_{i=1}^N)}{\sqrt{N}} \int \left|\left|\sum_{i=1}^{N} g_i(\omega)x_i^*\right|\right| d\omega \quad (5.4)$$

where

$$\alpha(\{x_i^*\}) := \sup\{(\sum |\langle x_i^*, x\rangle|^2)^{1/2} : x \in X, ||x|| \leq 1\}$$

$$\alpha(\{y_j\}) := \sup\{(\sum |\langle y_i, y^*\rangle|^2)^{1/2} : y^* \in Y^*, ||y^*|| \leq 1\}$$

and $\{g_i\}_{i=1}^N$ is a system of independent Gaussians with mean zero and variance one. Note that the norms in (5.4) refer respectively to the Banach spaces $B(X,Y)$, Y, and X^*.

Let $\ell^2[N]$ denote the set of real sequences $\mathbf{a} := \{a_n\}_{n=1}^N$. We will denote by X the Banach space obtained by considering this set with the norm $||\cdot||_{[m]}$ defined as follows. For a vector $\mathbf{a}$, we define $||\mathbf{a}||_{[m]}$ to be the infimum of positive $c \in \mathbb{R}$ such that scaling the convex hull of $\mathbb{S}_m$ by c results in a set containing $\mathbf{a}$. We take Y to be the space of real-valued functions on $\mathbb{T}$ equipped with the Orlicz norm associated to Γ_*.

Let x_i^* $(1 \leq i \leq N)$ denote the canonical unit vectors in $\mathbb{R}^N$ (which is naturally identified with the dual space X^*). We have, from Lemma 86, that

$$\mathbb{E}B(\mathcal{O}) \ll \frac{\alpha(\{x_i^*\}_{i=1}^N)}{\sqrt{N}}\mathbb{E}||\sum g_i\phi_i||_{\Gamma_*} + \frac{\alpha(\{\phi_i\}_{i=1}^N)}{\sqrt{N}}\mathbb{E}||\sum g_i x_i^*||_{X^*}.$$

In order to establish Proposition 85, we need to show the above is $\ll 1$. This follows from the following estimates:

$$\alpha(\{x_i^*\}_{i=1}^N) \ll 1,$$
$$\alpha(\{\phi_i\}_{i=1}^N) \ll \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5},$$
$$\mathbb{E}||\sum g_i\phi_i||_{\Gamma_*} \leq \sqrt{N},$$
$$\mathbb{E}||\sum g_i x_i^*||_{X^*} \leq \sqrt{m}\sqrt{\log\left(\frac{N}{m}+1\right)}.$$

The first estimate above follows from the observation that the convex hull of $\mathbb{S}_m$ is contained in the ℓ^2 unit ball in $\mathbb{R}^N$. We will prove the others in the following lemmas.

Lemma 87. We have that $\mathbb{E}||\sum g_i\phi_i||_{\Gamma_*} \ll \sqrt{N}$

Proof. Recall that $\mathbb{E}e^{(\sum a_i g_i)^2} \ll \sqrt{\sum a_i^2}$. Thus (by Fubini's theorem) we have $\mathbb{E}\int e^{(\sum g_i\phi_i(x))^2}dx \ll \int\sqrt{\sum\phi_i^2(x)} \ll N^{1/2}$. Since $e^{f^2/\lambda} \leq 1 + \frac{e^{f^2}}{\lambda}$ for $\lambda \geq 1$, we have that $\inf_{\lambda\in\mathbb{R}^+}\left\{\int e^{|f/\lambda|^2} \leq 2\right\} \ll 1 + \int e^{|f|^2}$. Thus we can upperbound $\mathbb{E}||\sum g_i\phi_i||_{\Gamma_*}$ by

$$\mathbb{E}\inf_{\lambda\in\mathbb{R}^+}\left\{\int e^{|\sum a_i\phi_i(x)/\lambda|^2} \leq 2\right\} \ll \mathbb{E}(1 + \int e^{(\sum a_i\phi_i(x))^2})dx \ll \sqrt{N}.$$

□

Lemma 88. We have that $\alpha(\{\phi_i\}_{i=1}^n) \ll \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5}$

Proof. From Lemma 82 it follows that $||f||_{\Gamma_*} \leq \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5}||f||_{L^2}$. Now

$$||g||_{\Gamma_*^*} = \sup_{f\in\Gamma_*}\frac{\langle f,g\rangle}{||f||_{\Gamma_*}} \geq \frac{\langle g,g\rangle}{||g||_{\Gamma_*}} \gg \frac{||g||_2^2}{\left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5}||g||_2}$$
$$\gg \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{-1/5}||g||_2.$$

Here we have used that the each element of the dual space Γ_*^* can be represented as by integration against a measurable function. This follows from standard properties of Orlicz spaces. In particular, see Theorem 14.2 of [35] since the modulus Γ_* satisfies the Δ_2 condition.

It now follows that if $||f||_{\Gamma_*} \leq 1$ then $||f||_2 \ll \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5}$. Thus by Bessel's inequality we have

$$\alpha(\{\phi_j\}) := \sup\{(\sum |\langle\phi_i,g\rangle|^2)^{1/2} : g\in\Gamma_*^*, ||g||_{\Gamma_*^*}\leq 1\} \ll \left(\frac{N}{m}\log\left(\frac{N}{m}+1\right)\right)^{1/5}$$

which completes the proof. □

Lemma 89. We have that $\mathbb{E}||\sum g_i x_i^*||_{X^*} \leq \sqrt{m}\sqrt{\log\left(\frac{N}{m}+1\right)}$

Proof. It follows from the definition of X^* that

$$\mathbb{E}\left|\left|\sum g_i x_i^*\right|\right|_{X^*} = \mathbb{E}\sup_{\mathbf{a}\in\mathbb{S}_m}\left|\sum g_i a_i\right|.$$

(Note that taking the supremum over the convex hull of $\mathbb{S}_m$ would yield the same result.)

The latter quantity is well studied in the theory of Gaussian processes. Recall that Dudley's bound gives

$$\ll \int_0^\infty \sqrt{\log\left(\mathcal{N}(\mathbb{S}_m, \epsilon)\right)} d\epsilon,$$

where $\mathcal{N}(\mathbb{S}_m, \epsilon)$ denotes the number of ℓ^2 balls of radius ϵ needed to cover $\mathbb{S}_m$. Now clearly $\mathbb{S}_m$ is a subset of the n-dimensional ℓ^2 unit ball, thus $\log\left(\mathcal{N}(\mathbb{S}_m, \epsilon)\right) = 0$ for $\epsilon \geq 1$, and the above quantity is equal to

$$\int_0^1 \sqrt{\log\left(\mathcal{N}(\mathbb{S}_m, \epsilon)\right)} d\epsilon.$$

Lemma 89 now follows from the following:

Lemma 90. For $0 \leq \epsilon \leq 1$ we have that

$$\mathcal{N}(\mathbb{S}_m, \epsilon) \ll \binom{N}{m} \left(\frac{3}{\epsilon}\right)^m$$

and thus

$$\log \mathcal{N}(\mathbb{S}_m, \epsilon) \ll m \log\left(\frac{N}{m} + 1\right) + m \log\left(\frac{3}{\epsilon}\right).$$

Proof. We use the well known fact that if K is a symmetric set in $\mathbb{R}^m$ then $\mathcal{N}'(K, \epsilon K) \leq \left(\frac{3}{\epsilon}\right)^m$, where $\mathcal{N}'(K, \epsilon K)$ denotes the number of translates of ϵK needed to cover K.

Fix m coordinates and consider the m-dimensional ℓ^2 ball. We can thus use the above to bound the covering numbers of this ball. Lastly, we sum over all $\binom{N}{m}$ such balls. □

This completes the proof of Lemma 89 and hence the proof of Proposition 85. □

5.3.1 Concentration of Measure on $\mathcal{O}(n)$

In the prior section, we proved that for any $1 \leq m \leq N$ we have $\mathbb{E}_{\mathcal{O}(N)} B(O) \ll 1$. It follows from Markov's inequality that for some large universal C, we have $\mu(\mathcal{A}(m)) \geq \frac{1}{2}$, where

$$\mathcal{A}(m) := \{O \in \mathcal{O}(N) : B(O) \leq C\}$$

and $\mu(\mathcal{A}(m))$ denotes the measure of the set $\mathcal{A}(m)$ in $\mathcal{O}(N)$.

Consider the Hilbert-Schmidt norm on the set of $N \times N$ matrices, $||A||_{\text{HS}} := \left(\sum_{1 \leq i,j \leq N} |A_{i,j}|^2\right)^{1/2}$. We note (see [4] Lemma 5.11):

Lemma 91. Let μ denote the Haar measure on the orthogonal group $O(N)$ and $A \subset O(N)$ such that $\mu(A) > \frac{1}{2}$. Then,

$$\mathbb{P}\left[A \in O(N) : \inf_{B \in A_c} ||A - B||_{\text{HS}} > \epsilon\right] \ll e^{-c\epsilon^2 N}$$

for some absolute positive constant c.

For any $N \times N$ matrix M, using the bounds from Lemma 82 we have

$$\begin{aligned} \left|\left|\sum_{1 \leq i,n \leq N} m_{i,n} a_i \phi_n\right|\right|_{\Gamma_*} &\ll \left(\frac{N}{m} \log\left(\frac{N}{m}\right)\right)^{1/5} \left(\sum_n \left(\sum_i m_{i,n} a_i\right)^2\right)^{1/2} \\ &\ll \left(\frac{N}{m} \log\left(\frac{N}{m}\right)\right)^{1/5} ||M||_{HS} ||\mathbf{a}||_{\ell^2}. \end{aligned} \tag{5.5}$$

for all $\mathbf{a} \in \mathbb{R}^N$. The final inequality follows from Cauchy-Schwartz.

Now consider $\mathcal{A}(m, \epsilon) \subset \mathcal{O}(N)$, defined to be the set of all orthogonal matrices that differ from an element of $\mathcal{A}(m)$ by a matrix with Hilbert-Schmidt

norm at most ϵ. Using (5.5), we have that for $O \in \mathcal{A}\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)$ we have $B(O) \leq C'$, where C' is a new absolute constant. On the other hand, denoting the complement of $\mathcal{A}\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)$ by $\mathcal{A}^c\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)$, by Lemma 91 we have

$$\mathbb{P}\left[O \in \mathcal{A}^c\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)\right] \ll e^{-cN^{2/5}}$$

for some positive constant c.

Now to conclude the proof of Proposition 84, it suffices to find a $O \in \mathcal{O}(N)$ such that for every $1 \leq m \leq N$ we have $O \in \mathcal{A}\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)$. However, for sufficiently large N, we see from the union bound that $\mu\left(\bigcup_{1\leq m\leq N} \mathcal{A}^c\left(m, \left(\frac{m}{N\log(\frac{N}{m})}\right)^{1/5}\right)\right) \leq Ne^{-cN^{2/5}} \leq 1$. This completes the proof of Proposition 84.

5.4 Maximal function decomposition

Proposition 92. For N fixed, let $\{\phi_n(x)\}_{n=1}^N$ be an ONS. There exists an orthogonal matrix O such that the associated system $\Psi(O) = \{\psi_n\}_{n=1}^N$ satisfies the following property. For any $f = \sum a_n\psi_n$, letting m denote support$(\{a_n\})$, we have that the maximal function defined by

$$\mathcal{M}f := \sup_{I\subseteq[N]}\left|\sum_{n\in I} a_n\psi_n\right|$$

can be decomposed as $\mathcal{M}f := \tilde{G} + \tilde{E}$ where $||\tilde{G}||_{\mathcal{G}(c)} \ll ||f||_2$ for some universal constant $c > 0$ and $||\tilde{E}||_2 \ll \left(\frac{m}{N}\right)^{c'} ||f||_2$ for some universal constant $c' > 0$.

To prove this, we fix O as in Proposition 84. We now decompose $[N]$ into a family of subintervals according to a concept of mass defined with respect to the a_i values. We define the *mass* of a subinterval $I \subseteq [N]$ as $M(I) := \sum_{n \in I} |a_n|^2$. By normalization, we may assume that $M([N]) = 1$. We define $I_{0,1} := [N]$ and we iteratively define $I_{k,s}$, for $1 \leq s \leq 2^k$, as follows. Assuming we have already defined $I_{k-1,s}$ for all $1 \leq s \leq 2^{k-1}$, we will define $I_{k,2s-1}$ and $I_{k,2s}$, which are subintervals of $I_{k-1,s}$. $I_{k,2s-1}$ begins at the left endpoint of $I_{k-1,s}$ and extends to the right as far as possible while covering strictly less than half the mass of $I_{k-1,s}$, while $I_{k,2s}$ ends at the right endpoint of $I_{k-1,s}$ and extends to the left as far as possible while covering at most half the mass of $I_{k-1,s}$. More formally, we define $I_{k,2s-1}$ as the maximal subinterval of $I_{k-1,s}$ which contains the left endpoint of $I_{k-1,s}$ and satisfies $M(I_{k,2s-1}) < \frac{1}{2} M(I_{k-1,s})$. We also define $I_{k,2s}$ as the maximal subinterval of $I_{k-1,s}$ which contains the right endpoint of $I_{k-1,s}$ and satisfies $M(I_{k,2s}) \leq \frac{1}{2} M(I_{k-1,s})$. We note that these subintervals are disjoint. We may express $I_{k-1,s} = I_{k,2s-1} \bigcup I_{k,2s} \bigcup i_{k,s}$, where $i_{k,s} \in I_{k-1,s}$. In other words, $i_{k,s}$ denotes the single element which lies between $I_{k,2s-1}$ and $I_{k,2s}$ (note that such a point always exists because we have required that $I_{k,2s-1}$ contains strictly less than half of the mass of the interval). Here it is acceptable, and in many instances necessary, for some choices of the intervals in this decomposition to be empty. By construction we have that

$$M(I_{k,s}) \leq 2^{-k}. \tag{5.6}$$

We call an interval $J \subseteq [N]$ admissible if it is an element of the decom-

position given above. We denote the collection of admissible intervals by $\mathcal{A}$. We additionally refer to the subset $\{I_{k,s}|1 \leq s \leq 2^k\}$ of $\mathcal{A}$ as the admissible intervals on level k and the subset $\{i_{k,s}|1 \leq s \leq 2^k\}$ as the admissible points on level k. We note that every point in $[N]$ is an admissible point on some level. (Eventually, we have subdivided all intervals down to being single elements.)

Now we write $\mathcal{I}_k := \{I_{k,s} : 1 \leq s \leq 2^k\}$. We decompose this as $\mathcal{I}_k^a := \{I \in \mathcal{I}_k : |I| \leq 2^{-k/2}N\}$ and its complement, $\mathcal{I}_k^b := \{I \in \mathcal{I}_k : |I| > 2^{-k/2}N\}$. Here, $|I|$ denotes the number of nonzero a_i values contained in an interval I.

For $J \subseteq [N]$, we define

$$S_J(x) = \sum_{n \in J} a_n \psi_n(x).$$

We also define

$$\tilde{S}_J(x) := \max_{I \subseteq J} \left| \sum_{n \in I} a_n \psi_n(x) \right|.$$

From Lemma 83 and Proposition 84, we deduce that $S_J = G_J + E_J$ where $||G_J||_{\mathcal{G}} \ll ||S_J||_2$ and $||E_J||_2 \ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2$ for some positive constant c'. Our purpose now is to show a similar decomposition for $\tilde{S}_J(x)$. Clearly, it suffices to show such a decomposition for a pointwise majorant. Denote the decomposition of $S_{I_{k,s}}$ by $S_{I_{k,s}} := G_{k,s} + E_{k,s}$, and the decomposition of $S_{i_{k,s}}$ by $S_{i_{k,s}} := G_{i_{k,s}} + E_{i_{k,s}}$. Setting $r = 3$, for an interval J we have the following bound, where the sums below are restricted to values of k, s such that $I_{k,s}, i_{k,s} \subseteq J$:

$$\tilde{S}_J(x) \ll \sum_k \left(\sum_s |G_{k,s} + E_{k,s}|^r \right)^{1/r} + \sum_k \left(\sum_s |G_{i_{k,s}} + E_{i_{k,s}}|^r \right)^{1/r}$$

$$\ll \left(\sum_k \left(\sum_s |G_{k,s}|^r\right)^{1/r} + \sum_k \left(\sum_s |G_{i_{k,s}}|^r\right)^{1/r}\right)$$
$$+ \left(\sum_k \left(\sum_s |E_{k,s}|^r\right)^{1/r} + \sum_k \left(\sum_s |E_{i_{k,s}}|^r\right)^{1/r}\right) =: \tilde{G}_J + \tilde{E}_J. \quad (5.7)$$

This follows from the observation that for each point x, the maximizing subinterval $I \subseteq J$ can be decomposed as a union of admissible intervals and points with at most two intervals and points on each level. The contribution on each level can then be bounded by a constant times the contribution from the "worst" interval/point, which is in turn bounded by the quantity inside the sum over k above for each level k.

For an admissible interval J, we let k^* denote the level of J. We note that the sums over k in (5.7) range only over $k \geq k^*$ (and the sums over s are also appropriately restricted). Next we show that $||\tilde{G}_J||_{\mathcal{G}(c)} \ll ||S_J||_2$ for some absolute constant c and $||\tilde{E}_J||_2 \ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2$.

