



On Superorthogonality

Lillian B. Pierce¹ 

Received: 21 July 2020 / Accepted: 6 January 2021
© Mathematica Josephina, Inc. 2021

Abstract

In this survey, we explore how superorthogonality amongst functions in a sequence f_1, f_2, f_3, \dots results in direct or converse inequalities for an associated square function. We distinguish between three main types of superorthogonality, which we demonstrate arise in a wide array of settings in harmonic analysis and number theory. This perspective gives clean proofs of central results, and unifies topics including Khintchine's inequality, Walsh–Paley series, discrete operators, decoupling, counting solutions to systems of Diophantine equations, multicorrelation of trace functions, and the Burgess bound for short character sums.

Keywords Superorthogonality · Square functions · Walsh–Paley series · Discrete operators · Multicorrelation sums · Trace functions · Character sums

Mathematics Subject Classification 42B20 · 42A16 · 42B25 · 11L40

1 Introduction

Let $\{f_n\}_n$ be a sequence of functions associated to a function f . Our goal is to understand two types of inequalities:

The direct inequality:

$$\left\| \sum_n f_n \right\|_{L^p} \leq c_p \left\| \left(\sum_n |f_n|^2 \right)^{1/2} \right\|_{L^p}.$$

Dedicated to the memory of Elias M. Stein.

With an “Appendix” by Emmanuel Kowalski.

✉ Lillian B. Pierce
pierce@math.duke.edu

¹ Department of Mathematics, Duke University, 120 Science Drive, Durham, NC 27708, USA

The converse inequality:

$$\left\| \left(\sum_n |f_n|^2 \right)^{1/2} \right\|_{L^p} \leq c_p' \|f\|_{L^p}.$$

Given an operator with a suitable decomposition

$$T = \sum_n T_n,$$

upon setting $f_n = T_n(f)$, if both estimates were true, they would imply that

$$\|Tf\|_{L^p} \leq c_p' c_p \|f\|_{L^p}.$$

Superorthogonality can be used to prove one or both of these inequalities. Superorthogonality is the property that for any tuple of functions $f_{n_1}, \dots, f_{n_{2r}}$ from the given sequence $\{f_n\}_n$,

$$\int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} = 0 \quad (1.1)$$

as long as an appropriate condition is satisfied by the tuple of indices (n_1, \dots, n_{2r}) . In this note, we show that a wide variety of topics in harmonic analysis and number theory can be united within the framework of superorthogonality, and associated direct and converse inequalities. We exhibit three main types of superorthogonality.

Type I

Type I superorthogonality is the case in which (1.1) holds if the tuple (n_1, \dots, n_{2r}) has the property that some value n_j appears an odd number of times. We show that any collection of functions with Type I superorthogonality satisfies a direct inequality.

Type I superorthogonality classically appeared in Khintchine's inequality for the Rademacher functions, which can be viewed as both a direct and a converse inequality. Furthermore we show that a refinement of Type I superorthogonality underpins a recent result of [30], a philosophical converse to the proof of the Vinogradov Mean Value Theorem via decoupling [6]. This notion of superorthogonality shows that counts for the number of diagonal solutions and near-solutions to a system of Diophantine equations can imply a direct inequality for a square function; this in turn implies a decoupling inequality for the extension operator associated to the corresponding curve.

Type II

Type II superorthogonality is the case in which (1.1) holds if the tuple (n_1, \dots, n_{2r}) has the property that some value n_j appears precisely once. We show that any collection of functions with Type II superorthogonality satisfies both a direct inequality and a multilinear direct inequality.

Any sequence $\{f_n\}_n$ in which $f_1, f_2, \dots, f_n, \dots$ are mutually independent random variables, and each has mean zero (in the sense that $\int f_n dx = 0$), satisfies the Type II condition. Supposing for simplicity the functions are real-valued, the mutual independence guarantees that

$$\int f_{n_1} f_{n_2} \cdots f_{n_{2r}} dx = \prod_{\ell} \left(\int f_{n_{\ell}}^{m_{\ell}} dx \right),$$

where m_{ℓ} is the multiplicity with which $f_{n_{\ell}}$ occurs in the product $f_{n_1} f_{n_2} \cdots f_{n_{2r}}$. Hence the defining property of Type II superorthogonality holds, since this integral vanishes as soon as at least one function has multiplicity one.

We show that Type II superorthogonality also holds in a completely different setting, namely for a sequence of discrete functions $\{f_{a/q}\}_{a/q}$ acting on \mathbb{Z} , indexed by a collection of rational numbers. Each function is defined according to

$$(f_{a/q})\widehat{\ }(\xi) = m(\varepsilon^{-1}(\xi - a/q))\widehat{f}(\xi),$$

where m is a periodization of an $L^p(\mathbb{R})$ multiplier supported in $(-1/2, 1/2]$, and ε is appropriately small. In this case, verifying Type II superorthogonality requires quite different methods—arithmetic rather than probabilistic, relating to the prime factorizations of the denominators in the rationals a/q . Using Type II superorthogonality, we prove a direct inequality and a multilinear direct inequality related to the collection $\{f_{a/q}\}_{a/q}$. Furthermore, we prove two types of converse inequalities in this setting. Taken altogether, these inequalities prove the ℓ^p boundedness of a discrete operator that is a building block in the celebrated work of Ionescu and Wainger [38] on discrete singular Radon transforms; see Theorem 5.1. Our presentation here serves as a friendly introduction to the influential method of Ionescu and Wainger.

Type III

Type III superorthogonality is the case in which (1.1) holds if the tuple (n_1, \dots, n_{2r}) has the property that some value n_j appears precisely once and is strictly greater than all other values in the tuple.

This type of superorthogonality occurred a few years after Khintchine's inequality, in Paley's work on the Walsh–Paley series [49], where he was able to use Type III superorthogonality to prove both a direct inequality and a converse inequality. Here we develop Paley's ideas in general terms, to show that any collection of functions with Type III superorthogonality, and two additional properties, satisfies both a direct and a converse inequality.

Quasi-superorthogonality

Fourth, we introduce the notion of quasi-superorthogonality: we no longer assume that (1.1) vanishes, but instead that it exhibits quantitative cancellation. Now instead of a direct inequality, we obtain a variant that also includes an “off-diagonal” term on the right-hand side. Such inequalities are nevertheless very useful.