Now let us estimate $||\tilde{E}_J||_2$. We first estimate the contribution from the admissible points $i_{k,s} \in J$. We observe

$$\left|\left|\sum_k \left(\sum_s |E_{i_{k,s}}|^r\right)^{\frac{1}{r}}\right|\right|_2 \leq \sum_k \left|\left|\left(\sum_s |E_{i_{k,s}}|^r\right)^{\frac{1}{r}}\right|\right|_2.$$

Since $r > 2$, this is

$$\leq \sum_k \left(\sum_s ||E_{i_{k,s}}||_2^2\right)^{\frac{1}{2}} \ll \left(\frac{1}{N}\right)^{c'} \sum_k \left(\sum_s ||S_{i_{k,s}}||_2^2\right)^{\frac{1}{2}},$$

where the latter inequality follows from the definition of $E_{i_{k,s}}$.

Now since these sums only range over values of k, s such that $i_{k,s} \in J$, we may split the sum over k into two portions as:

$$\sum_k \left(\sum_s ||S_{i_{k,s}}||_2^2 \right)^{\frac{1}{2}}$$

$$= \sum_{k=k^*}^{k^*+10\log(N)} \left(\sum_s ||S_{i_{k,s}}||_2^2 \right)^{\frac{1}{2}} + \sum_{k>k^*+10\log(N)} \left(\sum_s ||S_{i_{k,s}}||_2^2 \right)^{\frac{1}{2}}. \qquad (5.8)$$

To bound the first quantity in (5.8), it suffices to observe that the inner quantity for each k is at most 1, and hence its contribution is $\ll \log(N) \ll N^{-\epsilon}$, for a constant $\epsilon < c'$. (Thus we will adjust the value of c' for our final estimate by subtracting ϵ.)

To bound the second quantity in (5.8), we note that for any $i_{k,s} \in J$ with $k > k^* + 10\log(N)$, we have $||S_{i_{k,s}}||_2^2 \leq N^{-10}||S_J||_2^2$. There are at most N points $i_{k,s}$ in the sum, and thus

$$\sum_{k>k^*+10\log(N)} \left(\sum_s ||S_{i_{k,s}}||_2^2 \right)^{\frac{1}{2}} \ll N^{-4}||S_J||_2.$$

To estimate the contribution from the admissible intervals, we proceed as follows. For each $k \geq k^*$, we define $I_k^a(J)$ to be the set of admissible intervals I on level k contained in J such that $|I| < 2^{-(k-k^*)/2}|J|$ and we let $I_k^b(J)$ denote the set of remaining admissible intervals on level k contained in J. Note that $I_k^a(J)$ and $I_k^b(J)$ are disjoint, and their union is the set of all admissible intervals on level k contained in J. It thus suffices to estimate

$$\tilde{E}_J^a + \tilde{E}_J^b := \sum_{k \geq k^*} \left(\sum_{I_{k,s} \in I_k^a(J)} |E_{k,s}|^r \right)^{1/r} + \sum_k \left(\sum_{I_{k,s} \in I_k^b(J)} |E_{k,s}|^r \right)^{1/r}.$$

Now $|I_k^b(J)| \leq 2^{(k-k^*)/2}$, and we also have

$$||E_{k,s}||_2 \ll \left(\frac{|J|}{N}\right)^{c'} ||S_{k,s}||_2 \ll \left(\frac{|J|}{N}\right)^{c'} 2^{-(k-k^*)/2} ||S_J||_2.$$

Since $r > 2$, we have:

$$\left|\left|\sum_{k\geq k^*} \left(\sum_{s\in I_k^b(J)} |E_{k,s}|^r\right)^{1/r}\right|\right|_2 \leq \sum_{k\geq k^*} \left(\sum_{s\in I_k^b(J)} ||E_{k,s}||_2^2\right)^{1/2}$$

$$\ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2 \sum_{j\geq 0} 2^{-j/4} \ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2.$$

Next, we recall that $I \in I_k^a(J)$ implies $|I| \ll 2^{-(k-k^*)/2}|J|$. We have $||S_{I_{k,s}}||_2 \ll 2^{-(k-k^*)/2}||S_J||_2$, thus $||E_{k,s}||_2 \ll \left(\frac{|J|}{N}\right)^{c'} 2^{-c'(k-k^*)/2}||S_{I_{k,s}}||_2 \ll \left(\frac{|J|}{N}\right)^{c'} 2^{-(c'+1)(k-k^*)/2}||S_J||_2$.

We then have

$$\left|\left|\sum_{k\geq k^*} \left(\sum_{I_{k,s}\in I_k^a(J)} |E_{k,s}|^r\right)^{1/r}\right|\right|_2 \leq \sum_{k\geq k^*} \left(\sum_{I_{k,s}\in I_k^a(J)} ||E_{k,s}||_2^2\right)^{1/2}$$

$$\ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2 \sum_{k\geq k^*} 2^{k-k^*} 2^{-(c'+1)(k-k^*)} \ll \left(\frac{|J|}{N}\right)^{c'} ||S_J||_2.$$

Here we have used the fact that there are at most 2^{k-k^*} values of s such that $I_{k,s} \subseteq J$ for each $k \geq k^*$. (one also needs to deal with the individual points, but this is easy). We can apply this for $J = [N]$ in particular, recalling that $|J|$ denotes the number of nonzero a_i values contained in J, which in this case is m. This completes the proof that $||\tilde{E}||_2 \ll \left(\frac{m}{N}\right)^{c'} ||f||_2$ for some positive constant c'.

To show that $||\tilde{G}||_{\mathcal{G}(c)} \ll ||f||_2$ for some universal constant $c > 0$, we will use the following lemma. These implications and arguments are well-known, however we include a proof for completeness.

Lemma 93. Let A denote a fixed, positive constant. For positive constants c, C, we define the following sets of measurable functions:

$$S_1(c) := \{f : \mathbb{T} \to \mathbb{C} \text{ s.t. } ||f||_p \leq c\sqrt{p}A \ \ \forall p \geq 2\},$$

$$S_2(c, C) := \{f : \mathbb{T} \to \mathbb{C} \text{ s.t. } \mu(|f| \geq \lambda) \leq Ce^{-c\frac{\lambda^2}{A^2}} \ \ \forall \lambda \geq 0\},$$

$$S_3(c) := \{f : \mathbb{T} \to \mathbb{C} \text{ s.t. } ||f||_{\mathcal{G}(c)} \leq A\},$$

where $\mu(|f| \geq \lambda)$ denotes the Lebesgue measure of the subset of $x \in \mathbb{T}$ such that $|f(x)| \geq \lambda$. Then for any $c > 0$, there exist positive constants c', C', c'' (depending only on c) such that $S_1(c) \subseteq S_2(c', C')$ and $S_1(c) \subseteq S_3(c'')$. Similarly, for any $c, C > 0$, there exist positive constants c', c'' (depending only on c, C) such that $S_2(c, C) \subseteq S_1(c')$ and $S_2(c, C) \subseteq S_3(c)$. Finally, for any $c < 0$, there exist positive constants c', C', c'' (depending only on c) such that $S_3(c) \subseteq S_2(c', C')$ and $S_3(c) \subseteq S_1(c'')$.

Proof. Fixing c, C, we will determine c' such that $S_2(c, C) \subseteq S_3(c')$ (for every A). We consider an $f \in S_2(c, C)$. We consider $c' := d_1 d_2$ as a product of two variables d_1, d_2 whose values will be set later. We assume $d_1 \leq 1$. We have:

$$\int_{\mathbb{T}} e^{c'|f|^2/A^2} = \int_{\mathbb{T}} e^{d_1 d_2 |f|^2/A^2} \leq 1 + d_1 \int_{\mathbb{T}} e^{d_2|f|^2/A^2}, \tag{5.9}$$

using the inequality $e^{x/a} \leq \frac{1}{a}e^x + 1$ for all $a \geq 1$ and non-negative x (this can be seen by considering the Taylor expansion of e^x).

Now, we observe that

$$\int_{\mathbb{T}} e^{d_2|f|^2/A^2} \leq \sum_{k\geq 0} \int_{\mathbb{T}} e^{d_2|f|^2/A^2} \cdot 1_{A^2k\leq|f|^2<A^2(k+1)} \leq \sum_{k\geq 0} \mu(|f|^2 \geq A^2k) e^{d_2(k+1)},$$

where $1_{A^2k\leq|f|^2<A^2(k+1)}$ denotes the characteristic function of the set on which $|f|^2$ takes values between A^2k and $A^2(k+1)$. Since $f \in S_2(c, C)$, we have $\mu(|f|^2 \geq A^2k) \leq Ce^{-ck}$ for all $k \geq 0$. Thus, we conclude

$$\int_{\mathbb{T}} e^{d_2|f|^2/A^2} \leq \sum_{k\geq 0} Ce^{-ck+d_2(k+1)} = Ce^{d_2} \sum_{k\geq 0} e^{-(c-d_2)k} = \frac{Ce^c}{e^{c-d_2}-1}.$$

We set $d_2 = c/2$ and obtain $\leq Ce^c/(e^{c/2}-1)$. Letting $d_1 = \min\left\{1, \frac{e^{c/2}-1}{Ce^c}\right\}$, we have

$$d_1 \int_{\mathbb{T}} e^{d_2|f|^2/A^2} \leq 1,$$

and hence $\int_{\mathbb{T}} e^{c'|f|^2/A^2} - 1 \leq 1$ for $c' = d_1d_2$, showing that $f \in S_3(c')$. Note that $c' = d_1d_2$ depends only on c and C.

Conversely, we observe that for every $c > 0$, $S_3(c) \subseteq S_2(c, 2)$. To see this, consider $f \in S_3(c)$. Then we have

$$\int_{\mathbb{T}} e^{c|f|^2/A^2} - 1 \leq 1 \Rightarrow \int_{\mathbb{T}} e^{c|f|^2/A^2} \leq 2.$$

Thus for any $\lambda > 0$,

$$\mu(|f| \geq \lambda) e^{c\lambda^2/A^2} \leq \int_{\mathbb{T}} e^{c|f|^2/A^2} \leq 2.$$

It follows that $f \in S_2(c, 2)$.

For any $c > 0$, we will now show there exist c', C such that $S_1(c) \subseteq S_2(c', C)$ (for every A). We consider an $f \in S_1(c)$. This means that $||f||_p^p \leq$

$c^p p^{\frac{p}{2}} A^p$ for all $p \geq 2$. Thus, for every $\lambda > 0$, $\mu(|f| \geq \lambda)\lambda^p \leq (cA)^p p^{\frac{p}{2}}$, which implies

$$\mu(|f| \geq \lambda) \leq \frac{(cA)^p p^{\frac{p}{2}}}{\lambda^p}. \tag{5.10}$$

For a fixed λ, we may minimize this quantity over the choices of $p \geq 2$. In the case that $\frac{\lambda^2}{ec^2A^2} \geq 2$, we may set p equal to this value, and the quantity in (5.10) then becomes:

$$\left(\frac{cA}{\lambda}\right)^{\frac{\lambda^2}{ec^2A^2}} \left(\frac{\lambda^2}{ec^2A^2}\right)^{\frac{\lambda^2}{2ec^2A^2}} = e^{-\frac{\lambda^2}{2ec^2A^2}}.$$

Hence by setting $c' = \frac{1}{2ec^2}$, we achieve $\mu(|f| \geq \lambda) \leq e^{-c'\lambda^2/A^2}$ in these cases.

Now, when $\frac{\lambda^2}{ec^2A^2} < 2$, we note that $e^{-c'\lambda^2/A^2} \geq e^{-c'(2ec^2)} = e^{-1}$. Thus, setting $C = e$, we have $\mu(|f| \geq \lambda) \leq 1 \leq Ce^{-c'\lambda^2/A^2}$ in these cases. Hence, in all cases we have that

$$\mu(|f| \geq \lambda) \leq Ce^{-c'\lambda^2/A^2},$$

so $f \in S_2(c', C)$.

Conversely, for any $c, C > 0$, we will show there exists c' such that $S_2(c, C) \subseteq S_1(c')$ for every A. We consider an $f \in S_2(c, C)$. Then for every $\lambda \geq 0$, we have $\mu(|f| \geq \lambda) \leq Ce^{-c\frac{\lambda^2}{A^2}}$. We fix $p \geq 2$. We observe:

$$||f||_p^p = p\int_0^\infty \lambda^{p-1}\mu(|f| > \lambda)d\lambda \ll p\int_0^\infty \lambda^{p-1}e^{-c\lambda^2/A^2}d\lambda.$$

Substituting $\lambda = t^{\frac{1}{p}}$, we see this equals

$$\int_0^\infty e^{-ct^{\frac{2}{p}}/A^2}dt. \tag{5.11}$$

We note that identity $\frac{p}{2}\Gamma\left(\frac{p}{2}\right) = \int_0^\infty e^{-s^{\frac{2}{p}}} ds$ where Γ denotes the function $\Gamma(z) := \int_0^\infty y^{z-1}e^{-y}dy$. Setting $s = \left(\frac{c}{A^2}\right)^{\frac{p}{2}} t$, we see that the quantity in (5.11) is

$$= c^{-\frac{p}{2}} A^p \int_0^\infty e^{-s^{\frac{2}{p}}} ds = c^{-\frac{p}{2}} A^p \left(\frac{p}{2}\right) \Gamma\left(\frac{p}{2}\right).$$

By Sterling's formula, $\Gamma\left(\frac{p}{2}\right) \ll p^{-1/2}\left(\frac{p}{2e}\right)^{\frac{p}{2}}$. Hence,

$$||f||_p \ll A\sqrt{p}\left(p^{\frac{1}{2p}}\right) \ll A\sqrt{p},$$

as required.

□

Appealing to Lemma 93, we see that we may bound the quantity $||\tilde{G}_J||_{\mathcal{G}(c)}$ by considering the p norm. We recall that

$$\tilde{G}_J = \sum_k \left(\sum_s |G_{k,s}|^r\right)^{1/r} + \sum_k \left(\sum_s |G_{i_{k,s}}|^r\right)^{1/r},$$

where the sums are restricted to values of k, s such that $I_{k,s}, i_{k,s} \subseteq J$. We let k^* again denote the level of J, so we are only summing over values $k \geq k^*$.

We have

$$\left|\left|\sum_k \left(\sum_s |G_{k,s}|^r\right)^{1/r} + \sum_k \left(\sum_s |G_{i_{k,s}}|^r\right)^{1/r}\right|\right|_p$$

$$\leq \sum_k \left|\left|\left(\sum_s |G_{k,s}|^r\right)^{1/r}\right|\right|_p + \sum_k \left|\left|\left(\sum_s |G_{i_{k,s}}|^r\right)^{1/r}\right|\right|_p$$

by the triangle inequality, and this is

$$= \sum_k \left|\left| \sum_s |G_{k,s}|^r \right|\right|_{\frac{p}{r}}^{\frac{1}{r}} + \sum_k \left|\left| \sum_s |G_{i_{k,s}}|^r \right|\right|_{\frac{p}{r}}^{\frac{1}{r}}$$

$$\leq \sum_k \left(\sum_s |||G_{k,s}|^r||_{\frac{p}{r}} \right)^{\frac{1}{r}} + \sum_k \left(\sum_s \left|\left||G_{i_{k,s}}|^r\right|\right|_{\frac{p}{r}} \right)^{\frac{1}{r}}$$

$$= \sum_k \left(\sum_s ||G_{k,s}||_p^r \right)^{\frac{1}{r}} + \sum_k \left(\sum_s ||G_{i_{k,s}}||_p^r \right)^{\frac{1}{r}}$$

by another application of the triangle inequality.

Now, using that $||G_{k,s}||_p \ll \sqrt{p}||S_{I_{k,s}}||_2$ and $||G_{i_{k,s}}||_p \ll \sqrt{p}||S_{i_{k,s}}||_2$ by Lemma 93 and $||S_{I_{k,s}}||_2 \ll ||S_J||_2 2^{-(k-k^*)/2}$ and $||S_{i_{k,s}}||_2 \ll ||S_J||_2 2^{-(k-k^*)/2}$, we have

$$||\tilde{G}_J||_p \leq \sum_{k \geq k^*} \left(\sum_s ||G_{k,s}||_p^r \right)^{1/r} + \sum_{k \geq k^*} \left(\sum_s ||G_{i_{k,s}}||_p^r \right)^{1/r}$$

$$\ll \sqrt{p}||S_J||_2 \sum_{k \geq k^*} \left(\sum_s 2^{-r(k-k^*)/2} \right)^{\frac{1}{r}}.$$

Since the sum of s ranges over at most 2^{k-k^*} values (recall we only include values of s such that $I_{k,s} \subseteq J$) and $r > 2$, this is

$$\ll \sqrt{p}||S_J||_2 \sum_{k \geq k^*} 2^{(k-k^*)(r^{-1}-2^{-1})} \ll \sqrt{p}||S_J||_2.$$

It thus follows from Lemma 93 that

$$||\tilde{G}_J||_{\mathcal{G}(c)} \ll ||S_J||_2$$

for some positive constant c.