In fact, we observe that a deep application of ℓ -adic cohomology and the Riemann Hypothesis over finite fields proves that Type I quasi-superorthogonality holds for sequences of “trace functions”; this is the statement of multicorrelation of trace functions proved in [25]. Hence an approximate direct inequality holds for such functions. Moreover, the source of quasi-superorthogonality of trace functions is a consequence of “exact” superorthogonality in the sense of (1.1) for a different set of functions, combined with the Riemann Hypothesis over finite fields. An appendix by Emmanuel Kowalski makes this phenomenon explicit.

As an application, we give a complete proof of the Burgess bound for character sums [11] from the perspective of quasi-superorthogonality and an approximate direct inequality for square functions; see Theorem 8.1. This is a celebrated result in number theory that has long held the record for certain problems related to the Generalized Riemann Hypothesis. As remarked in [29], “While the original argument [of Burgess] is easily followed line-by-line, it seems hard to comprehend the larger sense of it, because several technical difficulties are being dealt with at the same time that the main idea is unfolding.” Here we give an intuitive motivation for the method by combining quasi-superorthogonality with simplifying ideas from [29,35]. This also highlights certain barriers to improving Burgess’s result.

In Memoriam

It was an honor and delight to learn from Elias M. Stein for twenty years. This paper is in many ways a joint product with Eli. It germinated from a brief note Eli wrote to me in the summer of 2018, while we were collaborating on a book manuscript. At the time, we were interested in the relationship of superorthogonality to square function estimates. We noticed variants of the basic notion in several settings, and began to divide superorthogonality into types. While the ideas of that hand-written note have now grown and changed, the heart of the matter was already on those foolscap pages. In homage, I follow Eli’s words closely in phrases in the introduction and in Sect. 4 (particularly Sect. 4.5). The material of Sect. 5 develops a special case of a key theorem in the book manuscript we were preparing, and represents our shared work. The later sections move on to connections with number theory, which we also enjoyed discussing that summer. I have taken the liberty of developing ideas from our conversations, notes, and drafts, in loving debt to Eli; I am of course solely responsible for any inaccuracies in the current presentation.

Outline

In Sect. 2 we introduce Type I superorthogonality and formally prove a direct inequality; from this we deduce Khintchine’s inequality for Rademacher functions and a variant of the Marcinkiewicz–Zygmund theorem, which we apply later. In Sect. 3 we introduce Type II superorthogonality and formally prove a direct inequality. In Sect. 4 we introduce Type III superorthogonality and use it to prove both a direct and a converse inequality; these apply for example to Walsh–Paley series. We then mention a variant Type III’ that applies to Fourier multiplier operators.

Having introduced the three main types, in Sect. 5 we then turn to the core technical work of applying Type II to prove a theorem about discrete operators. In Sect. 6 we refine Type I to Type I* and exhibit its relationship to decoupling and counting solutions to Diophantine equations.

We then turn to the notion of quasi-superorthogonality and its applications in number theory. In Sect. 7 we document why trace functions satisfy Type I quasi-superorthogonality, and deduce an approximate direct inequality. We then introduce the notion of incomplete sums of trace functions and the Pólya–Vinogradov method, leading to the difficult question of bounding short sums. In Sect. 8 we develop a schematic approach to bounding short sums via quasi-superorthogonality. We then carry this out precisely, first obtaining a weaker bound with a more intuitive proof, and then refining it to recover the classical Burgess bound.

Appendix A concerns further details related to the setting of Walsh–Paley series.

Appendix B by Emmanuel Kowalski provides an explicit description of how an instance of exact superorthogonality leads to quasi-superorthogonality for trace functions.

As this note covers territory within both analysis and number theory, it is written to be broadly accessible. In addition to the main “types” of superorthogonality we focus on here, we periodically make further remarks about other settings and other types and their variants, but given the universality of the phenomena, we do not intend this survey to be exhaustive. We anticipate that many further instances of superorthogonality will be recognized by readers.

Conventions

Strictly speaking, when one specifies that a collection of functions $\{f_n\}_n$ satisfies a superorthogonality condition (1.1), one should specify for which r this holds, the set of indices n , and the measure space in which integration takes place. In the settings we consider, the superorthogonality property holds for all integers $r \geq 1$. In formal arguments to deduce a direct or converse inequality using superorthogonality, we assume the sum $\sum_n f_n$ is taken over a finite set of indices, and then the desired inequality is proved with a constant that is uniform with respect to the cardinality of this set. In applications in which the set of indices is infinite, this suffices if appropriate limiting arguments apply. In formal arguments we suppress notation for the measure space $L^p(\mathcal{M}, d\mu)$ until we state a specific setting, at which point we then work precisely with spaces such as $L^p(\mathbb{R})$ and $L^p[0, 1]$ with Lebesgue measure, or $\ell^p(\mathbb{Z})$ and

$\ell^p(\mathbb{Z}/q\mathbb{Z})$ with counting measure. In the settings we consider, the functions f_n in the collection $\{f_n\}_n$ are assumed to be distinct.

Observe that Type I \Rightarrow Type II \Rightarrow Type III, in the sense that any sequence of functions $\{f_n\}_n$ that is of Type I must be of Type II, and so forth. While the condition that defines Type I and Type II superorthogonality is invariant under a change of ordering of the functions $f_1, f_2, \dots, f_n, \dots$, the condition that defines Type III is not. In what follows, we assume that the set $\{f_n\} = \{f_1, f_2, \dots, f_n, \dots\}$ has been given with an ordering.

Constants such as C_p, c_p, A_p and so on, may indicate certain dependencies, but may change in value from one occurrence to the next. The notation $f \ll_p g$ is also used, and indicates that there is an implicit constant C_p such that $|f| \leq C_p g$.

2 Type I Superorthogonality and the Rademacher Functions

We introduce a first notion of superorthogonality, working with real-valued functions for simplicity. It is the condition that for every $2r$ -tuple $f_{n_1}, \dots, f_{n_{2r}}$ of functions from a sequence $\{f_n\}_n$,

$$\int f_{n_1} f_{n_2} \cdots f_{n_{2r}} = 0 \quad (2.1)$$

as long as

Type I: the tuple $(n_1, n_2, \dots, n_{2r})$ has the property that there is a value n_j that appears an odd number of times.

Here we show formally that any sequence of functions satisfying the Type I condition obeys a direct inequality; then we observe that this holds for Rademacher functions, and derive Khintchine's inequality and a variant of the Marcinkiewicz–Zygmund theorem. Later we will return to applications of the Type I property in the settings of decoupling and trace functions.