5.5 Proof of the Main result

We are now ready to prove:

Theorem 94. Let $\mathcal{P}_N$ be the set of all partitions of $[N]$ into subintervals. Now recall the square variation operator of $f = \sum_{n=1}^{N} a_n \psi_n$

$$\mathcal{V}^2 f = \left(\sup_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \left| \sum_{n \in I} a_n \psi_n \right|^2 \right)^{1/2}.$$

We then have that

$$||\mathcal{V}^2 f||_2 \ll \sqrt{\log\log(N)} ||f||_2.$$

Here we use the mass decomposition (into dyadic subintervals $I_{k,s}$) stated previously. We use the following easily verified fact (see [41], Lemma 29):

Lemma 95. For every $J \subseteq [N]$, $(J \neq \emptyset)$ there exist $\tilde{J}_\ell, \tilde{J}_r \in \mathcal{A}$ and $i_J \in [N]$ such that $\tilde{J} := \tilde{J}_\ell \cup i_J \cup \tilde{J}_r$ is an interval (i.e. J_ℓ, i_J, J_ℓ are adjacent), $J \subseteq \tilde{J}$, and $M(\tilde{J}) \leq 2M(J)$.

Without loss of generality, we set $||f||_2 = 1$, and we have the pointwise inequality

$$|\mathcal{V}^2 f(x)|^2 \ll \sum_{k,s} |\tilde{S}_{I_{k,s}} 1_{B(I_{k,s})}|^2 + \sum_{k,s} |S_{i_{k,s}}|^2 + \log\log(N),$$

where $B(I_{k,s}) \subseteq \mathbb{T}$ is the set such that $|\tilde{S}_{I_{k,s}}(x)|^2 \geq C \log\log(N) M(I_{k,s})$, for a fixed constant C whose value will be chosen to be sufficiently large. Appealing to Proposition 92, for each $I_{k,s}$ we can decompose $\tilde{S}_{I_{k,s}} = \tilde{G}_{I_{k,s}} + \tilde{E}_{I_{k,s}}$. We then

define $B_G(I_{k,s}) \subseteq \mathbb{T}$ by $|\tilde{G}_{I_{k,s}}(x)|^2 \geq \frac{C}{10} \log\log(N) M(I_{k,s})$ and $B_E(I_{k,s}) \subseteq \mathbb{T}$ by $|\tilde{E}_{I_{k,s}}(x)|^2 \geq \frac{C}{10} \log\log(N) M(I_{k,s})$.

Clearly $\int \sum_{k,s} |S_{i_{k,s}}|^2 \leq 1$ is acceptable, so it suffices to show that

$$\int \sum_{k,s} |\tilde{S}_{I_{k,s}} 1_{B(I_{k,s})}|^2 \ll 1.$$

Now appealing to the decomposition above, we have

$$\int \sum_{k,s} |\tilde{S}_{I_{k,s}} 1_{B(I_{k,s})}|^2 \ll \int \sum_{k,s} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2 + \int \sum_{k,s} |\tilde{E}_{I_{k,s}} 1_{B_E(I_{k,s})}|^2.$$

First we estimate

$$\int \sum_{k,s} |\tilde{E}_{I_{k,s}} 1_{B_E(I_{k,s})}|^2 \ll \int \sum_{k,s} |\tilde{E}_{I_{k,s}}|^2.$$

Employing notation previously used above, we let $I_k^a := \{I_{k,s} \text{ s.t. } |I_{k,s}| \leq 2^{-k/2} N\}$ and $I_k^b := \{I_{k,s} \text{ s.t. } |I_{k,s}| > 2^{-k/2} N\}$. Thus $I \in I_k^a$ implies $|I| \leq 2^{-k/2} N$ and $|I_k^b| \leq 2^{k/2}$. We then have

$$\int \sum_{k,s} |\tilde{E}_{I_{k,s}}|^2 = \int \sum_{I_{k,s} \in I_k^a} |\tilde{E}_{I_{k,s}}|^2 + \int \sum_{I_{k,s} \in I_k^b} |\tilde{E}_{I_{k,s}}|^2.$$

Using that $I \in I_k^a$ implies $|I| \leq 2^{-k/2} N$, we have

$\int |\tilde{E}_{I_{k,s}}|^2 \ll 2^{-c'k/2} ||S_{I_{k,s}}||_2^2 \ll 2^{-k-c'k/2}$. Thus

$$\int \sum_{k,s} |\tilde{E}_{I_{k,s}}|^2 \ll \sum_k 2^{-c'k/2} \ll 1.$$

Next, using that $|I_k^b| \leq 2^{k/2}$ and $\int |\tilde{E}_{I_{k,s}}|^2 \ll 2^{-k}$, we have

$$\int \sum_{I_{k,s} \in I_k^b} |\tilde{E}_{I_{k,s}}|^2 \ll \sum_k 2^{-k/2} \ll 1.$$

Finally, we estimate

$$\int \sum_{k,s} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2.$$

We can choose C sufficiently large so that $|B_G(I_{k,s})| \ll \frac{1}{\log^{10}(N)}$ for all k, s. To see this, recall that $||\tilde{G}_{I_{k,s}}||_{\mathcal{G}(c)} \ll \sqrt{M(I_{k,s})}$. By Lemma 93, there exists a constant $c' > 0$ such that

$$\mu\left(|\tilde{G}_{I_{k,s}}| \geq \lambda\right) \ll e^{-c'\lambda^2/M(I_{k,s})}$$

for all $\lambda \geq 0$. Setting $\lambda^2 = \frac{C}{10} \log\log(N) M(I_{k,s})$, we obtain

$$|B_G(I_{k,s})| \ll \log(N)^{-c'C/10}.$$

We can then choose C sufficiently large with respect to c' make this estimate $\ll \frac{1}{\log^{10}(N)}$.

Now we split the sum at $k = 100\log(N)$ so

$$\int \sum_{k,s} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2$$

$$= \int \sum_{\substack{k,s \\ k \geq 100\log(N)}} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2 + \int \sum_{\substack{k,s \\ k < 100\log(N)}} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2.$$

By the Cauchy-Schwarz inequality,

$$\int \sum_{\substack{k,s \\ k < 100\log(N)}} 1_{B_G(I_{k,s})}|^2 \ll \sum_{k,s} ||\tilde{G}_{I_{k,s}}||_4^2 \, ||1_{B_G(I_{k,s})}||_4^2.$$

Now, by Lemma 93, we have $||\tilde{G}_{I_{k,s}}||_4^2 \ll ||S_{I_{k,s}}||_2^2 \ll 2^{-k}$ and, by the previous estimate, $||1_{B_G(I_{k,s})}||_4^2 \ll \frac{1}{\log^5(N)}$. Thus we have shown that the quantity above is

$$\ll \frac{1}{\log^5(N)} \int \sum_{\substack{k,s \\ k<100\log(N)}} ||\tilde{G}_{I_{k,s}}||_4^2 \ll \frac{1}{\log^4(N)} \ll 1.$$

Lastly, let $T \subset [N]$ denote the set of indices appearing in some $I_{k,s}$ for $k \geq 100\log(N)$. Note that any index will appear in at most N such intervals, and that $M(I_{k,s}) \leq N^{-100}$ if $k \geq 100\log(N)$. Thus $|a_n| \ll N^{-50}$ for $n \in T$. Thus we have

$$\int \sum_{\substack{k,s \\ k\geq 100\log(N)}} |\tilde{G}_{I_{k,s}} 1_{B_G(I_{k,s})}|^2 \ll N \int \sum_{n\in T} |a_n \phi_n(x)| \ll N^{-49} \int \sum_{n\in T} |\phi_n(x)| \ll 1.$$

This completes the proof.

Chapter 6

A Variational Barban-Davenport-Halberstam Theorem

6.1 Introduction

The prime number theorem implies the asymptotic $\psi(x) \sim x$, while the Riemann hypothesis predicts a bound of $|\psi(x) - x| \ll_\epsilon x^{\frac{1}{2}+\epsilon}$ on the error term. This extends naturally to arithmetic progressions, where the asymptotic $\psi(x; q, a) \sim \frac{x}{\phi(q)}$ holds for all coprime a and q. We recall that

$$\psi(x; q, a) := \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n).$$

Under the Generalized Riemann hypothesis, one obtains the error bound $\left|\psi(x; q, a) - \frac{x}{\phi(q)}\right| \ll_\epsilon x^{\frac{1}{2}+\epsilon}$. The stronger bound of $\ll_\epsilon x^{\frac{1}{2}+\epsilon}\phi(q)^{-\frac{1}{2}}$ is also conjectured. (For further definitions, see Section 6.2. For background material, see [10].)

An unconditional bound on the averaged error term for this is provided by the Barban-Davenport-Halberstam Theorem [10], which states:

Theorem 96. (Barban-Davenport-Halberstam) Let $A > 0$. For all positive real

numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \left(\psi(x; q, a) - \frac{x}{\phi(q)} \right)^2 \ll_A xQ \log(x).$$

We note that this holds also for the quantity $\theta(x; q, a)$, since the differences between $\psi(x; q, a)$ and $\theta(x; q, a)$ are of lower order.

An even stronger bound is due to Montgomery [45], refining work of Uchiyama [67], (see also the refinement of Hooley [27]):

Theorem 97. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \max_{y \leq x} \sum_{\substack{a \leq q \\ (a,q)=1}} \left(\psi(y; q, a) - \frac{y}{\phi(q)} \right)^2 \ll_A xQ \log(x).$$

We note that the quantity on the left has potentially increased compared to the quantity in Theorem 96, while the bound on the right is the same, up to the implicit constant.

Another variant of Theorem 96 is due to Uchiyama [67]:

Theorem 98. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{y \leq x} \left(\psi(y; q, a) - \frac{y}{\phi(q)} \right)^2 \ll_A xQ \log^3(x).$$

This is incomparable to Theorems 96 and 97, since the quantity being bounded is larger and the bound obtained is worse. Hooley, in [28], has an-

nounced a refinement to the $\log^3(N)$ for certain values of Q. This seems to have not yet appeared, however.

We work with the function θ instead of ψ because it is more convenient for our purposes, though this is a minor difference. To further refine our understanding of the deviation of $\theta(x;q,a)$ from its average value of $\frac{x}{\phi(q)}$, we introduce a variational operator in place of the maximal one in Theorem 98. Letting $\{c_n\}_{n=1}^N$ be a finite sequence of complex numbers and letting $\mathcal{P}_N$ denote the set of partitions of $[N] := \{1, 2, \ldots, N\}$ into disjoint intervals, we define the r-variation of the sequence to be:

$$\left|\left|\{c_n\}_{n=1}^N\right|\right|_{V^r} := \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} c_n \right|^r \right)^{\frac{1}{r}}.$$

We can think of $\theta(x;q,a)$ as a sum over a sequence $\{b_n\}_{n=1}^N$, where $N = \lfloor x \rfloor$ and

$$b_n := \begin{cases} \log(n), & n \text{ prime;} \\ 0, & \text{otherwise.} \end{cases}$$

For an interval I, we define

$$\theta(I;q,a) := \sum_{n \in I} b_n.$$

Letting $|I|$ denote the number of integers contained in I, we then have that

$$\max_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \left(\theta(I;q,a) - \frac{|I|}{\phi(q)} \right)^2$$

is the square of the 2-variation of the sequence $\{b_n - 1/\phi(q)\}_{n=1}^N$.

Our main result is an upper bound on this quantity, summing over $q \leq Q$ and a coprime to q as in the above theorems. This is a strengthening

of Theorem 98, since we obtain the same bound (up to the implied constant) on a larger quantity. To simplify our notation, we let $\mathcal{P}_x$ denote the set of partitions of $\{1, \dots, \lfloor x \rfloor\}$ into disjoint intervals. We prove:

Theorem 99. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\theta(I; q, a) - \frac{|I|}{\phi(q)} \right)^2 \ll_A xQ \log^3(x).$$

We also establish a variant of this, obtaining a better bound by allowing the partition to depend only on q and not on a:

Theorem 100. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \max_{\pi \in \mathcal{P}_x} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{I \in \pi} \left(\theta(I; a, q) - \frac{|I|}{\phi(q)} \right)^2 \ll_A xQ \log^2(x).$$

In comparison to Theorem 97, this maximizes over partitions instead of restricting to partial sums, but the bound obtained is worse by a multiplicative $\log(x)$ factor.

The introduction of this maximum over partitions allows us to apply our theorem to prove a weakened, averaged version of a conjecture made by Erdős. We let p_i denote the i^{th} prime. Erdős made the following conjecture:

Conjecture 101. (Erdős, [13])

$$\sum_{p_{i+1} \leq x} (p_{i+1} - p_i)^2 \ll x \log(x).$$

This asymptotic is heuristically suggested by the prime number theorem, which implies the reverse inequality. Assuming the Riemann Hypothesis, Selberg [63] obtained the bound

$$\sum_{p_{i+1}\leq x}(p_{i+1}-p_i)^2 \ll x\log^3(x).$$

It is natural to extend the conjecture to arithmetic progressions. Fixing a, q such that $(a,q)=1$, we let $p_i^{a,q}$ denote the i^{th} prime congruent to a modulo q. One then formulates the conjecture as:

Conjecture 102. For any a, q such that $(a,q)=1$,

$$\sum_{p_i^{a,q}\leq x}\left(\frac{p_{i+1}^{a,q}-p_i^{a,q}}{\phi(q)}\right)^2 \ll \frac{x\log(x)}{\phi(q)}.$$

If we then sum over all $q \leq Q$ and all a coprime to q, we would expect to get $\ll Qx\log(x)$. We derive the following weaker bound:

Corollary 103. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q\leq Q}\sum_{\substack{a\leq q\\(a,q)=1}}\sum_{p_{i+1}^{a,q}\leq x}\left(\frac{p_{i+1}^{a,q}-p_i^{a,q}}{\phi(q)}\right)^2 \ll Qx\log^3(x).$$

This can be viewed as an averaged, unconditional version of Selberg's bound, and is easily obtained from Theorem 99.

More generally, the study of variational quantities introduces new and interesting questions. For example, is there an elementary function f such

that

$$\max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\sum_{n \in I} (\Lambda(n) - 1) \right)^2 \sim f(x)? \tag{6.1}$$

The prime number theorem gives an (asymptotic) lower bound of $x \log(x)$ on this quantity. We note, however, that one cannot hope to have $f(x) = x \log(x)$. This follows from the work of Cheer and Goldston [7], who proved

Theorem 104. For any $\epsilon > 0$, there exists an X_0 such that for all $x > X_0$,

$$\sum_{p_{i+1} \leq x} |p_{i+1} - p_i|^2 \geq (193/192 - \epsilon) x \log x.$$

(Note, as seen from Lemma 105 below, the contribution to (6.1) from prime powers is of lower order.) This does not rule out the possibility of $f(x) = Cx \log(x)$ for some larger C, for example.

6.2 Preliminaries

We first recall some standard definitions. When q is a positive integer, $\phi(q)$ denotes the Euler totient function. For positive integers a and q, (a, q) denotes the g.c.d. of a and q.

For a positive real number x, we define

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^\alpha \leq x} \log(p),$$

$$\theta(x) = \sum_{p \leq x} \log(p).$$

Here, log denotes the natural logarithm. The latter sum for ψ is over prime powers p^α, while the sum for θ is over primes p. $\Lambda(n)$ denotes the von Mangoldt

function, which is equal to $\log(p)$ whenever n is a power of a prime p and equal to 0 otherwise.

Letting a and q be positive integers, we similarly define

$$\psi(x;q,a) = \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} \Lambda(n), \quad \theta(x;q,a) = \sum_{\substack{p\leq x \\ p\equiv a \bmod q}} \log(p).$$

Letting I be an interval, we also define

$$\psi(I;q,a) = \sum_{\substack{n\in I \\ n\equiv a \bmod q}} \Lambda(n), \quad \theta(I;q,a) = \sum_{\substack{p\in I \\ p\equiv a \bmod q}} \log(p).$$

The size of an interval I is defined to be the number of integers it contains, and is denoted by $|I|$. For a fixed positive real number x, we let $\mathcal{P}_x$ denote the set of all partitions of $[1, \lfloor x \rfloor]$ into intervals. Thus an element $\pi \in \mathcal{P}_x$ is a collection of disjoint intervals whose union is the interval from 1 to $\lfloor x \rfloor$.

We recall the prime number theorem, which states that $\psi(x) \sim x$. We will later also use the following standard fact (we include the short proof here for completeness):

Lemma 105. For $x \geq 2$, $\theta(x) = \psi(x) + O(x^{\frac{1}{2}})$.

Proof. Since $p^\alpha \leq x$ holds if and only if $p \leq x^{\frac{1}{\alpha}}$, we have

$$\psi(x) = \sum_{\alpha=1}^{\infty} \theta\left(x^{\frac{1}{\alpha}}\right) \text{ and } \psi(x) - \theta(x) = \sum_{\alpha\geq 2} \theta\left(x^{\frac{1}{\alpha}}\right).$$

Noting that $x^{\frac{1}{\alpha}} \geq 2$ only for $\alpha = O(\log x)$ and $\theta(x^{\frac{1}{\alpha}}) \leq \psi(x^{\frac{1}{\alpha}}) \ll x^{\frac{1}{\alpha}}$, we see this is $\ll x^{\frac{1}{2}} + x^{\frac{1}{3}} \log x \ll x^{\frac{1}{2}}$. □

6.3 A Variational Form of the Barban-Davenport-Halberstam Theorem

We now prove:

Theorem 99. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\theta(I; q, a) - \frac{|I|}{\phi(q)} \right)^2 \ll_A xQ \log^3(x).$$

We will deduce this by combining the proof of the standard Barban-Davenport-Halberstam theorem with some combinatorial arguments and a variational form of the Siegel-Walfisz Theorem that is developed in the following subsection.