It is an elementary observation that a collection $\{f_n\}$ with Type I superorthogonality satisfies an identity in L^2 :

$$\left\| \sum_n f_n \right\|_{L^2}^2 = \left\| \left(\sum_n f_n^2 \right)^{1/2} \right\|_{L^2}^2. \quad (2.2)$$

This follows from expanding the left-hand side and observing that the off-diagonal cross terms vanish, by the superorthogonality assumption.

More generally, if a set of functions $\{f_n\}$ satisfies the Type I condition, we may immediately verify the direct inequality in L^{2r} for each integer $r \geq 1$. We expand the L^{2r} norm using a multinomial expansion,

$$\left\| \sum_n f_n \right\|_{L^{2r}}^{2r} = \int \left| \sum_n f_n \right|^{2r} = \sum_{(a_1, \dots, a_s)} C(a_1, \dots, a_s) \int f_{n_1}^{a_1} \cdots f_{n_s}^{a_s},$$

where the sum ranges over all $s \leq 2r$, all pairwise distinct n_1, \dots, n_s in the (finite) index set, and all (a_1, \dots, a_s) with $a_1 + \dots + a_s = 2r$; here $C(a_1, \dots, a_s) = (a_1 + \dots + a_s)!/(a_1! \cdots a_s!)$. By the Type I property, the integral vanishes except for those (a_1, \dots, a_s) with each a_i even, say $a_i = 2b_i$. Moreover, non-vanishing terms on the right-hand side must have $s \leq r$.

On the other hand, observe that

$$\sum_{(b_1, \dots, b_s)} C(b_1, \dots, b_s) \int f_{n_1}^{2b_1} \cdots f_{n_s}^{2b_s} = \int \left(\sum_n f_n^2 \right)^r = \left\| \left(\sum_n f_n^2 \right)^{1/2} \right\|_{L^{2r}}^{2r} \quad (2.3)$$

where the left-most sum ranges over all $s \leq r$, all pairwise distinct n_1, \dots, n_s in the index set, and all (b_1, \dots, b_s) with $b_1 + \dots + b_s = r$. We may conclude that

$$\left\| \sum_n f_n \right\|_{L^{2r}}^{2r} \leq C_r \left\| \left(\sum_n f_n^2 \right)^{1/2} \right\|_{L^{2r}}^{2r},$$

where we define

$$C_r = \max_{(b_1, \dots, b_s)} \frac{C(2b_1, \dots, 2b_s)}{C(b_1, \dots, b_s)},$$

and the maximum is taken over all (b_1, \dots, b_s) with $b_1 + \dots + b_s = r$ and $s \leq r$. One can observe for example that $C_r \leq \frac{(2r)!}{r! 2^r} < r^r$, but all we require is that it depends only on r . In conclusion, we have verified the direct inequality for the set of functions $\{f_n\}$, for each $p = 2r$.

This argument has been written in the spirit of Paley and Zygmund [50, Lemma 2], where it was developed to prove the Khintchine inequality for Rademacher functions. As we will require this result later on, and it is a nice illustration of Type I superorthogonality, we now also demonstrate its proof.

2.1 The Rademacher Functions

We recall the definition of the Rademacher functions [57, §VI, p. 130]: for $n = 0$,

$$r_0(t) = 1 \quad \text{for } 0 \leq t < 1/2, \quad r_0(t) = -1 \quad \text{for } 1/2 \leq t < 1, \quad r_0(t+1) = r_0(t).$$

Then we set $r_n(t) = r_0(2^n t)$ for each $n = 1, 2, 3, \dots$. These satisfy the property that for distinct n_1, n_2, \dots, n_s ,

$$\int_0^1 r_{n_1}^{a_1}(t) r_{n_2}^{a_2}(t) \cdots r_{n_s}^{a_s}(t) dt = 0 \quad (2.4)$$

unless all the integers a_1, \dots, a_s are even, in which case the integral evaluates to 1. In particular, $\{r_n\}$ satisfies Type I superorthogonality on $L^{2r}[0, 1]$ for every integer $r \geq 1$.

We may verify this as follows. Since for any n , $r_n(t)^2 \equiv 1$, it suffices to prove that (2.4) vanishes in the case in which $n_1 > n_2 > \dots > n_s$ and all $a_i = 1$. Observe that the function $r_{n_2}(t) \cdots r_{n_s}(t)$ is a step function that is constant on 2^{n_2+1} intervals of length $2^{-(n_2+1)}$. Thus it suffices to show that on each of these intervals, say I , $\int_I r_{n_1}(t) dt = 0$. In turn, each such interval I can be dissected into $2^{n_1-n_2}$ intervals of equal length, and on half these intervals $r_{n_1}(t)$ takes the value +1 while on the other intervals $r_{n_1}(t)$ takes the value -1. Consequently the integral of $r_{n_1}(t)$ over I is zero, and from this we deduce (2.4). This proof is in the spirit of Kaczmarz and Steinhaus, e.g. [42, p. 236], [43, p. 125]; other classic sources are e.g. [40, 71].

We mention that Rademacher proved that if $\sum_{n=0}^{\infty} |a_n|^2 < \infty$ then the series $\sum_{n=0}^{\infty} a_n r_n(t)$ converges pointwise for almost all $t \in [0, 1]$ [57, pp. 135–138]; see also [71, vol. 1, Chap. V, Thm. 82] for a modern citation.

2.2 Khintchine's Inequality

We can apply the formal ideas developed above to deduce a useful inequality. This is Khintchine's inequality: for each $0 < p < \infty$, for any sequence $\{a_n\}$ of complex numbers,

$$\left(\sum_{n=0}^{\infty} |a_n|^2 \right)^{1/2} \ll_p \left\| \sum_{n=0}^{\infty} a_n r_n(t) \right\|_{L^p[0,1]} \ll_p \left(\sum_{n=0}^{\infty} |a_n|^2 \right)^{1/2}. \quad (2.5)$$

We will call the right-most inequality the direct inequality, and the left-most inequality the converse inequality. Standard modern proofs can be found in e.g. [61, Appendix D], [70, Prop. 4.5] (see [32] for precise constants). We will consider the case $p > 1$, and our interest is that for $p = 2r$ with $r \geq 1$ integral, we can prove this as an application of Type I superorthogonality; this treatment is in the spirit of older proofs, e.g. [50, Lemma 2], [71, vol. I, Chap. V, Thm. 8.4].

First, there are various reductions. One can treat the real and imaginary parts separately, so that we only consider the case in which each a_n is real. Due to the pointwise a.e. convergence mentioned above, it suffices to prove the inequalities for a truncated sum over $0 \leq n \leq N$, uniformly in N . First note that by (2.2), there is an identity on $L^2[0, 1]$:

$$\left(\int_0^1 \left| \sum_{n=0}^N a_n r_n(t) \right|^2 dt \right)^{1/2} = \left(\sum_{n_1, n_2} a_{n_1} a_{n_2} \int_0^1 r_{n_1}(t) r_{n_2}(t) dt \right)^{1/2} = \left(\sum_{n=0}^N |a_n|^2 \right)^{1/2}.$$

For the direct inequality, the main content of (2.5) thus lies in the case $p > 2$, since for $p < 2$, Hölder's inequality shows that $\left\| \sum a_n r_n \right\|_{L^p[0,1]} \leq \left\| \sum a_n r_n \right\|_{L^2[0,1]} = \left(\sum |a_n|^2 \right)^{1/2}$; analogously, for the converse inequality the main content lies in the

case $p < 2$. Moreover, for $p < 2$ the converse inequality can be deduced from the direct inequality: let $r > 2$ be such that $1/2 = (1/2)(1/p + 1/r)$, so that by Hölder's inequality

$$\left(\sum_{n=0}^N |a_n|^2 \right)^{1/2} = \left\| \sum a_n r_n \right\|_{L^2} \leq \left\| \sum a_n r_n \right\|_{L^p}^{1/2} \left\| \sum a_n r_n \right\|_{L^r}^{1/2}.$$

Then upon applying the direct inequality for L^r , we conclude that the converse inequality holds for L^p . Thus it only remains to verify the direct inequality for $p > 2$. Moreover, it suffices to consider the case $p = 2r$ with $r \geq 1$ an integer, since given any $p > 2$ if we let r denote that integer such that $2(r-1) \leq p < 2r$, then for any function f on the space $[0, 1]$, $\|f\|_{L^{2r-2}[0,1]} \leq \|f\|_{L^p[0,1]} \leq \|f\|_{L^{2r}[0,1]}$.

Now let $p = 2r$ with $r \geq 1$ an integer. We may apply our formal argument for Type I functions with $f_n = a_n r_n$. Moreover, using the fact that the integral in (2.4) evaluates to 1 when it is nonvanishing, we see in (2.3) that

$$\begin{aligned} & \sum_{(b_1, \dots, b_s)} C(b_1, \dots, b_s) \int f_{n_1}^{2b_1} \cdots f_{n_s}^{2b_s} \\ &= \sum_{(b_1, \dots, b_s)} C(b_1, \dots, b_s) a_{n_1}^{2b_1} \cdots a_{n_s}^{2b_s} = \left(\sum_n a_n^2 \right)^r. \end{aligned}$$

Thus the argument concludes as desired, and

$$\left\| \sum_n f_n \right\|_{L^{2r}} \leq C_r^{1/2r} \left(\sum_n a_n^2 \right)^{1/2}.$$

2.3 A Theorem of Marcinkiewicz–Zygmund

We state a nice consequence of Khintchine's inequality, which we will apply in our study of discrete operators in Sect. 5. We work here with a measure space $(X, d\mu)$; in Sect. 5 we apply it to $\ell^p(\mathbb{Z})$ with counting measure, with appropriate associated Fourier transform mapping to functions on $(-1/2, 1/2]$ (identified with the torus).

Theorem 2.1 (Marcinkiewicz–Zygmund) *Let $1 \leq p < \infty$ be fixed and suppose that T is a bounded linear operator from $L^p(X)$ to $L^p(X)$, with norm M_p , that is, for all $f \in L^p(X)$,*

$$\|Tf\|_{L^p(X)} \leq M_p \|f\|_{L^p(X)}.$$

(I) Then there exists a constant C_p such that for any sequence $\{f_j\}$ of functions with $f_j \in L^p(X)$,

$$\left\| \left(\sum_{j=1}^{\infty} |Tf_j|^2 \right)^{1/2} \right\|_{L^p(X)} \leq M_p C_p \left\| \left(\sum_{j=1}^{\infty} |f_j|^2 \right)^{1/2} \right\|_{L^p(X)}.$$

(II) Suppose moreover that T is a translation-invariant operator with corresponding Fourier multiplier $m(\xi)$, and that $\{\xi_j\}_j$ is a fixed set of points. Define for each j the associated operator T_j acting by $(T_j f) \widehat{}(\xi) = m(\xi - \xi_j) \widehat{f}(\xi)$. Then

$$\left\| \left(\sum_{j=1}^{\infty} |T_j f_j|^2 \right)^{1/2} \right\|_{L^p(X)} \leq M_p C_p \left\| \left(\sum_{j=1}^{\infty} |f_j|^2 \right)^{1/2} \right\|_{L^p(X)}.$$

Proof To prove part (I), it suffices to consider the case of a finite sequence of functions f_1, \dots, f_N , from which the general statement follows by the monotone convergence theorem. Recall the Rademacher functions $\{r_j\}_j$. Given f_1, \dots, f_N , we define for $t \in [0, 1]$ the function

$$F(x, t) = \sum_{1 \leq j \leq N} r_j(t) f_j(x).$$

Since T is linear, $T F(x, t) = \sum_j r_j(t) T f_j(x)$, so that by the assumed boundedness of T ,

$$\int_X \left| \sum_j r_j(t) T f_j(x) \right|^p d\mu(x) \leq M_p \int_X \left| \sum_j r_j(t) f_j(x) \right|^p d\mu(x)$$

for each t . By integrating in t and applying Fubini's theorem,

$$\int_X \int_0^1 \left| \sum_j r_j(t) T f_j(x) \right|^p dt d\mu(x) \leq M_p \int_X \int_0^1 \left| \sum_j r_j(t) f_j(x) \right|^p dt d\mu(x).$$

Applying Khintchine's inequality for each fixed x then shows that the left and right-hand sides are comparable to

$$\int_X \left(\sum_j |T f_j|^2 \right)^{p/2} dx \quad \text{and} \quad \int_X \left(\sum_j |f_j|^2 \right)^{p/2} dx,$$

respectively.

To prove part (II), observe that $(T_j f)(x) = e^{2\pi i x \xi_j} (T(f(\cdot)) e^{-2\pi i (\cdot) \xi_j})(x)$. As a result, for any sequence $\{f_j\}$,

$$\sum_j |T_j(f_j)|^2 = \sum_j |T(f_j e^{-2\pi i x \xi_j})|^2.$$

Thus the conclusion of (II) follows from applying the conclusion of (I) to the right-hand side. \square

3 Type II Superorthogonality

We introduce a second notion of superorthogonality, now for complex-valued functions. It is the condition that for every $2r$ -tuple of functions from a sequence $\{f_n\}$,

$$\int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} = 0$$

as long as:

Type II: the tuple $(n_1, n_2, \dots, n_{2r})$ has the property that there is a value n_j that appears precisely once, in which case we say that the tuple has *the uniqueness property*.