For a fixed positive integer q, we consider Dirichlet characters modulo q. A function $\chi : \mathbb{Z}_q^* \to \mathbb{C}$ is called a Dirichlet character modulo q if it is a group homomorphism. We can extend such a χ to be a function from $\mathbb{Z}$ to $\mathbb{C}$ by defining $\chi(n)$ to be equal to the value of the character on the residue class of n modulo q when n is coprime to q and 0 otherwise. From now on, we will consider Dirichlet characters to be functions on $\mathbb{Z}$. A character χ mod q is said to be *primitive* if its period as a function on $\mathbb{Z}$ is precisely q (conversely it is non-primitive if it has a smaller period dividing q).

We fix positive integers M and N. Given a Dirchlet character χ mod q and complex numbers $\{a_n\}_{n=M+1}^{M+N}$, we define

$$T(\chi) = \sum_{n=M+1}^{M+N} a_n \chi(n).$$

More generally, for any interval $I \subseteq [M+1, M+N]$, we define

$$T(\chi, I) = \sum_{n \in I} a_n \chi(n).$$

The large sieve inequality [10] states:

Theorem 106. (The Large Sieve Inequality) For any positive integers Q, M, N and complex numbers $\{a_n\}_{n=M+1}^{M+N}$:

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} |T(\chi)|^2 \ll (N + Q^2) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Here, the the inner sum $\sum_{\chi}^{*}$ is over the **primitive** characters modulo q (this is what the $*$ superscript signifies).

In our proof of Theorem 99, we will use the large sieve inequality directly as it is stated above. However, we will later establish variational versions of this in Sections 6.4 and 6.5.

6.3.1 A Variational Form of the Siegel-Walfisz Theorem

For a positive real number x and a Dirichlet character $\chi \bmod q$, we define

$$\psi(x, \chi) = \sum_{p^\alpha \leq x} \chi(p^\alpha) \log(p), \text{ and } \theta(x, \chi) = \sum_{p \leq x} \chi(p) \log(p).$$

For an interval I, we similarly define

$$\theta(I, \chi) = \sum_{p \in I} \chi(p) \log(p).$$

We refer to the unique $\chi \bmod q$ that takes the value 1 on all integers coprime to q as the *principal* character modulo q, and all other characters as non-principal.

The Siegel-Walfisz Theorem [10] states:

Theorem 107. (Siegel-Walfisz Theorem) Let A be a positive real number. Then there exists some positive constant c_A depending only on A such that

$$|\psi(x,\chi)| \ll_A xe^{-c_A \log^{\frac{1}{2}}(x)}$$

for all non-principal characters $\chi \bmod q$ for all moduli $q \leq \log^A(x)$.

We will find it more convenient to work with the following corollary:

Corollary 108. Let A be a positive real number. Then there exists some positive constant c_A depending only on A such that

$$|\theta(x,\chi)| \ll_A xe^{-c_A \log^{\frac{1}{2}}(x)}$$

for all non-principal characters $\chi \bmod q$ for all moduli $q \leq \log^A(x)$.

Proof. By the triangle inequality, $|\theta(x,\chi)| \leq |\psi(x,\chi)| + |\psi(x,\chi) - \theta(x,\chi)|$. The first quantity is bounded by Theorem 107. To bound the second quantity, we observe

$$|\psi(x,\chi) - \theta(x,\chi)| = \left| \sum_{\substack{p^\alpha \leq x \\ \alpha > 1}} \chi(p^\alpha) \log(p) \right| \leq \sum_{\substack{p^\alpha \leq x \\ \alpha > 1}} \log(p) = \psi(x) - \theta(x),$$

by the triangle inequality and the fact that $|\chi(p^\alpha)|$ is always either 0 or 1. Applying Lemma 105, we see that $|\psi(x,\chi) - \theta(x,\chi)| \ll x^{\frac{1}{2}}$, where the implicit constant is independent of q and χ. □

We now prove a variational form of this:

Lemma 109. Let A be a positive real number. Then there exists some positive constant c'_A depending only on A such that

$$\sqrt{\max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} |\theta(I, \chi)|^2} \ll_A x e^{-c'_A \log^{\frac{1}{2}}(x)} \tag{6.2}$$

for all non-principal characters $\chi \bmod q$ for all moduli $q \leq \log^A(x)$.

Proof. Since every $I \in \pi$ is a subinterval of $[1, x]$, the left hand side of (6.2) is

$$\ll \sqrt{\max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} |\theta(I, \chi)| \cdot \max_{J \subseteq [1,x]} |\theta(J, \chi)|}. \tag{6.3}$$

We consider the inner quantity $\sum_{I \in \pi} |\theta(I, \chi)|$. By definition, we have

$$\sum_{I \in \pi} |\theta(I, \chi)| = \sum_{I \in \pi} \left| \sum_{p \in I} \chi(p) \log(p) \right|.$$

Applying the triangle inequality, this is

$$\leq \sum_{I \in \pi} \sum_{p \in I} |\chi(p) \log(p)| \leq \sum_{I \in \pi} \sum_{p \in I} \log(p) = \theta(x).$$

Here, we have used the fact that $|\chi(p)|$ is always either 1 or 0.

We then have that (6.3) is

$$\ll \sqrt{\theta(x) \max_{J \subseteq [1,x]} |\theta(J, \chi)|}.$$

Since $\theta(x) \leq \psi(x) \ll x$, this is

$$\ll \sqrt{x \max_{J \subseteq [1,x]} |\theta(J, \chi)|}. \tag{6.4}$$

We consider the quantity $\max_{J \subseteq [1,x]} |\theta(J,\chi)|$. We observe that this is $\ll \max_{y \leq x} |\theta(y,\chi)|$. We will upper bound this quantity for each y separately. For larger y values, we will employ Corollary 108 for the value $2A$ (using $2A$ instead of A will allow us to apply the corollary to a larger range of y values). We let c_{2A} denote the constant for $2A$ in the exponent. More precisely, for y such that $q \leq \log^{2A}(y)$, we have $|\theta(y,\chi)| \ll_A y e^{-c_{2A}\log^{\frac{1}{2}}(y)}$ by Corollary 108. Since $y \leq x$, this is $\ll_A x e^{-c_{2A}\log^{\frac{1}{2}}(x)}$.

We now consider y such that $\log^{2A}(y) \leq q$. This is equivalent to the condition $y \leq e^{q^{\frac{1}{2A}}}$. For these small y values, we will use the basic estimate $|\theta(y,\chi)| \ll \theta(y) \ll y$. Since $\log^{A}(x) \geq q$ holds by assumption, we have $\log(x) \geq q^{\frac{1}{A}} \geq \log^2(y)$. We then have $y \leq e^{\log^{\frac{1}{2}}(x)} \ll_A x e^{-c_{2A}\log^{\frac{1}{2}}(x)}$. Hence,

$$\max_{y \leq x} |\theta(y,\chi)| \ll_A x e^{-c_{2A}\log^{\frac{1}{2}}(x)}.$$

Thus, the quantity in (6.4) is

$$\ll_A \sqrt{x^2 e^{-c_{2A}\log^{\frac{1}{2}}(x)}} = x e^{-\frac{1}{2}\cdot c_{2A}\log^{\frac{1}{2}}(x)}.$$

This proves Lemma 109 with $c'_A := \frac{1}{2} \cdot c_{2A}$. □

We note that, conditional on the generalized Riemann hypothesis, for a nonprincipal Dirichlet of modulus q one has the bound

$$|\psi(x,\chi)| \ll x^{1/2}\log(x)\log(qx)$$

where the implied constant is absolute (see Theorem 13.7 in [47]). This can be used as in the argument above to obtain:

Lemma 110. Let χ be a nonprincipal character mod q. Assuming the generalized Riemann hypothesis, we have that

$$\max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} |\theta(I, \chi)|^2 \ll x^{3/2} \log(x) \log(qx). \tag{6.5}$$

This could be used in place of Lemma 109 in the following arguments to conditionally extend the range of Q in the statements of Theorems 99 and 100. This is quite routine, and we omit the details. It may be possible to further improve (conditionally) the exponent of the $x^{3/2}$ term. We leave this as an interesting open problem.

6.3.2 Proof of Theorem 99

We now bound the quantity

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\theta(I; q, a) - \frac{|I|}{\phi(q)} \right)^2. \tag{6.6}$$

The structure of our proof will resemble the proof of the non-variational version of the theorem in [10].

We let 2^k denote the smallest power of two that is $\geq x$. We can then decompose $[1, 2^k]$ into dyadic intervals $I_{c,\ell} = ((c-1)2^\ell, c2^\ell]$, where ℓ ranges from 0 to 2^k and c ranges from 1 to $2^{k-\ell}$. We note the following lemma [41] or Chapter 4:

Lemma 111. Any subinterval of $S \subset [1, 2^k]$ can be expressed as the disjoint union of intervals of the form $I_{c,\ell}$, such as

$$S = \bigcup_m I_{c_m, \ell_m}$$

where at most two of the intervals I_{c_m,ℓ_m} in the union are of each size, and where the union consists of at most $2k$ intervals.

In other words, each $I \subseteq [x]$ can be decomposed as a disjoint union of these dyadic intervals using at most two intervals on each level ℓ. We let $D(I)$ denote the set of dyadic intervals in the decomposition of I. We observe

$$\theta(I;q,a) - \frac{|I|}{\phi(q)} = \sum_{J \in D(I)} \left(\theta(J;q,a) - \frac{|J|}{\phi(q)} \right)$$

for any I, since $\sum_{J \in D(I)} |J| = |I|$. For each ℓ, we let $D_\ell(I)$ denote the intervals in $D(I)$ on level ℓ (so $|D_\ell(I)| \leq 2$). We can rewrite (6.6) as:

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\sum_{\ell=0}^{2^k} \sum_{J \in D_\ell(I)} \theta(J;q,a) - \frac{|J|}{\phi(q)} \right)^2.$$

By the triangle inequality for the ℓ^2 norm, we have

$$\sqrt{\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\theta(I;q,a) - \frac{|I|}{\phi(q)} \right)^2}$$

$$\ll \sum_{\ell=0}^{k} \left(\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\sum_{J \in D_\ell(I)} \theta(J;q,a) - \frac{|J|}{\phi(q)} \right)^2 \right)^{\frac{1}{2}}. \tag{6.7}$$

Since $|D_\ell(I)| \leq 2$ for all ℓ, I and each dyadic interval can appear in $D(I)$ for at most one $I \in \pi$,

$$\max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \left(\sum_{J \in D_\ell(I)} \theta(J;q,a) - \frac{|J|}{\phi(q)} \right)^2 \ll \sum_{c=1}^{2^{k-\ell}} \left(\theta(I_{c,\ell};q,a) - \frac{|I_{c,\ell}|}{\phi(q)} \right)^2$$

for all a, q, ℓ. Therefore the quantity in (6.7) is

$$\ll \sum_{\ell=0}^{k} \left(\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{c=1}^{2^{k-\ell}} \left(\theta(I_{c,\ell}; q, a) - \frac{|I_{c,\ell}|}{\phi(q)} \right)^2 \right)^{\frac{1}{2}}. \tag{6.8}$$

For each fixed ℓ, we consider the quantity

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{c=1}^{2^{k-\ell}} \left(\theta(I_{c,\ell}; q, a) - \frac{|I_{c,\ell}|}{\phi(q)} \right)^2. \tag{6.9}$$

We will bound this quantity using the large sieve inequality and the Siegel-Walfisz Theorem, so we need to first express it in terms of characters χ modulo q. For this, we will introduce some convenient notation. Fixing q, we let χ_0 denote the principal character modulo q. For any character χ modulo q, we define

$$\theta'(I, \chi) := \begin{cases} \theta(I, \chi), & \chi \neq \chi_0; \\ \theta(I, \chi_0) - |I|, & \chi = \chi_0. \end{cases}$$

We will employ the following lemma:

Lemma 112. For any interval I and any coprime positive integers q, a,

$$\theta(I; q, a) - \frac{|I|}{\phi(q)} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \theta'(I, \chi),$$

where $\overline{\chi}$ denotes the character obtained from χ by complex conjugation.

Proof. We note that for each integer n,

$$\sum_{\chi \bmod q} \chi(n) = \begin{cases} \phi(q), & n \equiv 1 \bmod q; \\ 0, & \text{otherwise.} \end{cases}$$

For any integer a coprime to q, we let $\overline{a}$ denote an integer such that $\overline{a}a \equiv 1 \bmod q$. Then, for any $\chi \bmod q$, $\overline{\chi}(a)\chi(n) = \chi(\overline{a})\chi(n) = \chi(\overline{a}n)$. Since $\overline{a}n \equiv 1 \bmod q$ if and only if $n \equiv a \bmod q$, we have

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a)\chi(n) = \begin{cases} 1, & n \equiv a \bmod q; \\ 0, & \text{otherwise.} \end{cases}$$

We then observe

$$\begin{aligned} \theta(I; q, a) &= \sum_{\substack{p \in I \\ p \equiv a \bmod q}} \log(p) \\ &= \frac{1}{\phi(q)} \sum_{p \in I} \log(p) \sum_{\chi \bmod q} \overline{\chi}(a)\chi(p) \\ &= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a)\theta(I, \chi). \end{aligned}$$

By definition of $\theta'(I, \chi)$, it then follows that

$$\theta(I; q, a) - \frac{|I|}{\phi(q)} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a)\theta'(I, \chi).$$

□

The quantity (6.9) can then be expressed as

$$\sum_{q \le Q} \frac{1}{\phi(q)^2} \sum_{c=1}^{2^{k-\ell}} \sum_{\substack{a \le q \\ (a,q)=1}} \left| \sum_{\chi \bmod q} \overline{\chi}(a)\theta'(I_{c,\ell}, \chi) \right|^2. \tag{6.10}$$

For fixed q and c, the inner quantity can be expanded as:

$$= \sum_{\substack{a \le q \\ (a,q)=1}} \sum_{\chi_1 \bmod q} \sum_{\chi_2 \bmod q} \overline{\chi_1}(a)\chi_2(a)\theta'(I_{c,\ell}, \chi_1)\overline{\theta'(I_{c,\ell}, \chi_2)}$$

Reordering the sums, this is

$$\sum_{\chi_1 \bmod q} \sum_{\chi_2 \bmod q} \theta'(I_{c,\ell}, \chi_1)\overline{\theta'(I_{c,\ell}, \chi_2)} \sum_{\substack{a \leq q \\ (a,q)=1}} \overline{\chi_1}(a)\chi_2(a).$$

The innermost sum is now the inner product of the characters χ_1, χ_2. Since the distinct characters modulo q are orthogonal under this inner product, this innermost sum is 0 unless $\chi_1 = \chi_2$. Therefore, (6.10) is equal to

$$\sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{c=1}^{2^{k-\ell}} \sum_{\chi \bmod q} \left|\theta'(I_{c,\ell}, \chi)\right|^2. \tag{6.11}$$

In order to use the large sieve inequality as stated in Theorem 106, we need to adjust our character sum to be over the primitive characters modulo q instead of all characters modulo q. For this, we first note that every character χ modulo q is induced by some primitive character χ_1 modulo q_1 where $q_1 \leq q$. We then have:

Lemma 113. For any I and any character χ modulo q induced by χ_1 modulo q_1,

$$|\theta'(I, \chi_1) - \theta'(I, \chi)| \leq \log(q).$$

Proof. For all integers n coprime to q, $\chi(n) = \chi_1(n)$. In fact,

$$\theta'(I, \chi_1) - \theta'(I, \chi) = \sum_{\substack{p \in I \\ p|q}} \chi_1(p) \log(p).$$

Therefore,

$$|\theta'(I, \chi_1) - \theta'(I, \chi)| \leq \sum_{\substack{p \in I \\ p|q}} \log(p) \leq \log(q).$$

To see the final inequality, consider the prime factorization of $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then $\log(q) = \alpha_1 \log(p_1) + \cdots + \alpha_r \log(p_r)$. $\square$

As a consequence of Lemma 113, we have $|\theta'(I_{c,\ell}, \chi)|^2 \ll |\theta'(I_{c,\ell}, \chi_1)|^2 + \log^2 q$ for all dyadic intervals $I_{c,\ell}$ and all non-primitive characters χ. Thus, the quantity in (6.11) is

$$\begin{aligned} &\ll \sum_{q \le Q} \frac{1}{\phi(q)} \sum_{c=1}^{2^{k-\ell}} \sum_{\chi \bmod q} \left(\log^2(q) + |\theta'(I_{c,\ell}, \chi_1)|^2 \right) \\ &= \sum_{q \le Q} \frac{1}{\phi(q)} \sum_{c=1}^{2^{k-\ell}} \sum_{\chi \bmod q} \log^2(q) + \sum_{q \le Q} \frac{1}{\phi(q)} \sum_{c=1}^{2^{k-\ell}} \sum_{\chi \bmod q} |\theta'(I_{c,\ell}, \chi_1)|^2. \quad (6.12) \end{aligned}$$

As above, χ_1 here denotes the primitive character that induces χ.

We bound the contribution of this first sum to the quantity in (6.8) (noting that there are $\phi(q)$ characters modulo q):

$$\sum_{0 \le \ell \le k} \sqrt{\sum_{q \le Q} 2^{k-\ell} \log^2(q)} = \left(\sum_{0 \le \ell \le k} (2^{\frac{1}{2}})^{k-\ell} \right) \sqrt{\sum_{q \le Q} \log^2(q)} \ll 2^{\frac{k}{2}} \sqrt{Q \log^2(Q)}.$$

Since (6.8) is an upper bound on the square root of (6.6), the contribution to (6.6) is therefore $\ll 2^k Q \log^2(Q) \ll xQ \log^2(x)$, which is acceptable.

It thus suffices to consider

$$\sum_{q \le Q} \frac{1}{\phi(q)} \sum_{c=1}^{2^{k-\ell}} \sum_{\chi \bmod q} |\theta'(I_{c,\ell}, \chi_1)|^2 \quad (6.13)$$

for each fixed ℓ. Each primitive character χ_1 modulo q_1 induces characters χ modulo q for every q that is a multiple of q_1. We can use this to rewrite the

above quantity in terms of a sum over only primitive characters:

$$= \sum_{q \leq Q} \sum_{c=1}^{2^{k-\ell}} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I_{c,\ell}, \chi)|^2 \left(\sum_{j \leq \frac{Q}{q}} \frac{1}{\phi(jq)} \right).$$

We note that

$$\sum_{j \leq \frac{Q}{q}} \frac{1}{\phi(jq)} \ll \phi(q)^{-1} \log(2Q/q)$$

(see [10], pp. 163), so this is

$$\ll \sum_{q \leq Q} \frac{1}{\phi(q)} \log\left(\frac{2Q}{q}\right) \sum_{c=1}^{2^{k-\ell}} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I_{c,\ell}, \chi)|^2. \tag{6.14}$$

We will split this sum over $q \leq Q$ into ranges and bound each piece separately. For a fixed $1 \leq U \leq Q$, we consider

$$\sum_{c=1}^{2^{k-\ell}} \sum_{U < q \leq 2U} \frac{1}{\phi(q)} \log\left(\frac{2Q}{q}\right) \sideset{}{^*}\sum_{\chi \bmod q} |\theta(I_{c,\ell}, \chi)|^2. \tag{6.15}$$

Note that we have switched notation from θ' to θ here without changing the quantity, since θ' and θ only differ on the trivial character, and this is only included in the primitive characters modulo q when $q = 1$. Since $U \geq 1$ and our sum here is over $q > U$, θ and θ' behave identically here.

We observe that for each fixed c, the contribution to (6.15) is

$$\ll U^{-1} \log\left(\frac{2Q}{U}\right) \sum_{q \leq 2U} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} |\theta(I_{c,\ell}, \chi)|^2.$$

Letting $a_p := \log(p)$ for primes p and $a_n := 0$ for all non-primes n, we apply Theorem 106 to see that this is

$$\ll U^{-1} \log\left(\frac{2Q}{U}\right) \left(|I_{c,\ell}| + U^2\right) \sum_{p \in I_{c,\ell}} \log^2(p).$$

We define $Q_1 := \log^{A+1}(x)$. We consider the values $U = Q2^{-j}$ as j ranges from 0 to $J := \lceil \log(\frac{Q}{Q_1}) \rceil$. We then have:

$$\sum_{Q_1 < q \leq Q} \frac{1}{\phi(q)} \log\left(\frac{2Q}{q}\right) \sideset{}{^*}\sum_{\chi \bmod q} |\theta(I_{c,\ell}, \chi)|^2$$

$$\ll Q^{-1} \sum_{j=0}^{J} 2^j (j+1) \left(|I_{c,\ell}| + Q^2 2^{-2j}\right) \sum_{p \in I_{c,\ell}} \log^2(p).$$

We expand the latter quantity as

$$= |I_{c,\ell}| Q^{-1} \left(\sum_{j=0}^{J} (j+1) 2^j\right) \left(\sum_{p \in I_{c,\ell}} \log^2(p)\right)$$

$$+ Q \left(\sum_{j=0}^{J} (j+1) 2^{-j}\right) \left(\sum_{p \in I_{c,\ell}} \log^2(p)\right).$$

Inserting this into the sum over the c values, we then have

$$\sum_{c=1}^{2^{k-\ell}} \sum_{Q_1 < q \leq Q} \frac{1}{\phi(q)} \log\left(\frac{2Q}{q}\right) \sideset{}{^*}\sum_{\chi \bmod q} |\theta(I_{c,\ell}, \chi)|^2$$

$$\ll \sum_{c=1}^{2^{k-\ell}} |I_{c,\ell}| Q^{-1} \left(\sum_{j=0}^{J} (j+1) 2^j\right) \left(\sum_{p \in I_{c,\ell}} \log^2(p)\right)$$

$$+ \sum_{c=1}^{2^{k-\ell}} Q \left(\sum_{j=0}^{J} j 2^{-j}\right) \left(\sum_{p \in I_{c,\ell}} \log^2(p)\right).$$

We observe that

$$\sum_{c=1}^{2^{k-\ell}} \sum_{p \in I_{c,\ell}} \log^2(p) = \sum_{p \leq 2^k} \log^2(p),$$

since the union of the intervals $I_{c,\ell}$ as c ranges from 1 to $2^{k-\ell}$ is equal to the interval $[2^k]$. We then have that $\sum_{p\leq 2^k}\log^2(p) \ll k2^k$. We also note that

$$\sum_{j=0}^{J}(j+1)2^j = J2^{J+1}+1 \ll J2^J \text{ and } \sum_{j=0}^{J}(j+1)2^{-j} \ll 1.$$

Therefore, we have shown

$$\sum_{c=1}^{2^{k-\ell}}\sum_{Q_1<q\leq Q}\frac{1}{\phi(q)}\log\left(\frac{2Q}{q}\right)\sum_{\chi \bmod q}^{*}|\theta(I_{c,\ell},\chi)|^2 \ll Q^{-1}(2^\ell)(J2^J)(k2^k)+Q(k2^k). \tag{6.16}$$

Recalling that $2^k \ll x$, $k \ll \log(x)$, $J = \lceil \log(\frac{Q}{Q_1})\rceil$, and $Q \leq x$, we see that the contribution to (6.14) from q's between Q_1 and Q is

$$\ll Q_1^{-1}(2^\ell)(x\log^2(x))+Q(x\log(x)).$$

We now consider values of $q \leq Q_1$. For every primitive character χ modulo q where $q>1$, χ is non-principal. Note that for the principal character χ_0 modulo 1, $\theta'(I_{c,\ell},\chi_0) = \theta(I_{c,\ell},\chi_0) - |I_{c,\ell}| = 0$. Thus, the contribution to (6.14) from values $q \leq Q_1$ can be written as:

$$\sum_{1<q\leq Q_1}\frac{1}{\phi(q)}\log\left(\frac{2Q}{q}\right)\sum_{\chi \bmod q}^{*}\sum_{c=1}^{2^{k-\ell}}|\theta'(I_{c,\ell},\chi)|^2. \tag{6.17}$$

This innermost sum over c is a sum over a partition of $[2^k]$, so we can apply Lemma 109 (with $A+1$ as the constant) to conclude that

$$\sum_{c=1}^{2^{k-\ell}}|\theta'(I_{c,\ell},\chi)|^2 \ll_A x^2 e^{-\tilde{c}_A\log^{\frac{1}{2}}(x)}$$

for some positive constant $\tilde{c}_A$ depending only on A. The quantity in (6.17) is then

$\ll_A Q_1 \log(Q) \cdot x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)}$.

Putting this all together, we have that the quantity in (6.14) is:

$$\ll_A Q_1 \log(Q) \cdot x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} + Q_1^{-1}(2^\ell)(x \log^2(x)) + Q(x \log(x)).$$

Thus, the contribution to (6.8) is bounded by:

$$\ll_A \sum_{\ell=0}^{k} \sqrt{Q_1 \log(Q) \cdot x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} + Q_1^{-1}(2^\ell)(x \log^2(x)) + Q(x \log(x))}$$

$$\ll_A \log(x) \sqrt{Q_1 \log(Q) \cdot x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)}} + \sqrt{Q_1^{-1} x^2 \log^2(x)} + \log(x) \sqrt{Q(x \log(x))}.$$

Hence the contribution to (6.6) is bounded by the square of this:

$$\ll_A Q_1 \log(Q) \log^2(x) x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} + Q_1^{-1} x^2 \log^2(x) + Qx \log^3(x).$$

Recalling that $Q_1 = \log^{A+1}(x)$ and $x \log^{-A}(x) \leq Q \leq x$, we see that this is

$$\ll_A \log^{A+4}(x) x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} + Qx \log(x) + Qx \log^3(x).$$

Since $e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} \ll_A \log^{-2A-1}(x)$, this first term is $\ll_A Qx \log^3(x)$, as required. This completes the proof of Theorem 99.

6.3.3 An Averaged Variant of Erdős' Conjecture

We now apply our variational form of the Barban-Davenport-Halberstam Theorem to prove Corollary 103.

Corollary 8. Let $A > 0$. For all positive real numbers x and Q satisfying $x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{p_{i+1}^{a,q} \leq x} \left(\frac{p_{i+1}^{a,q} - p_i^{a,q}}{\phi(q)} \right)^2 \ll Qx \log^3(x).$$

Proof. For each fixed a, q, we consider a partition in $\mathcal{P}_x$ containing all the intervals of the form

$$I_i := \left(p_i^{a,q}, p_{i+1}^{a,q} \right).$$

By definition of θ and I_i, the quantity $\theta(I_i; q, a)$ equals 0 for all i. Hence,

$$\left(\theta(I_i; q, a) - \frac{|I_i|}{\phi(q)} \right)^2 = \left(\frac{p_{i+1}^{a,q} - p_i^{a,q} - 1}{\phi(q)} \right)^2.$$

We note that $(p_{i+1}^{a,q} - p_i^{a,q} - 1)^2 \gg (p_{i+1}^{a,q} - p_i^{a,q})^2$ (except for the case where $p_{i+1}^{a,q} = 3$ and $p_i^{a,q} = 2$, but this only occurs for $q = 1$ and so can be ignored). Thus, Theorem 99 implies

$$\sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{p_{i+1}^{a,q} \leq x} \left(\frac{p_{i+1}^{a,q} - p_i^{a,q}}{\phi(q)} \right)^2 \ll Qx \log^3(x).$$

□

6.4 Another Variational Form of the Barban-Davenport-Halberstam Theorem

We now prove:

Theorem 100. Let $A > 0$. For all positive real numbers x and Q satisfying

$x(\log(x))^{-A} \leq Q \leq x$,

$$\sum_{q \leq Q} \max_{\pi \in \mathcal{P}_x} \sum_{\substack{a \leq q \\ (a,q)=1}} \sum_{I \in \pi} \left(\theta(I; a, q) - \frac{|I|}{\phi(q)} \right)^2 \ll_A xQ \log^2(x).$$

We will need some additional notation. We let $e(x) := e^{2\pi i x}$. For any real numbers $\{a_n\}_{n=1}^N$, we define a function $S : \mathbb{T} \to \mathbb{C}$ by

$$S(\alpha) := \sum_{n=1}^{N} a_n e(n\alpha).$$

For $\delta > 0$, we say that points $\alpha_1, \ldots, \alpha_R \in \mathbb{T}$ are δ-*separated* if $||\alpha_i - \alpha_j|| \geq \delta$ for all $i \neq j$, where the $|| \cdot ||$ denotes the norm modulo 1.

We let $\mathcal{P}_N$ denote the set of all partitions of $[N]$ into a union of disjoint intervals. We then define

$$||S(\alpha)||_{V^r} := \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n e(n\alpha) \right|^r \right)^{\frac{1}{r}}.$$

We note the variational Carleson Theorem [52]:

Theorem 114. For any real numbers $\{a_n\}_{n=1}^N$ and any $r > 2$,

$$\int_{\mathbb{T}} ||S(\alpha)||_{V^r}^2 d\alpha \ll_r \sum_{n=1}^{N} |a_n|^2.$$

The case of $r = 2$ is addressed in the following theorem, which follows immediately from Corollary 4 in [41]:

Theorem 115. For any real numbers $\{a_n\}_{n=1}^N$,

$$\int_{\mathbb{T}} ||S(\alpha)||_{V^2}^2 d\alpha \ll \log(N) \sum_{n=1}^{N} |a_n|^2.$$

We note that the $\log(N)$ factor is known to be sharp. We will first prove the following lemma, which is a variational version of the analytic large sieve inequality.

Lemma 116. For any $\delta > 0$ and for any points $\alpha_1, \dots, \alpha_R \in \mathbb{T}$ that are δ-separated,

$$\sum_{i=1}^{R} ||S(\alpha_i)||_{V^r}^2 \ll_r (N + \delta^{-1} + 1) \sum_{n=1}^{N} |a_n|^2$$

for any $r > 2$. Also,

$$\sum_{i=1}^{R} ||S(\alpha_i)||_{V^2}^2 \ll (N + \delta^{-1} + 1) \log(N) \sum_{n=1}^{N} |a_n|^2.$$

Proof. This proof will be a variational adaptation of the proof of Theorem 5 in [46]. By a theorem of Selberg [68], there exists an entire function $K(z)$ such that K is real-valued on $\mathbb{R}$, $K(x) \geq 0$ for all real x, and $K(x) \geq 1$ for all $1 \leq x \leq N$. Moreover, $K(x)$ is integrable, and $\widehat{K}(0) = N - 1 + \delta^{-1}$. By a theorem of Fejér, there is another entire function $k(z)$ such that $K(x) = |k(x)|^2$ for all $x \in \mathbb{R}$, and $\hat{k}$ (the fourier transform of $k(x)$) has support in $\left(-\frac{\delta}{2}, \frac{\delta}{2}\right)$. We note that

$$k(x) = \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} \hat{k}(\xi) e(x\xi) d\xi.$$

We define a function $T : \mathbb{T} \to \mathbb{C}$ by

$$T(\alpha) := \sum_{n=1}^{N} a_n k(n)^{-1} e(n\alpha).$$

Similarly, we define

$$||T(\alpha)||_{V^r} := \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n k(n)^{-1} e(n\alpha) \right|^r \right)^{\frac{1}{r}}.$$

For any α and any $r \geq 2$, we have

$$\begin{aligned} ||S(\alpha)||_{V^r} &= \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n e(n\alpha) \right|^r \right)^{\frac{1}{r}} \\ &= \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n k(n)^{-1} e(n\alpha) \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} \hat{k}(\xi) e(n\xi) d\xi \right|^r \right)^{\frac{1}{r}} \\ &= \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} \hat{k}(\xi) \sum_{n \in I} a_n k(n)^{-1} e(n(\alpha + \xi)) d\xi \right|^r \right)^{\frac{1}{r}}. \end{aligned}$$

By Minkowski's integral inequality (see [24], Theorem 201 for example), this last quantity is

$$\leq \max_{\pi \in \mathcal{P}_N} \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} \left(\sum_{I \in \pi} \left| \hat{k}(\xi) \sum_{n \in I} a_n k(n)^{-1} e(n(\alpha + \xi)) \right|^r \right)^{\frac{1}{r}} d\xi$$

$$= \max_{\pi \in \mathcal{P}_N} \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} |\hat{k}(\xi)| \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n k(n)^{-1} e(n(\alpha + \xi)) \right|^r \right)^{\frac{1}{r}} d\xi$$

$$\leq \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} |\hat{k}(\xi)| \max_{\pi \in \mathcal{P}_N} \left(\sum_{I \in \pi} \left| \sum_{n \in I} a_n k(n)^{-1} e(n(\alpha + \xi)) \right|^r \right)^{\frac{1}{r}} d\xi.$$

Now applying the Cauchy-Schwarz inequality, we see this is

$$\leq \left(\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} |\hat{k}(\xi)|^2 d\xi \right)^{\frac{1}{2}} \left(\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} ||T(\xi + \alpha)||_{V^r}^2 d\xi \right)^{\frac{1}{2}}.$$

By the properties of k and K, we have

$$\left(\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} |\hat{k}(\xi)|^2 d\xi \right)^{\frac{1}{2}}$$

$$= \left(\int_{-\infty}^{\infty} |k(x)|^2 dx \right)^{\frac{1}{2}} = \left(\int_{-\infty}^{\infty} K(x) dx \right)^{\frac{1}{2}} = \left(\widehat{K}(0) \right)^{\frac{1}{2}} = \left(N - 1 + \delta^{-1} \right)^{\frac{1}{2}}.$$

Therefore, we have shown that

$$\sum_{i=1}^{R} ||S(\alpha_i)||_{V^r}^2 \leq (N-1+\delta^{-1}) \sum_{i=1}^{R} \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} ||T(\xi+\alpha_i)||_{V^r}^2 d\xi.$$

Since the α_i's are δ-separated, the ranges $(-\frac{\delta}{2}+\alpha_i, \frac{\delta}{2}+\alpha_i)$ are disjoint in $\mathbb{T}$, and hence

$$\sum_{i=1}^{R} ||S(\alpha_i)||_{V^r}^2 \leq (N-1+\delta^{-1}) \int_{\mathbb{T}} ||T(\xi)||_{V^r}^2 d\xi. \tag{6.18}$$

For $r > 2$, we may apply Theorem 114 for the real numbers $\{a_n k(n)^{-1}\}_{n=1}^N$ to conclude that the righthand side of (6.18) is

$$\ll_r (N-1+\delta^{-1}) \sum_{n=1}^{N} |a_n k(n)^{-1}|^2.$$

Recalling that $\frac{1}{|k(n)|^2} = \frac{1}{K(n)}$ and $K(n) \geq 1$ for all n from 1 to N, we obtain

$$\sum_{i=1}^{R} ||S(\alpha_i)||_{V^r}^2 \ll_r (N-1+\delta^{-1}) \sum_{n=1}^{N} |a_n|^2$$

for all $r > 2$, as required.