In this section, we prove that any collection of functions satisfying the Type II condition satisfies a direct inequality. In Sect. 5 we will return to this type in more detail, when we study its application to discrete operators; we will also apply this type in the setting of trace functions, when we prove the Burgess bound.

3.1 The Direct Inequality

In general, a collection $\{f_n\}$ with Type II superorthogonality satisfies a direct inequality in L^{2r} for all integers $r \geq 1$. We expand

$$\left\| \sum_n f_n \right\|_{L^{2r}}^{2r} = \sum_{(n_1, \dots, n_{2r})} \int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}}$$

in which the sum is over all tuples (n_1, \dots, n_{2r}) in the index set. Under the Type II assumption, the contribution vanishes for any such tuple with the uniqueness property; hence we need only consider tuples in which every index appears at least twice, so in particular the indices take at most r distinct values. Thus we can write the above expression as

$$\sum_A \sum_{\substack{(n_1, \dots, n_{2r}) \\ \{n_1, \dots, n_{2r}\} = A}} \int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}},$$

in which the first sum is over all subsets A of indices, with $|A| \leq r$. Here we distinguish between a tuple (n_1, \dots, n_{2r}) and the set of (distinct) values $\{n_1, \dots, n_{2r}\}$ appearing in the tuple. Note that once such a set A is fixed, there are at most d_r possible $2r$ -tuples with values corresponding to the set A , for a combinatorial constant d_r .

The right-hand side of the direct inequality can be expanded as

$$\left\| \left(\sum_n |f_n|^2 \right)^{1/2} \right\|_{L^{2r}}^{2r} = \sum_A \sum_{\substack{(n_1, \dots, n_r) \\ \{n_1, \dots, n_r\} = A}} \int |f_{n_1}|^2 \cdots |f_{n_r}|^2,$$

where the sum is over all sets A with cardinality at most r . To verify the direct inequality, it suffices to show that for each set A with $|A| \leq r$, for every tuple (n_1, \dots, n_{2r}) without the uniqueness property such that $\{n_1, \dots, n_{2r}\} = A$,

$$\int |f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}}| \leq \sum_{\{n_1, \dots, n_r\} = A} \int |f_{n_1}|^2 \cdots |f_{n_r}|^2. \quad (3.1)$$

Then upon summing over all such tuples and all such sets A , the direct inequality will hold, with $c_{2r}^{2r} = d_r$.

In order to verify (3.1), we claim the following. Fix any set A with $|A| \leq r$. We may partition each $2r$ -tuple (n_1, \dots, n_{2r}) without the uniqueness property whose set of distinct values is A , into two r -tuples, say $(n_{i_1,0}, \dots, n_{i_r,0})$ and $(n_{i_1,1}, \dots, n_{i_r,1})$, such that

$$\{n_{i_1,0}, \dots, n_{i_r,0}\} = A = \{n_{i_1,1}, \dots, n_{i_r,1}\}.$$

Equivalently, we claim that we can color the entries in the $2r$ -tuple so that r of the entries are red and r of the entries are blue, and moreover each entry of A appears in red at least once and in blue at least once.

Let us prove this. Suppose the set A has entries a_1, \dots, a_s for some $s \leq r$. For each value a_i that appears an even number of times in the $2r$ -tuple, say $2k_i$ times, we color k_i of these red and k_i of these blue. Next we consider the set of all entries $a_i \in A$ that each appear an odd number of times in the $2r$ -tuple, say $2k_i + 1$ times, with $k_i \geq 1$. (Each a_i must appear at least 3 times, since the $2r$ -tuple does not have the uniqueness property.) Since $2r$ is even, there must be an even number of such entries a_i in A . For half of them, we color $k_i + 1$ red and k_i blue, and for the other half we color k_i red and $k_i + 1$ blue, and this proves the claim.

Now we apply the partition to verify (3.1). Fix a $2r$ -tuple (n_1, \dots, n_{2r}) with $\{n_1, \dots, n_{2r}\} = A$ and construct the r -tuples $(n_{i_1,0}, \dots, n_{i_r,0})$ and $(n_{i_1,1}, \dots, n_{i_r,1})$ as above. Then, also using the fact that for any $\alpha, \beta \geq 0$ we have $2\alpha\beta \leq \alpha^2 + \beta^2$,

$$\begin{aligned} \int |f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}}| &= \int |f_{n_{i_1,0}}| \cdots |f_{n_{i_r,0}}| \cdot |f_{n_{i_1,1}}| \cdots |f_{n_{i_r,1}}| \\ &\leq \frac{1}{2} \int |f_{n_{i_1,0}}|^2 \cdots |f_{n_{i_r,0}}|^2 + \frac{1}{2} \int |f_{n_{i_1,1}}|^2 \cdots |f_{n_{i_r,1}}|^2 \end{aligned}$$

$$\leq \sum_{\{n_1, \dots, n_r\}=A} \int |f_{n_1}|^2 \cdots |f_{n_r}|^2.$$

This proves (3.1) and hence verifies the direct inequality, for $p = 2r$ an even integer. In general, the converse inequality needs a different argument, and we will return to this in the specific setting of Sect. 5.

4 Type III Superorthogonality in the Work of Paley

We now introduce a third notion of superorthogonality, again working with real-valued functions for simplicity: it is the condition that for every $2r$ -tuple of functions from a sequence $\{f_n\}$ indexed by integers n ,

$$\int f_{n_1} f_{n_2} \cdots f_{n_{2r}} = 0$$

as long as:

Type III: the tuple $(n_1, n_2, \dots, n_{2r})$ has the property that there is an $n_j > n_\ell$ for all $\ell \neq j$.

Type III superorthogonality was exploited by Paley in his study of the Walsh–Paley series [49]. Recalling the Rademacher functions $\{r_n\}$, we define a set of functions $\{w_n\}$ as follows. Set $w_0(t) = 1$. For $n = 2^{n_1} + 2^{n_2} + \cdots + 2^{n_s}$ (with $n_1 > \cdots > n_s$) set

$$w_n(t) = r_{n_1}(t) r_{n_2}(t) \cdots r_{n_s}(t). \quad (4.1)$$

The orthogonality property (2.4) of the Rademacher functions immediately implies that

$$\int_0^1 w_m(t) w_n(t) dt = \begin{cases} 1 & \text{if } n = m, \\ 0 & \text{if } n \neq m. \end{cases}$$

Walsh [66], Kaczmarz [41] and Paley [49] studied the functions $\{w_n\}$ extensively, and Fine [23, §2] recognized them as the characters of the Walsh group or “dyadic group.”

Fundamentally, the collection $\{w_n\}$ is a complete orthonormal system of functions on $[0, 1]$; see e.g. [49, p. 243]. For each $n \geq 1$, define for any real-valued function f on $[0, 1]$ the partial sum

$$S_n f(t) = \sum_{m=0}^{n-1} c_m(f) w_m(t), \quad \text{with } c_m(f) = \int_0^1 f(\theta) w_m(\theta) d\theta.$$

Following Stein, we call this a Walsh–Paley series. Paley developed numerous properties of the partial sums $S_n f$, proving for example via the Hardy–Littlewood maximal function (new at that time), that for integrable f , the dyadic partial sums converge

pointwise as $n \rightarrow \infty$,

$$S_{2^n} f(t) \rightarrow f(t) \quad (4.2)$$

for almost every $t \in [0, 1]$ [49, Thm. IV]. See also the earlier proof of Kaczmarz [41]. (The pointwise a.e. convergence of the non-dyadic sums $S_n f(t) \rightarrow f(t)$ for $f \in L^p[0, 1]$ with $p > 1$ was much more difficult, and was resolved after Carleson's work; see [3, 59, 63], and see [60, Thm. 7] for a counterexample on $L^1[0, 1]$.)

To illustrate Type III superorthogonality, we will focus on the dyadic differences f_n defined by

$$f_n = S_{2^n} f - S_{2^{n-1}} f. \quad (4.3)$$

Paley [49, Thm. V] proved a direct inequality and a converse inequality for the sequence $\{f_n\}$: for any $1 < p < \infty$, for any (real-valued) $f \in L^p[0, 1]$,

$$\left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p[0,1]} \ll_p \|f\|_{L^p[0,1]} \ll_p \left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p[0,1]}. \quad (4.4)$$

From these direct and converse inequalities, Paley deduced for any fixed n the bound

$$\|S_n f\|_{L^p[0,1]} \leq B_p \|f\|_{L^p[0,1]} \quad (4.5)$$

for any $1 < p < \infty$ [49, Thm. VI]. Here the deduction of the operator bound from the direct and converse inequalities is not as simple as in the formal setting of the introduction, since the direct and converse inequalities are for dyadic differences, while (4.5) is for a non-dyadic partial sum. We provide Paley's clever proof in Appendix A.

In this section, we demonstrate Paley's method to prove the direct and converse inequalities in (4.4) in the case of $p = 2r$ an even integer. In particular, we expose a curious feature of Paley's method, which is that he applies Type III superorthogonality not just for the direct inequality, but also to prove the converse inequality. This introduces a nonconcentration inequality (Lemma 4.1) that will play a key role in the next section, on discrete operators.

We first work formally, abstracting Paley's ideas to a general sequence of functions $\{g_n\}$ satisfying certain properties, and at the end of the section we verify that the dyadic differences $\{f_n\}$ defined above for Walsh–Paley series satisfy all the requirements of our proof. We reserve certain details more specific to the setting of Walsh–Paley series (limiting arguments, and the reduction to $p = 2r$, which again applies Khintchine's inequality), to Appendix A.

4.1 Formal Setting

We now describe the formal setting in which we will work before specializing to the Walsh–Paley series. Let $\{\mu_m\}$ be a sequence of real-valued functions on $[0, 1]$ (with

small adaptations, a finite measure space will do), let $\{c_m\}$ be a fixed sequence of real numbers, and let $\{\alpha_m\}$ be a strictly-increasing sequence of non-negative integers. For each $n \geq 0$, let G_n denote the partial sum

$$G_n(t) = \sum_{0 \leq m < \alpha_n} c_m \mu_m(t).$$

Then define $g_n(t) = G_n(t) - G_{n-1}(t)$, with the convention that $g_0(t) = G_0(t)$ (or analogously $G_{-1}(t) = 0$).

We will prove that for every even integer $p = 2r$, uniformly in $N \geq 0$,

$$\left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p[0,1]} \ll_p \left\| \sum_{n=0}^N g_n \right\|_{L^p[0,1]} \ll_p \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p[0,1]}. \quad (4.6)$$

We refer to the right-most inequality as the direct inequality, and the left-most inequality as the converse inequality. We prove these inequalities under three assumptions. First, we assume that the functions $\{g_n\}$ satisfy the Type III superorthogonality condition, so that

$$\int_0^1 g_{n_1}(t) \cdots g_{n_{2r}}(t) dt = 0 \quad (4.7)$$

as long as $n_1 > \max\{n_2, \dots, n_{2r}\}$. Second, we assume that uniformly in N ,

$$\left\| \sup_{0 \leq n \leq N} |G_{n-1}| \right\|_{L^p[0,1]} \ll_p \|G_N\|_{L^p[0,1]}. \quad (4.8)$$

Third, we assume that uniformly in N ,

$$\left\| \left(\sum_{n=0}^N g_n^p \right)^{1/p} \right\|_{L^p[0,1]} \ll_p \|G_N\|_{L^p[0,1]}. \quad (4.9)$$

4.2 The Direct Inequality

We now prove the direct inequality for the functions $\{g_n\}$. Recall that when we proved the direct inequality for the Type I and the Type II case, we could work quite formally, using nothing but the superorthogonality condition. Here, we also require (4.8).