For $r = 2$, we may apply Theorem 115 for the real numbers $\{a_n k(n)^{-1}\}_{n=1}^N$ to conclude that the righthand side of (6.18) is

$$\ll (N-1+\delta^{-1}) \log(N) \sum_{n=1}^{N} |a_n k(n)^{-1}|^2 \ll (N-1+\delta^{-1}) \log(N) \sum_{n=1}^{N} |a_n|^2.$$

□

We next prove the following lemma:

Lemma 117. For any real numbers $\{a_n\}_{n=1}^N$,

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \max_{\pi \in \mathcal{P}_N} \sum_{\chi \bmod q}^{*} \sum_{I \in \pi} |T(I,\chi)|^2 \ll (N+Q^2) \log(N) \sum_{n=1}^{N} |a_n|^2.$$

Proof. This proof is adapted from the proof of Theorem 4 in [10]. For a character χ modulo q, we define the complex value $\tau(\chi)$ by

$$\tau(\chi) := \sum_{a \leq q} \chi(a) e\left(\frac{a}{q}\right).$$

We have

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a \leq q} \overline{\chi}(a) e\left(\frac{an}{q}\right)$$

for all n for all primitive χ (see [10], chapter 9). Therefore, for any interval I and any primitive χ modulo q,

$$T(I, \chi) = \sum_{n \in I} a_n \chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a \leq q} \overline{\chi}(a) \sum_{n \in I} a_n e\left(\frac{an}{q}\right).$$

We then note that when χ is primitive, $|\tau(\chi)| = q^{\frac{1}{2}}$ (see [10], p. 66). This yields (for any partition π):

$$\sum_{I \in \pi} |T(I, \chi)|^2 = \frac{1}{q} \sum_{I \in \pi} \left| \sum_{a \leq q} \overline{\chi}(a) \sum_{n \in I} a_n e\left(\frac{an}{q}\right) \right|^2.$$

Now summing over primitive characters, we have

$$\sum_{\chi \bmod q}^{*} \sum_{I \in \pi} |T(\chi, I)|^2 = \frac{1}{q} \sum_{I \in \pi} \sum_{\chi \bmod q}^{*} \left| \sum_{a \leq q} \overline{\chi}(a) \sum_{n \in I} a_n e\left(\frac{an}{q}\right) \right|^2.$$

This quantity can only increase if we sum over all characters modulo q, so this is

$$\leq \frac{1}{q} \sum_{I \in \pi} \sum_{a \leq q} \sum_{b \leq q} \left(\sum_{n \in I} a_n e\left(\frac{an}{q}\right) \right) \left(\sum_{n \in I} a_n \overline{e}\left(\frac{bn}{q}\right) \right) \sum_{\chi \bmod q} \overline{\chi}(a) \chi(b). \quad (6.19)$$

Here, $\overline{e}$ denotes conjugation. We note that this innermost sum over characters is equal to 0 unless $a = b$ and a is coprime to q. In this case, it is equal to $\phi(q)$. Plugging this into (6.19), we have

$$= \frac{\phi(q)}{q} \sum_{I \in \pi} \sum_{\substack{a \leq q \\ (a,q)=1}} \left| \sum_{n \in I} a_n e\left(\frac{an}{q}\right) \right|^2.$$

Recalling that

$$||S(\alpha)||_{V^2}^2 := \max_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \left| \sum_{n \in I} a_n e(n\alpha) \right|^2,$$

we conclude that

$$\begin{aligned} \sum_{q \leq Q} \frac{q}{\phi(q)} \max_{\pi \in \mathcal{P}_N} \sideset{}{^*}\sum_{\chi \bmod q} \sum_{I \in \pi} |T(I,\chi)|^2 &\ll \sum_{q \leq Q} \max_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \sum_{\substack{a \leq q \\ (a,q)=1}} \left| \sum_{n \in I} a_n e\left(\frac{an}{q}\right) \right|^2 \\ &\leq \sum_{q \leq Q} \sum_{\substack{a \leq q \\ (a,q)=1}} ||S(a/q)||_{V^2}^2. \end{aligned}$$

Here we have used the fact that moving the maximum inside the sum over a's coprime to q can only make the quantity larger. The points $\frac{a}{q}$ as q ranges from 1 to Q and a ranges over values coprime to q are $\frac{1}{Q^2}$-separated as points in $\mathbb{T}$. Thus, applying Lemma 116, this is $\ll (N + Q^2) \log(N) \sum_{n=1}^N |a_n|^2$. □

We are now equipped to prove Theorem 100. We recall Lemma 112, which states that

$$\theta(I; q, a) - \frac{|I|}{\phi(q)} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \theta'(I, \chi).$$

We then have

$$\sum_{q\le Q}\max_{\pi\in\mathcal{P}_x}\sum_{\substack{a\le q\\(a,q)=1}}\sum_{I\in\pi}\left(\theta(I;q,a)-\frac{|I|}{\phi(q)}\right)^2$$

$$=\sum_{q\le Q}\frac{1}{\phi(q)^2}\max_{\pi\in\mathcal{P}_x}\sum_{\substack{a\le q\\(a,q)=1}}\sum_{I\in\pi}\left|\sum_{\chi \bmod q}\overline{\chi}(a)\theta'(I,\chi)\right|^2.$$

By expanding the square and rearranging the sums inside the maximum, this is

$$=\sum_{q\le Q}\frac{1}{\phi(q)^2}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi_1 \bmod q}\sum_{\chi_2 \bmod q}\theta'(I,\chi_1)\overline{\theta'(I,\chi_2)}\sum_{\substack{a\le q\\(a,q)=1}}\overline{\chi_1}(a)\chi_2(a).$$

This innermost sum over a's coprime to q is equal to $\phi(q)$ whenever $\chi_1=\chi_2$, and is equal to 0 otherwise. Hence this quantity is

$$=\sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi \bmod q}|\theta'(I,\chi)|^2. \tag{6.20}$$

Each character $\chi \bmod q$ is induced by some primitive character $\chi_1 \bmod q_1$, where q_1 divides q. Applying the triangle inequality, we see that (6.20) is

$$\ll\sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi \bmod q}|\theta'(I,\chi_1)|^2+\sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi \bmod q}|\theta'(I,\chi)-\theta'(I,\chi_1)|^2. \tag{6.21}$$

We consider the second quantity in (6.21). This is

$$\le\sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\left(\sum_{I\in\pi}\sum_{\chi \bmod q}|\theta'(I,\chi)-\theta'(I,\chi_1)|\right)^2.$$

Recalling the definitions of $\theta'(I,\chi)$ and $\theta'(I,\chi_1)$, we note that

$$|\theta'(I,\chi)-\theta'(I,\chi_1)| \le \sum_{\substack{p\in I\\ p|q}} \log p.$$

Thus, the second quantity in (6.21) is

$$\le \sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\left(\sum_{I\in\pi}\sum_{\chi \bmod q}\sum_{\substack{p\in I\\ p|q}}\log(p)\right)^2 = \sum_{q\le Q}\phi(q)\left(\sum_{\substack{p\le x\\ p|q}}\log(p)\right)^2.$$

Since $\sum_{p|q}\log(p)\le\log(q)$, this is

$$\le \sum_{q\le Q}\phi(q)\log^2(q) \ll Q^2\log^2(Q)\le xQ\log^2(x),$$

for $Q\le x$.

It now suffices to bound the first quantity in (6.21). Every primitive character $\chi_1 \bmod q_1$ induces characters modulo q for every q that is a multiple of q_1. Also, the set of primitive characters χ_1 inducing characters modulo q can be divided into primitive characters modulo each divisor of q. By applying the triangle inequality and maximizing separately for each divisor of q, we see that for each q:

$$\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi \bmod q}|\theta'(I,\chi_1)|^2 \le \sum_{q_1|q}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi_1 \bmod q_1}^{*}|\theta'(I,\chi_1)|^2.$$

Now summing over q and accounting for the multiple occurrences of each q_1, we have

$$\sum_{q\le Q}\frac{1}{\phi(q)}\max_{\pi\in\mathcal{P}_x}\sum_{\pi\in I}\sum_{\chi \bmod q}|\theta'(I,\chi_1)|^2 \le \sum_{q\le Q}\max_{\pi\in\mathcal{P}_x}\sum_{I\in\pi}\sum_{\chi \bmod q}^{*}|\theta'(I,\chi)|^2\left(\sum_{j\le\frac{Q}{q}}\frac{1}{\phi(jq)}\right).$$

As previously noted, this final sum over j is $\ll \phi(q)^{-1}\log(2Q/q)$. Hence the above quantity is

$$\ll \sum_{q\leq Q} \frac{\log(2Q/q)}{\phi(q)} \max_{\pi\in\mathcal{P}_x} \sum_{I\in\pi} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I,\chi)|^2.$$

As in the proof of Theorem 99, we break this sum over q into smaller ranges. For any $1 \leq U \leq Q$, we have

$$\sum_{U<q\leq 2U} \frac{\log(2Q/q)}{\phi(q)} \max_{\pi\in\mathcal{P}_x} \sum_{I\in\pi} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I,\chi)|^2$$

$$\ll U^{-1}\log(2Q/U) \sum_{q\leq 2U} \frac{q}{\phi(q)} \max_{\pi\in\mathcal{P}_x} \sum_{I\in\pi} \sideset{}{^*}\sum_{\chi \bmod q} |\theta(I,\chi)|^2 \tag{6.22}$$

(note that the change of notation from θ' to θ does not change any values). We may now apply Lemma 117 with $a_p = \log(p)$ for all primes p and $a_n = 0$ otherwise. We conclude that the righthand side of (6.22) is

$$\ll U^{-1}\log(2Q/U)(x+U^2)\log(x)\left(\sum_{p\leq x}\log^2(p)\right)$$

$$\ll U^{-1}\log(2Q/U)(x+U^2)x\log^2(x).$$

We define $Q_1 = \log^{A+1}(x)$. Setting $U = Q2^{-j}$ and summing over j from 0 to $J := \lceil \log(Q/Q_1)\rceil$, we see that

$$\sum_{Q_1<q\leq Q} \frac{\log(2Q/q)}{\phi(q)} \max_{\pi\in\mathcal{P}_x} \sum_{I\in\pi} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I,\chi)|^2 \ll Q^{-1}x\log^2(x)\sum_{j=0}^{J} 2^j(j+1)(x+Q^2 2^{-2j}).$$

Since $\sum_{j=0}^{\infty}(j+1)2^{-j}$ converges and $\sum_{j=0}^{J}(j+1)2^j \ll J2^J$, this quantity is $\ll Q_1^{-1}x^2\log^2(x)\log(Q) + xQ\log^2(x)$. Recalling that $Q_1 = \log^{A+1}(x)$ and $x\log^{-A}(x) \leq Q \leq x$, we see this is $\ll xQ\log^2(x)$ as required.

It only remains to bound the contribution from the values of $q \leq Q_1$. We observe that

$$\sum_{q \leq Q_1} \frac{\log(2Q/q)}{\phi(q)} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} \sideset{}{^*}\sum_{\chi \bmod q} |\theta'(I, \chi)|^2$$

$$\ll \log(Q) \sum_{q \leq Q_1} \frac{1}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} |\theta'(I, \chi)|^2.$$

Now, every primitive character modulo q for $q > 1$ is non-principal. For the principal character χ_0 modulo 1, the value of $\theta'(I, \chi_0)$ is 0 for any I, so we may rewrite our quantity as

$$\log(Q) \sum_{1 < q \leq Q_1} \frac{1}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \max_{\pi \in \mathcal{P}_x} \sum_{I \in \pi} |\theta(I, \chi)|^2.$$

Applying Lemma 109 for the constant $A + 1$, we see this is

$$\ll_A \log(Q) \sum_{1 < q \leq Q_1} \frac{1}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)},$$

for some positive constant $\tilde{c}_A$ depending only on A. Since there are $\phi(q)$ characters modulo q (and hence at most $\phi(q)$ primitive ones), this is $\ll_A Q_1 \log(Q) x^2 e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)}$. Recalling that $Q \leq x$ and $Q_1 = \log^{A+1}(x)$ and noting that $e^{-\tilde{c}_A \log^{\frac{1}{2}}(x)} \ll_A \log^{-2A}(x)$, we see this $\ll_A xQ \log^2(x)$. This completes the proof of Theorem 100.

6.5 A Variational Form of the Large Sieve Inequality

We now prove another variational form of Theorem 106. This will refine an estimate of Uchiyama stated below. The techniques are similar to those used above. We let $\mathcal{P}_{M,N}$ denote the set of partitions of $[M + 1, M + N]$.

Lemma 118. For all positive integers Q, M, N and complex numbers $\{a_n\}_{n=M+1}^{M+N}$,

$$\sum_{q\leq Q}\frac{q}{\phi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{\pi\in\mathcal{P}_{M,N}}\sum_{I\in\pi}|T(\chi,I)|^2 \ll \log^2(N)\left(N+Q^2\right)\sum_{n=M+1}^{N+M}|a_n|^2. \quad (6.23)$$

Proof. Without loss of generality, we assume that $N = 2^k$ for some k (rounding N up to the nearest power of 2 can be absorbed by the implicit constant). The interval from $M+1$ to $M+N$ can then be decomposed into dyadic intervals of the form $I_{c,\ell} := (M+(c-1)2^\ell, M+c2^\ell]$ for each ℓ from 0 to k, where c ranges from 1 to $2^{k-\ell}$. If we fix ℓ and let c vary, we refer to the resulting set of intervals as the dyadic intervals on *level* ℓ.

For a fixed q and primitive character $\chi \bmod q$, we consider a maximizing partition π^* in $\mathcal{P}_{M,N}$. By Lemma 111, every interval $I \in \pi^*$ can be decomposed as a union of $O(\log N)$ dyadic intervals of the form $I_{c,\ell}$ for varying c and ℓ values, such that there are at most 2 intervals included on each level. We let $D(I)$ denote the set of dyadic intervals in the decomposition of I. For each ℓ, $D_\ell(I)$ denotes the subset of intervals in $D(I)$ on level ℓ.

We can now express the square root of the left hand side of (6.23) as:

$$\sqrt{\sum_{q\leq Q}\frac{q}{\phi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\sum_{I\in\pi^*}\left|\sum_{J\in D(I)}T(\chi,J)\right|^2}.$$

We can alternatively express this as:

$$\sqrt{\sum_{q\leq Q}\frac{q}{\phi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\sum_{I\in\pi^*}\left|\sum_{\ell=0}^{k}\sum_{J\in D_\ell(I)}T(\chi,J)\right|^2}.$$

Applying the triangle inequality for the ℓ^2 norm, this quantity is

$$\leq \sum_{\ell=0}^{k} \sqrt{\sum_{q\leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \sum_{I\in\pi^*} \left| \sum_{J\in D_\ell(I)} T(\chi, J) \right|^2}. \tag{6.24}$$

For a fixed ℓ, we consider the quantity

$$\sum_{q\leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \sum_{I\in\pi^*} \left| \sum_{J\in D_\ell(I)} T(\chi, J) \right|^2. \tag{6.25}$$

We note that the innermost sum contains at most two intervals J, since the dyadic decomposition of each I contains at most two intervals on level ℓ. Noting that $|a+b|^2 \ll |a|^2 + |b|^2$ holds for all complex numbers a and b and that each dyadic interval on level ℓ can occur in the decomposition of at most one $I \in \pi^*$, the quantity in (6.25) is

$$\ll \sum_{q\leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \sum_{c=1}^{2^{k-\ell}} |T(\chi, I_{c,\ell})|^2.$$

Now the innermost sum is simply over the set of dyadic intervals on level ℓ. Reordering the finite sums, this is

$$= \sum_{c=1}^{2^{k-\ell}} \sum_{q\leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} |T(\chi, I_{c,\ell})|^2.$$

For each c, we can apply Theorem 106 to obtain:

$$\sum_{q\leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} |T(\chi, I_{c,\ell})|^2 \ll (2^\ell + Q^2) \sum_{n\in I_{c,\ell}} |a_n|^2.$$

Thus, the quantity in (6.25) is $\ll (2^\ell + Q^2) \sum_{n=M+1}^{M+2^k} |a_n|^2$.

Substituting this back into (6.24), we see that the square root of the left hand side of (6.23) is

$$\ll \sum_{\ell=0}^{k} \sqrt{(2^\ell + Q^2) \sum_{n=M+1}^{M+2^k} |a_n|^2}.$$

Hence, the left hand side of (6.23) is

$$\ll \left(\sum_{\ell=0}^{k} \sqrt{2^\ell + Q^2} \right)^2 \sum_{n=M+1}^{M+2^k} |a_n|^2.$$

Recalling that $2^k = N$ and loosely bounding $2^\ell + Q^2 \leq 2^k + Q^2$ for all ℓ, we see this is

$$\ll \left(k\sqrt{2^k + Q^2} \right)^2 \sum_{n=M+1}^{M+2^k} |a_n|^2$$

$$= k^2(2^k + Q^2) \sum_{n=M+1}^{M+2^k} |a_n|^2 \ll \log^2(N)(N + Q^2) \sum_{n=M+1}^{M+N} |a_n|^2.$$

□

We note that this refines Uchiyama's Maximal large sieve inequality [67], which states:

Lemma 119. For all positive integers Q, M, N and complex numbers $\{a_n\}_{n=M+1}^{M+N}$,

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sideset{}{^*}\sum_{\chi \bmod q} \max_{I \subseteq [N]} |T(\chi, I)|^2 \ll \log^2(N) \left(N + Q^2\right) \sum_{n=M+1}^{N+M} |a_n|^2. \tag{6.26}$$

Montgomery [45] has asked if the $\log^2(N)$ can be removed. We do not have an answer to this question (though we obtain a lower bound on a

related quantity in [37] and Chapter 7). We note that the $\log^2(N)$ cannot be completely removed in our variational refinement.