Fix $p = 2r$ with $r \geq 1$ an integer. One could try to expand $(\sum_{0 \leq n \leq N} g_n)^p = G_N^p$ directly, hoping to apply the Type III property wherever possible. But this is more subtle to apply than Type I or Type II superorthogonality, since one needs not just a uniqueness property amongst the indices but a magnitude comparison. Instead, Paley

introduces a telescoping sum

$$G_N^p = \sum_{n=0}^N (G_n^p - G_{n-1}^p) = \sum_{n=0}^N ((g_n + G_{n-1})^p - G_{n-1}^p).$$

For $n = 0$, the contribution is g_n^p , which will lead to an acceptable contribution in (4.11) below. For each index $n \geq 1$, we write

$$\int_0^1 (G_n^p - G_{n-1}^p) = \int_0^1 \left(g_n^p + pg_n^{p-1} G_{n-1} + \cdots + \binom{p}{2} g_n^2 G_{n-1}^{p-2} + pg_n G_{n-1}^{p-1} \right).$$

For each term $g_n^j G_{n-1}^{p-j}$ with $3 \leq j \leq p-1$ there exists some $\theta(j) \in (0, 1)$ such that

$$\left| \int_0^1 g_n^j G_{n-1}^{p-j} \right| \leq \left(\int_0^1 g_n^2 G_{n-1}^{p-2} \right)^{\theta(j)} \left(\int_0^1 g_n^p \right)^{1-\theta(j)} \leq \int_0^1 g_n^2 G_{n-1}^{p-2} + \int_0^1 g_n^p; \quad (4.10)$$

the first inequality is by Hölder's inequality, and the second is the simple fact that for any exponent $\theta \in (0, 1)$, and $A, B \geq 0$, $A^\theta B^{1-\theta} \leq \max\{A, B\} \leq A + B$. (Here we use that p is even so that all quantities are non-negative.) Of course the last inequality in (4.10) trivially holds for the cases $j = 2$ and $j = p$ as well.

The case $j = 1$ could not be argued in this way, but in fact the integral of $g_n G_{n-1}^{p-1}$ vanishes by the Type III condition (4.7): the index n of g_n is strictly greater than any index m that appears in the expansion $G_{n-1}^{p-1} = \left(\sum_{m=0}^{n-1} g_m \right)^{p-1}$ so that Type III superorthogonality applies. In total, we can conclude that for each $n \geq 0$,

$$\int_0^1 (G_n^p - G_{n-1}^p) \ll_p \int_0^1 g_n^2 G_{n-1}^{p-2} + \int_0^1 g_n^p, \quad (4.11)$$

so that upon summing over $0 \leq n \leq N$,

$$\int_0^1 G_N^p \ll_p \int_0^1 \left(\sum_{n=0}^N g_n^2 \right) \left(\max_{0 \leq n \leq N} |G_{n-1} f| \right)^{p-2} + \int_0^1 \sum_{n=0}^N g_n^p. \quad (4.12)$$

We can apply Hölder's inequality to the first term, and trivially apply $\sum_{n=0}^N g_n^p \leq \left(\sum_{n=0}^N g_n^2 \right)^{p/2}$ to the second (again using that p is even), to conclude that

$$\|G_N\|_{L^p}^p \ll_p \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^2 \left\| \max_{0 \leq n \leq N} |G_{n-1} f| \right\|_{L^p}^{p-2} + \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^p.$$

By the assumed maximal bound (4.8),

$$\|G_N\|_{L^p}^p \ll_p \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^2 \|G_N\|_{L^p}^{p-2} + \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^p. \quad (4.13)$$

This is an inequality of the form $A^p \leq B^2 A^{p-2} + B^p$ for non-negative A, B . If $A \leq B$, we have already proved the direct inequality, while if $A \geq B$ so that $B/A \leq 1$, we now deduce from (4.13) that $A^2 \leq B^2(1 + (B/A)^{p-2}) \ll B^2$. Thus we conclude that

$$\|G_N\|_{L^p} \ll_p \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p},$$

proving the direct inequality.

4.3 The Converse Inequality

A straightforward expansion of

$$\int_0^1 \left(\sum_{n=0}^N g_n^2 \right)^{p/2}$$

is uninformative for applying a superorthogonality condition; many tuples of indices in the expansion will not have a uniqueness property or magnitude comparison property. Instead, Paley employs the following useful fact, which we call a nonconcentration inequality, following the nomenclature of Gressman [31] in a related setting.

Lemma 4.1 *For any integer $r \geq 1$, for any non-negative real numbers a_n indexed by a finite set I ,*

$$\left(\sum_{n \in I} a_n \right)^r \leq (r(r-1))^{r-1} \sum_{n \in I} a_n^r + 2 \sum_{(n_1, \dots, n_r) \in I^r}^{\sharp} a_{n_1} \cdots a_{n_r} \quad (4.14)$$

in which \sum^{\sharp} indicates that the sum restricts to those ordered tuples $(n_1, \dots, n_r) \in I^r$ with all pairwise distinct entries.

This shows that the dominant values of the function $(n_1, \dots, n_r) \mapsto a_{n_1} \cdots a_{n_r}$ cannot concentrate on the zero-set of the function

$$\Phi(x_1, \dots, x_r) = \prod_{i \neq j} (x_i - x_j), \quad (4.15)$$

except at the origin $x_1 = \cdots = x_r = 0$. Of course one must allow for the values to concentrate on $n_1 = \cdots = n_r$, which could dominate if for example there exists $n \in I$

such that $a_n > a_{n'}$ for all $n' \neq n$. Nonconcentration inequalities are broadly useful in arguments involving superorthogonality, including our next section on discrete operators; they are also frequently used in decoupling (see e.g. the first display equation of [6, p. 653]). We provide a proof of the inequality at the end of the section.

Paley applies the nonconcentration inequality to conclude that for $p = 2r$,

$$\int_0^1 \left(\sum_{n=0}^N g_n^2 \right)^{p/2} dt \ll_p \int_0^1 \sum_{n=0}^N g_n^p dt + G^\sharp, \quad (4.16)$$

where

$$G^\sharp = \sum_{\substack{(n_1, \dots, n_r) \\ 0 \leq n_1, \dots, n_r \leq N}}^\sharp \int_0^1 g_{n_1}^2 \cdots g_{n_r}^2 dt,$$

and as usual the superscript \sharp indicates that the sum restricts to tuples with pairwise distinct entries. By the assumed bound (4.9), the first term may be bounded by $\ll_p \|G_N\|_{L^p}^p$. The main work is to show that

$$G^\sharp \ll_p \int_0^1 G_N^2 \left(\sum_{n=0}^N g_n^2 \right)^{\frac{p-2}{2}} dt. \quad (4.17)$$

Once we have proved this, we can apply these two bounds in (4.16), followed by Hölder's inequality, to conclude that

$$\left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^p \ll_p \|G_N\|_{L^p}^p + \|G_N\|_{L^p}^2 \left\| \left(\sum_{n=0}^N g_n^2 \right)^{1/2} \right\|_{L^p}^{p-2}.$$

This is again an inequality of the form $A^p \ll B^2 A^{p-2} + B^p$, so that an argument analogous to that applied to (4.13) confirms that the converse inequality holds.