To see this, we use the lemma below, which follows easily from Lemma 22 in [41] (Lemma 59 in Chapter 4) and the Cauchy-Schwarz inequality:

Lemma 120. Let $c_1, \ldots, c_N$ denote complex numbers $|c_i| \geq \delta$, for some $\delta > 0$. Let $X_1, \ldots, X_N$ denote independent Gaussian random variables each with mean 0 and variance 1. Then

$$\mathbb{E}\left[\sup_{\pi \in \mathcal{P}_N} \sum_{I \in \pi} \left| \sum_{n \in I} c_n X_n \right|^2 \right] \gg \delta^2 N \log\log(N)$$

Strictly speaking, the lemma in [41] is stated for real $c_1, \ldots, c_N$, but it can easily be deduced for complex numbers by splitting into real and imaginary parts. Now we consider (118) with interval $[N]$ and $a_n = X_n$ for each $n \in [N]$. To apply Lemma 120 for each q and each character modulo q, we consider only the indices n such that n is coprime to q. On these values, the character will be nonzero. We let $C(q)$ denote the number of these indices for each q. Then, from Lemma 120, the expectation of the left hand side can be estimated by

$$\gg \sum_{q \leq Q} q \cdot C(q) \cdot \log\log(C(q)). \tag{6.27}$$

Now, we note that $\sum_{q \leq Q} C(q)$ is equal to the number of pairs (n, q) such that n and q are coprime. This is also equal to $\sum_{n=1}^{N} Q\frac{\phi(n)}{n}$. By Theorem 330 in [25], $\sum_{n=1}^{N} \phi(n) = \frac{3}{\pi^2}N^2 + O(N\log(N))$, which implies $\sum_{n=1}^{N} \frac{\phi(n)}{n} \gg N$. Thus, $\sum_{q \leq Q} C(q) \gg QN$. It follows that there exist positive constants ϵ, δ

such that $C(q) \geq \epsilon N$ for at least δQ values of q. Hence, the quantity in (6.27) is $\gg Q^2 N \log\log(N)$, while the expectation of the sum of squares of the $a_n = X_n$ will be $\ll N$. Thus, at least when $N \ll Q^2$, one needs at least a factor of $\log\log(N)$ in (118). Refining the gap between $\log\log(N)$ and $\log^2(N)$ would be interesting.

Chapter 7

Maximal Operators Associated to Multiplicative Characters

7.1 Introduction

The Carleson-Hunt inequality states that there exists a finite constant C such that

$$\left(\int_0^1 \left| \max_{\ell} \left| \sum_{n=0}^{\ell} a_n e(xn) \right| \right|^2 dx \right)^{1/2} \leq C \left(\sum_{n=0}^{\infty} |a_n|^2 \right)^{1/2} \tag{7.1}$$

for any sequence of complex numbers $\{a_n\}_{n=1}^{\infty}$ (denoting $e(x) := e^{2\pi i x}$). It is not hard to see that this is equivalent to the discretized claim that

$$\left(\frac{1}{N} \sum_{a=0}^{N-1} \left| \max_{\ell < N} \left| \sum_{n=0}^{\ell} a_n e(an/N) \right| \right|^2 \right)^{1/2} \leq C \left(\sum_{n=0}^{N-1} |a_n|^2 \right)^{1/2} \tag{7.2}$$

holds with a universal constant C, independent of N. This can be viewed as a natural analog of the Carleson-Hunt inequality in the family of additive groups, $\mathbb{Z}_N$. The fact that this inequality implies (7.1) follows from an easy approximation argument. The reverse implication is slightly more subtle but can be obtained, for instance, from Montgomery's maximal large sieve inequality [45] (Theorem 2).

In light of (7.2), it is natural to consider the analogous maximal operator on the family of multiplicative groups, $\mathbb{Z}_N^*$. That is, we consider the inequality

$$\left(\frac{1}{\phi(N)} \sum_{\chi \bmod N} \left| \max_{\ell < N} \left| \sum_{\substack{n=1 \\ (n,N)=1}}^{\ell} a_n \chi(n) \right| \right|^2 \right)^{1/2} \leq \Delta(N) \left(\sum_{\substack{n=1 \\ (n,N)=1}}^{N-1} |a_n|^2 \right)^{1/2} \tag{7.3}$$

where the sum $\sum_{\chi \bmod N}$ is over all Dirichlet characters modulo N, $\phi(N)$ is the Euler totient function, and $\Delta(N)$ is the smallest value such that the inequality holds. We are interested in the growth of the function $\Delta(N)$. It is easy to see that $\Delta(N) \ll \log(N)$ by the Rademacher-Menshov theorem. By comparison to (7.2), one might hope that $\Delta(N) \ll 1$. In fact, we show in Section 2 that if one could take $\Delta(N) = O(1)$ in (7.3), then the Carleson-Hunt inequality for the trigonometric system would be an easy corollary. We note that in the case that $a_n = 1$ for all n it follows from work of Montgomery and Vaughan [48] that (7.3) holds with a universal constant independent of N.

Unfortunately, it turns out that $\Delta(N) \neq O(1)$. We prove:

Theorem 121. There exists a subset $\mathcal{S}$ of primes of positive relative density such that for every $p \in \mathcal{S}$,

$$(\log \log(p))^{1/4} \ll \Delta(p). \tag{7.4}$$

Thus $(\log \log(N))^{1/4} \ll \Delta(N)$ holds infinitely often. It remains an interesting problem to establish sharp bounds on the growth of $\Delta(N)$. In

particular, any refinement of the upper bound $\Delta(N) \ll \log(N)$ (from the Rademacher-Menshov theorem) would be extremely interesting.

7.2 Connection with the Carleson-Hunt inequality

In this section we prove that if (7.3) with $\Delta(N) = O(1)$ did hold then the classical Carleson-Hunt inequality (7.1) would easily follow. By a standard density argument, it suffices to prove (7.1) for finite sequences $\{a_n\}_{n=1}^k$ as long as the constant C does not depend on k. Indeed, once k is fixed, we will show that

$$\left(\frac{1}{M}\sum_{x=1}^{M}\left|\max_{\ell<k}\left|\sum_{n=0}^{\ell}a_n e(xn/M)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_n|^2\right)^{1/2} \tag{7.5}$$

holds for an infinite increasing sequence of integral M's and a constant C independent of k. Clearly, this is sufficient as the sum on the left will converge to the Riemann integral over the unit interval. Consider a large prime $2^k < p$. Now we apply (7.3) with $\Delta(p) \leq C$, and associating the coefficient a_i to $\chi(2^i)$ we have

$$\left(\frac{1}{\phi(p)}\sum_{\chi \bmod p}\left|\max_{\ell<k}\left|\sum_{i=1}^{\ell}a_i\chi(2^i)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_k|^2\right)^{1/2}. \tag{7.6}$$

We let α be a generator of $\mathbb{Z}_p^*$. For $g \in \mathbb{Z}_p^*$, we define $\nu(g)$ to be the element of $[p-1]$ such that $\alpha^{\nu(g)} = g$. We may express $\chi(g) = e(a\nu(g)/(p-1))$

(for some $0 \leq a < p-1$). Thus $\nu(g)$ can be thought of as a permutation of $[p-1]$. In addition, it follows from this definition that $\nu(2^i) = i\nu(2)$. We thus have that (7.6) can be expressed as:

$$\left(\frac{1}{p-1}\sum_{x=1}^{p-1}\left|\max_{\ell<k}\left|\sum_{i=1}^{\ell}a_i e\left(\frac{i\nu(2)x}{p-1}\right)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_k|^2\right)^{1/2}. \tag{7.7}$$

We define coprime $L, M \in \mathbb{Z}$ by $\frac{\nu(2)}{p-1} = \frac{L}{M}$. We observe that $M > \log_2(p)$. To see this, consider that $M\nu(2) = L(p-1)$ implies $2^M = \alpha^{L(p-1)} \equiv 1$. Note that $M|(p-1)$. Substituting this into (7.7), we have

$$\left(\frac{1}{p-1}\sum_{x=1}^{p-1}\left|\max_{\ell<k}\left|\sum_{i=1}^{\ell}a_i e\left(\frac{iLx}{M}\right)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_k|^2\right)^{1/2}. \tag{7.8}$$

Since $M|(p-1)$ and $e\left(\frac{iLx}{M}\right)$ has period M as a function of x, this can be rewritten as:

$$\left(\frac{1}{M}\sum_{x=1}^{M}\left|\max_{\ell<k}\left|\sum_{i=1}^{\ell}a_i e\left(\frac{iLx}{M}\right)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_k|^2\right)^{1/2}. \tag{7.9}$$

We perform the change of variable $Lx \to y$ to obtain

$$\left(\frac{1}{M}\sum_{y=1}^{M}\left|\max_{\ell<k}\left|\sum_{i=1}^{\ell}a_i e\left(\frac{iy}{M}\right)\right|\right|^2\right)^{1/2} \leq C\left(\sum_{n=1}^{k}|a_k|^2\right)^{1/2}. \tag{7.10}$$

for some $M \gg \log(p)$. This completes the proof.

Remark 122. One could also deduce the Carleson-Hunt inequality for Walsh series from the claim that $\Delta(N) = O(1)$. We briefly sketch the argument.

Choose N to be the product of d distinct odd primes. Then Z_N^* will contain an isomorphic copy of the group Z_2^d. The characters of this group are distributionally equivalent with the first 2^d Walsh functions. The maximal operator on $\mathbb{Z}_N^*$ will induce some ordering on these functions other than the standard ordering. It follows, however, from a combinatorial lemma of Bourgain [4] (Lemma 2.3) that there is a function $B(d)$ (tending to infinity) such that any ordering of the first 2^d Walsh functions must contain a subsequence of length $B(d)$ distributionally equivalent to the first $B(d)$ Walsh functions in the standard ordering.

7.3 Auxiliary Results

In this section we collect some auxiliary results that will be needed in the proof of Theorem 121. We first note the following result from [19]:

Proposition 123. (Fouvry) Let $\mathcal{P}(N)$ denote the largest prime divisor of N. Then for a positive proportion of the primes p, we have $\mathcal{P}(p-1) \geq Bp^{.6687}$ for some positive constant B.

For our purposes, $\mathcal{P}(p-1) \gg p^{\frac{1}{2}+\epsilon}$ for any fixed $\epsilon > 0$ would suffice. We will need a quantitative multi-dimensional form of Weyl's criterion which can be found in Chapter 2 of [33]:

Proposition 124. (Erdös-Turan-Koksma) Let P denote a sequence of N points, $x_1, x_2, \ldots, x_N \in [0,1]^s$. Define the discrepancy of this sequence as

$$D_N(x_1, x_2, \ldots, x_N) := \sup_{I \in \mathcal{B}} \left| \frac{|I \cap P|}{N} - |I| \right|$$

where $\mathcal{B}$ denotes the set of all s-dimensional boxes, and $|I|$ denotes the measure of I. Furthermore, for $h \in \mathbb{Z}^s$ let

$$r(h) := \prod_{i=1}^{s} \max(1, |h_i|).$$

Then, for all $m \in \mathbb{N}$, we have that

$$D_N(x_1, x_2, \ldots, x_N) \leq 2s^2 3^{s+1} \left(\frac{1}{m} + \sum_{\substack{h \in \mathbb{Z}^s \\ 0 < ||h||_\infty \leq m}} \frac{1}{r(h)} \left| \frac{1}{N} \sum_{n=1}^{N} e(\langle h, x_n \rangle) \right| \right). \tag{7.11}$$

We will also need the following version of Weil's character sum estimate. This can be found, for instance, on page 45 of [62].

Proposition 125. (Weil) Let p be a prime and $g(x) = g_n x^n + \ldots + g_0$ a degree n polynomial ($0 < n < p$) with integer coefficients such that p does not divide g_n. Then,

$$\left| \sum_{x=0}^{p-1} e(g(x)/p) \right| \leq (n-1)p^{1/2}. \tag{7.12}$$

We will also use the following quantitative form of Kolmogorov's rearrangement theorem due to Nakata [49] (Lemma 4).

Proposition 126. (Nakata) There exist universal real constants $c_1, c_2 > 0$ with the following property. For any $N \in \mathbb{N}$, there exists a permutation $\sigma : [N] \to [N]$ and complex numbers $\{a_n\}_{n=1}^N$ satisfying $\sum_{n=1}^N |a_n|^2 = 1$ such that

$$\left|\{x \in [0,1] : \widetilde{\mathcal{M}}(x) > c_1 \log^{1/4}(N)\}\right| \geq c_2$$

holds where

$$\widetilde{\mathcal{M}}(x) := \max_{\ell \leq N} \left| \sum_{n=1}^{\ell} a_n e(\sigma(n)x) \right|.$$

We remark that Nakata has a slightly stronger refinement of Kolmogorv's rearrangement theorem [50] where there are some additional iterated logarithmic factors. However, the result there is formulated in a slightly different way and it would require some additional work to derive a statement sufficient for our purposes from it. For the sake of simplicity, we will not pursue this modification here. A simple averaging argument gives the following discrete version of Proposition 126.

Corollary 127. There exists universal real constants $c_1, c_2 > 0$ with the following property. For any $N \in \mathbb{N}$, there exists a permutation $\sigma : [N] \to [N]$ and complex numbers $\{b_n\}_{n=1}^N$ satisfying $\sum_{n=1}^N |b_n|^2 = 1$ such that

$$\left|\{a \in [M] : \mathcal{M}(a) > c_1 \log^{1/4}(N)\}\right| \geq c_2 M$$

holds for any positive integer M, where $\mathcal{M} : [N] \to \mathbb{R}$ is defined by

$$\mathcal{M}(a) := \max_{\ell \leq N} \left| \sum_{n=1}^{\ell} b_n e(\sigma(n)a/M) \right|.$$

From these results, we obtain

Proposition 128. We will denote the fractional part of $a \in \mathbb{R}$ by $\{a\}$. We let p, q denote primes such that $q|p-1$ and $q \geq Bp^{.6687}$. We let $\mathcal{A}$ denote the subgroup of order q in $\mathbb{Z}_p^*$ (i.e. $\mathcal{A} = \left\{ g^{\frac{p-1}{q}} : g \in \mathbb{Z}_p^* \right\}$). There exists a universal constant $\delta > 0$ such that for any $s < \delta \log^{1/2}(p)$, and any permutation $\sigma : [s] \to [s]$, there exists an $x \in \mathcal{A}$ such that

$$\left\{ \frac{x^{\sigma(1)}}{p} \right\} < \left\{ \frac{x^{\sigma(2)}}{p} \right\} < \ldots < \left\{ \frac{x^{\sigma(s)}}{p} \right\}.$$

Proof. We let $g_1, \ldots, g_q$ denote the elements of $\mathcal{A}$ inside $\mathbb{Z}_p^*$ in the order induced by $\mathbb{Z}_p^*$. For each i from 1 to q, we define

$y_i \in [0,1]^s$ as $y_i = \left(\left\{ \frac{g_i^1}{p} \right\}, \left\{ \frac{g_i^2}{p} \right\}, \ldots, \left\{ \frac{g_i^s}{p} \right\} \right)$. We then divide $[0,1]^s$ into $(3s)^s$ boxes of equal measure by dividing each coordinate into $3s$ equal intervals in the obvious way. The conclusion will now follow if we show that there exists a point y_i in each of the $(3s)^s$ boxes. To see this, consider the $3s$ intervals in each coordinate as being s groups of 3 intervals each, and let I_j^k denote the "middle" interval of the j^{th} group in the k^{th} coordinate. Note that I_j^k and $I_{j'}^k$ for $j \neq j'$ do not intersect. Given a permutation σ, it suffices to obtain a point in the box whose k^{th} side is equal to $I_{\sigma(k)}^k$.

To establish the existence of a point y_i in every box, it suffices to show

$D(y_1, y_2, \ldots, y_q) < (3s)^{-s}$. Invoking Proposition 124, we have that

$$D(y_1, y_2, \ldots, y_q) \leq 2s^2 3^{s+1} \left(\frac{1}{m} + \sum_{0<||h||_\infty \leq m} \frac{1}{r(h)} \left| \frac{1}{q} \sum_{i=1}^{q} e(\langle h, y_i \rangle) \right| \right). \quad (7.13)$$

We define

$$f_h(x) = h_s x^{s\frac{p-1}{q}} + h_{s-1} x^{(s-1)\frac{p-1}{q}} + \ldots + h_1 x^{\frac{p-1}{q}}.$$

We then have:

$$\frac{1}{q} \sum_{i=1}^{q} e(\langle h, y_i \rangle) = \frac{1}{p-1} \left(-1 + \sum_{x=0}^{p-1} e(f_h(x)/p) \right).$$

We note that

$$\sum_{0<||h||_\infty \leq m} \frac{1}{r(h)} = \left(1 + \sum_{j=1}^{m} j^{-1} \right)^s \leq C^s \log^s(m)$$

for some constant C. Whenever some h_i is not divisible by p, we may apply Proposition 125 to bound the quantity $\left| \sum_{x=0}^{p-1} e(f_h(x)/p) \right|$. We will choose $m < p$ so that all h's will have this property. We may thus bound the right hand side of (7.13) by

$$\leq 2s^2 3^{s+1} \left(\frac{1}{m} + sp^{-.1687} C^s \log^s(m) \right), \quad (7.14)$$

when $m < p$ (for some new value of C). Here, we have applied Proposition 125 to polynomials of degree $\leq s\left(\frac{p-1}{q}\right)$.

For any constant $\delta_2 > 0$, we can set $m = s^{\delta_1 s}$ for some constant δ_1 sufficiently large so that (7.14) is

$$\leq s^{-\delta_2 s} + p^{-.1687} s C^s (\delta_1 s \log(s))^s. \quad (7.15)$$

Fixing δ_2 such that $s^{-\delta_2 s} \leq \frac{1}{2}(3s)^{-s}$ for all $s > 1$ say (note that the Proposition is trivial for $s = 1$), we may then require that s satisfy $p \geq s^{\delta_3 s}$ for δ_3 sufficiently large so that $\delta_3 > \delta_1$ and the quantity in (7.15) is $< (3s)^{-s}$. We observe that $s^{\delta_3 s} \leq p$ is equivalent to $\delta_3 s \log(s) \leq \log(p)$, which can be guaranteed by $s \leq \delta \log^{1/2}(p)$ for a suitable choice of δ. □

7.4 Proof of the Main Theorem

We define $\mathcal{S}$ to be the set of primes p such that there exists a prime q dividing $p-1$ with $q \geq Bp^{.6687}$. By Proposition 123, this is an infinite set of positive relative density in the primes. For each $p \in \mathcal{S}$, we let $\mathcal{A}$ denote the subgroup of order q in $\mathbb{Z}_p^*$. Our goal is to define suitable coefficients supported on $\mathcal{A}$ to show that $\Delta(p)$ is $\gg (\log\log(p))^{\frac{1}{4}}$.

We enumerate the elements of $\mathcal{A}$ in the natural way (that is so their smallest representatives in $\mathbb{Z}_+$ are ordered in increasing order), say $\{g_n\}_{n=1}^q$. Next, we let α be a generator of $\mathcal{A}$. We define $\nu(g_n)$ to be the element of $[q]$ such that $\alpha^{\nu(g_n)} = g_n$. By restricting the coefficients in (7.3) to $\mathcal{A}$, we see that the quantity in (7.3) to be bounded is:

$$\left(\frac{1}{p-1}\sum_{\chi \bmod p}\max_{\ell \leq q}\left|\sum_{n=1}^{\ell} a_n \chi(g_n)\right|^2\right)^{\frac{1}{2}} = \left(\frac{1}{q}\sum_{x=1}^{q}\max_{\ell \leq q}\left|\sum_{n=1}^{\ell} a_n e(\nu(g_n)x/q)\right|^2\right)^{\frac{1}{2}}. \tag{7.16}$$

This follows because restricting $\chi \bmod p$ to $\mathcal{A}$ yields a character on $\mathcal{A}$.

Let $s = \lfloor \delta \log^{1/2}(p) \rfloor$ and $\sigma : [s] \to [s]$ be the permutation in Corollary 127, along with coefficients $b_1, \ldots, b_s$ such that $\sum_{m=1}^{s} |b_m|^2 = 1$. By Proposi-

tion 128, we have a $g \in \mathcal{A}$ such that

$$\left\{\frac{g^{\sigma(1)}}{p}\right\} < \left\{\frac{g^{\sigma(2)}}{p}\right\} < \ldots < \left\{\frac{g^{\sigma(s)}}{p}\right\}.$$

Of course $g^{\sigma(1)}, g^{\sigma(2)}, \ldots, g^{\sigma(s)} \in \mathcal{A}$.

By restricting the support of our coefficients to these terms in (7.16) and using $b_1, \ldots, b_s$ as our coefficients, it suffices to consider the quantity

$$\left(\frac{1}{q}\sum_{x=1}^{q}\left|\max_{\ell<s}\left|\sum_{m=0}^{\ell} b_m e(\nu(g^{\sigma(m)})x/q)\right|\right|^2\right)^{1/2}$$
$$= \left(\frac{1}{q}\sum_{x=1}^{q}\left|\max_{\ell<s}\left|\sum_{m=0}^{\ell} b_m e(\sigma(m)\nu(g)x/q)\right|\right|^2\right)^{1/2} \tag{7.17}$$

where we have exploited the fact that $\nu(g^i) = i\nu(g)$. Finally, by the change of variables $x\nu(g) \to y$, we have

$$chmaxd : DirichletMax4 = \left(\frac{1}{q}\sum_{y=1}^{q}\left|\max_{\ell\leq s}\left|\sum_{m=1}^{\ell} b_m e(\sigma(m)y/q)\right|\right|^2\right)^{1/2}. \tag{7.18}$$

Applying Corollary 127 with $M = q$, we see that this quantity is $\gg (\log(s))^{1/4} \gg (\log(\log(p)))^{1/4}$. This completes the proof.

7.5 Concluding Remarks

There is some flexibility in the techniques applied in the proof of Theorem 121, and variants of these arguments should give lower bounds on $\Delta(N)$ for some more general N. However, a more delicate analysis will be needed to obtain a uniform lower bound in N.

It is consistent with our knowledge that one might be able to replace the $\log^{1/4}(N)$ in Proposition 126 with a $\log(N)$. This would allow one to strengthen the conclusion of Theorem 121 to $\log\log(p) \ll \Delta(N)$. However, the Rademacher-Menshov theorem prevents the conclusion of Proposition 126 from holding with any function growing faster than $\log(N)$. Thus a lower bound of $\log\log(N)$ would be the limitation of the approach developed here.

One can interpret the proof of Theorem 121 as showing that the permutation of $[q]$ defined by $\nu(\cdot)$ is sufficiently pseudorandom that it contains the same increasing subsequences that could be found in a random permutation (with large probability). In connection with this interpretation, we note that Bourgain [4] has shown that the L^2 norm of the maximal function of a randomly ordered bounded orthonormal system is at most $\log\log(N)$ (with large probability). Perhaps this is some indication that the correct bound on $\Delta(N)$ may be near $\log\log(N)$, or at least somewhat smaller than the trivial bound of $\log(N)$.

Bibliography

[1] N. Alon and P. Erdős. An application of graph theory to additive number theory. *European J. Combin.*, 6(3):201–203, 1985.

[2] Y. Benyamini and Y. Gordon. Random factorization of operators between Banach spaces. *J. Analyse Math.*, 39:45–74, 1981.

[3] J. Bourgain. Bounded orthogonal systems and the $\Lambda(p)$-set problem. *Acta Math.*, 162(3-4):227–245, 1989.

[4] J. Bourgain. On Kolmogorov's rearrangement problem for orthogonal systems and Garsia's conjecture. In *Geometric aspects of functional analysis (1987–88)*, volume 1376 of *Lecture Notes in Math.*, pages 209–250. Springer, Berlin, 1989.

[5] J. Bourgain. Λ_p-sets in analysis: results, problems and related aspects. In *Handbook of the geometry of Banach spaces, Vol. I*, pages 195–232. North-Holland, Amsterdam, 2001.

[6] A. Carbery. Harmonic analysis on vector spaces over finite fields. *http://www.maths.ed.ac.uk/uploads/assets/7_fflpublic.pdf*.

[7] A. Y. Cheer and D. A. Goldston. Longer than average intervals containing no primes. *Trans. Amer. Math. Soc.*, 304(2):469–486, 1987.

[8] S. Chevet. Séries de variables aléatoires gaussiennes à valeurs dans $E\hat{\otimes}_\varepsilon F$. Application aux produits d'espaces de Wiener abstraits. In *Séminaire sur la Géométrie des Espaces de Banach (1977–1978)*, pages Exp. No. 19, 15. École Polytech., Palaiseau, 1978.

[9] M. Christ and A. Kiselev. Maximal functions associated to filtrations. *J. Funct. Anal.*, 179(2):409–425, 2001.

[10] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[11] R. Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer, Heidelberg, fourth edition, 2010.

[12] J. L. Doob. *Stochastic processes*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1990. Reprint of the 1953 original, A Wiley-Interscience Publication.

[13] P. Erdös. The difference of consecutive primes. *Duke Math. J.*, 6:438–441, 1940.

[14] P. Erdős. Some applications of Ramsey's theorem to additive number theory. *European J. Combin.*, 1(1):43–46, 1980.

[15] P. Erdős. Extremal problems in number theory, combinatorics and geometry. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 51–70, Warsaw, 1984. PWN.

[16] P. Erdős, J. Nešetřil, and V. Rödl. On Pisier type problems and results (combinatorial applications to number theory). In *Mathematics of Ramsey theory*, volume 5 of *Algorithms Combin.*, pages 214–231. Springer, Berlin, 1990.

[17] N. Etemadi. On some classical results in probability theory. *Sankhyā Ser. A*, 47(2):215–221, 1985.

[18] G. Folland. *Real analysis*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1999. Modern techniques and their applications, A Wiley-Interscience Publication.

[19] É. Fouvry. Théorème de Brun-Titchmarsh: application au théorème de Fermat. *Invent. Math.*, 79(2):383–407, 1985.

[20] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[21] A. Garsia. Existence of almost everywhere convergent rearrangements for Fourier series of L_2 functions. *Ann. of Math. (2)*, 79:623–629, 1964.

[22] A. Garsia. *Topics in almost everywhere convergence*, volume 4 of *Lectures in Advanced Mathematics*. Markham Publishing Co., Chicago, Ill., 1970.

[23] H. Halberstam and K. Roth. *Sequences*. Springer-Verlag, New York, second edition, 1983.

[24] G. H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities*. Cambridge, at the University Press, 1952. 2d ed.

[25] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[26] W. Hoeffding. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc.*, 58:13–30, 1963.

[27] C. Hooley. On the Barban-Davenport-Halberstam theorem. IV. *J. London Math. Soc. (2)*, 11(4):399–407, 1975.

[28] C. Hooley. On theorems of Barban-Davenport-Halberstam type. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 195–228. A K Peters, Natick, MA, 2002.

[29] 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(2):611–628, 2008.

[30] A. Iosevich and D. Koh. Extension theorems for paraboloids in the finite field setting. *Math. Z.*, 266(2):471–487, 2010.

[31] A. Iosevich and D. Koh. Extension theorems for spheres in the finite field setting. *Forum Math.*, 22(3):457–483, 2010.

[32] R. Jones and G. Wang. Variation inequalities for the Fejér and Poisson kernels. *Trans. Amer. Math. Soc.*, 356(11):4493–4518 (electronic), 2004.

[33] L. Keĭpers and G. Niderreĭter. *Ravnomernoe raspredelenie posledovatelnostei*. "Nauka", Moscow, 1985. Translated from the English by B. B. Pokhodzeĭ and I. M. Sobol′, Translation edited and with a preface by S. M. Ermakov.

[34] I. Klemes. Examples of $\Lambda(4)$ sets E and a graph structure in $E \times E$. *Studia Math.*, 133(2):101–120, 1999.

[35] M. A. Krasnosel′skiĭ and Ja. B. Rutickiĭ. *Convex functions and Orlicz spaces*. Translated from the first Russian edition by Leo F. Boron. P. Noordhoff Ltd., Groningen, 1961.

[36] A. Lewko and M. Lewko. An exact asymptotic for the square variation of partial sum processes. *Preprint (arxiv.org)*.

[37] A. Lewko and M. Lewko. Maximal operators associated to multiplicative characters. *Preprint (arxiv.org)*.

[38] A. Lewko and M. Lewko. A variational Barban-Davenport-Halberstam theorem. *J. Number Theory, to appear*.

[39] A. Lewko and M. Lewko. On the structure of sets of large doubling. *European J. Combin.*, 32(5):688–708, 2011.

[40] A. Lewko and M. Lewko. Endpoint restriction estimates for the paraboloid over finite fields. *Proc. Amer. Math. Soc*, 140, 2012.

[41] A. Lewko and M. Lewko. Estimates for the square variation of partial sums of fourier series and their rearrangements. *J. Funct. Anal.*, 262:2561–2607, 2012.

[42] M. Marcus and G. Pisier. *Random Fourier series with applications to harmonic analysis*, volume 101 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J., 1981.

[43] Y. Meyer. Endomorphismes des idéaux fermés de $L^1(G)$, classes de Hardy et séries de Fourier lacunaires. *Ann. Sci. École Norm. Sup. (4)*, 1:499–580, 1968.

[44] G. Mockenhaupt and T. Tao. Restriction and Kakeya phenomena for finite fields. *Duke Math. J.*, 121(1):35–74, 2004.

[45] H. Montgomery. Maximal variants of the large sieve. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):805–812 (1982), 1981.

[46] H. Montgomery and J. Vaaler. Maximal variants of basic inequalities. In *Proceedings of the Congress on Number Theory (Spanish) (Zarauz, 1984)*, pages 181–197, Bilbao, 1989. Univ. País Vasco-Euskal Herriko Unib.

[47] H. Montgomery and R. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[48] H. L. Montgomery and R. C. Vaughan. Mean values of character sums. *Canad. J. Math.*, 31(3):476–487, 1979.

[49] S. Nakata. On the divergence of rearranged Fourier series of square integrable functions. *Acta Sci. Math. (Szeged)*, 32:59–70, 1971.

[50] S. Nakata. On the divergence of rearranged trigonometric series. *Tôhoku Math. J. (2)*, 27(2):241–246, 1975.

[51] J. Nešetřil and V. Rödl. Two proofs in combinatorial number theory. *Proc. Amer. Math. Soc.*, 93(1):185–188, 1985.

[52] R. Oberlin, A. Seeger, T. Tao, C. Thiele, and J. Wright. A variation norm carleson theorem. *Journal of the European Mathematics Society, to appear.*

[53] K. O'Bryant. A complete annotated bibliography of work related to sidon sequences. *Electronic Journal of Combinatorics*, 11(39), 2004.

[54] A. M. Olevskiĭ. *Fourier series with respect to general orthogonal systems.* Springer-Verlag, New York, 1975. Translated from the Russian by B. P. Marshall and H. J. Christoffers, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 86.

[55] V. V. Petrov. *Sums of independent random variables.* Springer-Verlag, New York, 1975. Translated from the Russian by A. A. Brown, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 82.

[56] G. Pisier. Ensembles de Sidon et processus gaussiens. *C. R. Acad. Sci. Paris Sér. A-B*, 286(15):A671–A674, 1978.

[57] G. Pisier. De nouvelles caractérisations des ensembles de Sidon. In *Mathematical analysis and applications, Part B*, volume 7 of *Adv. in Math. Suppl. Stud.*, pages 685–726. Academic Press, New York, 1981.

[58] J. Qian. The p-variation of partial sum processes and the empirical process. *Ann. Probab.*, 26(3):1370–1383, 1998.

[59] B. Rosén. On an inequality of Hoeffding. *Ann. Math. Statist.*, 38:382–392, 1967.

[60] H. Rosenthal. On the subspaces of L^p spanned by sequences of independent random variables. *Israel J. Math.*, 8:273–303, 1970.

[61] W. Rudin. Trigonometric series with gaps. *J. Math. Mech.*, 9:203–227, 1960.

[62] W. Schmidt. *Equations over finite fields. An elementary approach.* Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin, 1976.

[63] A. Selberg. On the normal density of primes in small intervals, and the difference between consecutive primes. *Arch. Math. Naturvid.*, 47(6):87–105, 1943.

[64] E. Stein. *Topics in harmonic analysis related to the Littlewood-Paley theory.* Annals of Mathematics Studies, No. 63. Princeton University Press, Princeton, N.J., 1970.

[65] T. Tao. Some recent progress on the restriction conjecture. In *Fourier analysis and convexity*, Appl. Numer. Harmon. Anal., pages 217–243. Birkhäuser Boston, Boston, MA, 2004.

[66] T. Tao and V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012].

[67] S. Uchiyama. The maximal large sieve. *Hokkaido Math. J.*, 1:117–126, 1972.

[68] J. Vaaler. Some extremal functions in Fourier analysis. *Bull. Amer. Math. Soc. (N.S.)*, 12(2):183–216, 1985.

[69] D. Yang and T. Lyons. The partial sum process of orthogonal expansion as geometric rough process with fourier series as an example—an improvement of menshov-rademacher theorem. *arXiv:1109.1072, arxiv.org*.

[70] D. Yen, R. Oberlin, and A. Eyvindur. Variational bounds for a dyadic model of the bilinear hilbert transform. *arXiv:1203.5135, arxiv.org*.

Vita

Mark Lewko was born in Claremont, New Hampshire on May 6, 1983, the son of Zachary F. Lewko and Viola F. Lewko. He received the Bachelor of Arts degree in Mathematics from Princeton University in 2005. He began his graduate studies at the University of Texas at Austin in the Fall of 2006. In December of 2009 he married Allison Bishop Lewko.

Permanent address: mlewko@gmail.com

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.