We now demonstrate Paley's proof of (4.17) using Type III superorthogonality. If a tuple (n_1, \dots, n_r) appears in G^\sharp then n_1, \dots, n_r are all pairwise distinct and in particular there exists a strict ordering of the indices, which without loss of generality we can assume is $n_r < \dots < n_2 < n_1 \leq N$. In particular, we could be in a position to apply Type III superorthogonality, except for the fact that each function appearing in G^\sharp is squared. Paley cleverly circumvents this by considering the quantity

$$\int_0^1 G_N^2 g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt$$

for any $n_r \leq \dots \leq n_3 \leq n_2 \leq N$ (so far not assuming strict inequalities). Note that we can write $G_N = g_N + g_{N-1} + \dots + g_{n_2+1} + G_{n_2}$. Thus we can expand the integral

above as

$$\int_0^1 G_{n_2}^2 g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt + \sum_{n_1=n_2+1}^N \int_0^1 g_{n_1}^2 g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt \\ + 2 \sum_{n=n_2+1}^N \int_0^1 g_n G_{n_2} g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt + 2 \sum_{\substack{n \neq m \\ n_2 < n, m \leq N}} \int_0^1 g_n g_m g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt.$$

Now Type III superorthogonality shows that the last term vanishes. Furthermore the penultimate term also vanishes by the Type III property: we can write $G_{n_2} = \sum_{0 \leq m \leq n_2} (g_m - g_{m-1})$, so that expanding the penultimate integral, we can apply (4.7) to see that each summand in the expansion vanishes.

The non-negativity of the first term allows us to conclude that

$$\sum_{n_1=n_2+1}^N \int_0^1 g_{n_1}^2 g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt \leq \int_0^1 G_N^2 g_{n_2}^2 g_{n_3}^2 \cdots g_{n_r}^2 dt. \quad (4.18)$$

Now we consider the strictly ordered tuples that appear in G^\sharp ; in each of these there is a unique largest element in the tuple, which will play the role of n_1 above. In particular, summing (4.18) over all possible values of $n_r < \cdots < n_2 \leq N$, we see that

$$G^\sharp \ll_p \int_0^1 G_N^2 \left(\sum_{n_r < \cdots < n_2 \leq N} g_{n_2}^2 \cdots g_{n_r}^2 \right) dt \ll_p \int_0^1 G_N^2 \left(\sum_{n=0}^N g_n^2 \right)^{\frac{p-2}{2}} dt,$$

where the last inequality follows by non-negativity of the functions g_n^2 . This verifies (4.17), and the converse inequality in (4.6) follows.

4.4 Application to the Walsh–Paley Setting

We have proved in a formal setting that the direct and converse inequalities in (4.6) hold for a sequence $\{g_n\}$ of partial sum differences, under three assumptions. We now indicate why the Walsh–Paley setting satisfies the required assumptions.

Recall the definition of f_n from (4.3), defined according to a fixed real-valued function f . Thus f_n plays the role of g_n , the strictly increasing sequence is $\alpha_n = 2^n$, and S_{2^n} plays the role of G_n . (We use the convention that $f_0 = S_{2^0}$, or analogously $S_{2^{-1}} f = 0$.)

To see that the sequence $\{f_n\}$ satisfies the Type III condition, suppose that $m_1 > \max\{m_2, \dots, m_{2r}\}$; we claim that

$$\int_0^1 f_{m_1} f_{m_2} \cdots f_{m_{2r}} dt = 0. \quad (4.19)$$

Recall the expansion of the functions $\{w_m\}$ in terms of the Rademacher functions via (4.1). Observe that

$$f_{m_1}(t) = S_{2^{m_1}} f(t) - S_{2^{m_1-1}} f(t) = \sum_{2^{m_1-1} \leq m < 2^{m_1}} c_m(f) w_m(t),$$

so that f_{m_1} includes r_{m_1-1} as a factor in every summand of this expansion. On the other hand, after expanding each f_{m_j} with $j \geq 2$ in terms of the Rademacher functions, under the assumption that $m_j < m_1$, we see that r_{m_1-1} does not occur in any of the expansions, and hence does not occur in the expansion of $f_{m_2} \cdots f_{m_r}$. Thus the Type III condition (4.19) holds for $\{f_n\}$ by means of the Type I property (2.4) of the Rademacher functions. (Note that here we crucially used the fact that m_1 was a strict maximum; the Type I or Type II property need not hold for the sequence $\{f_n\}$.)

Remark 4.2 By the same proof method, the sequence $\{f_n\}$ satisfies a stronger condition, that $\int_0^1 (f_{m_1})^k f_{m_2} \cdots f_{m_s} dt = 0$ if k is an odd positive integer and $m_1 > \{m_2, \dots, m_s\}$. This type has a relation to both Type III (the case where $k = 1$) and to Type I. See [59, Lemma 1.4].

Remark 4.3 In the formal setting of § 4.1, if the functions $\{\mu_m\}$ were themselves of Type III, then the $\{g_n\}$ would inherit this property, for any strictly increasing choice of $\{\alpha_m\}$. But in the Walsh–Paley setting, while the functions $\{w_n\}$ are orthogonal, they do not themselves possess superorthogonality properties for $2r$ -tuples with $r \geq 2$; see Appendix A. The proof that the differences $\{f_n\}$ of dyadic sums are of Type III relies on the precise nature of the expansions of the functions w_n in terms of the Rademacher functions, and the lacunary choice $\alpha_m = 2^m$. (See [49] for further generalizations to other lacunary sequences.)

We next record that the maximal bound (4.8) holds in the Walsh–Paley setting, by [49, Thm. 1]. Indeed, Paley observes that $S_{2^n} f(t)$ is a (normalized) average of f over an interval of length 2^{-n} containing the point t , and deduces that $|S_{2^n} f(t)| \leq 2\mathcal{M}f(t)$ pointwise in t , uniformly in n , where $\mathcal{M}f$ is the (uncentered) Hardy–Littlewood maximal function of f . By the boundedness of the Hardy–Littlewood maximal function, for all $1 < p \leq \infty$, for all $f \in L^p$,

$$\left\| \sup_n |S_{2^n} f| \right\|_{L^p[0,1]} \ll_p \|f\|_{L^p[0,1]}. \quad (4.20)$$

If we apply this with the function f replaced by $S_{2^N} f$, and use the fact that for $n \leq N$, $S_{2^{N-1}}(S_{2^N} f) = S_{2^{N-1}} f$, we see that $\|\max_{0 \leq n \leq N} |S_{2^{N-1}} f|\|_{L^p[0,1]} \ll_p \|S_{2^N} f\|_{L^p[0,1]}$, verifying (4.8).

Finally, we verify (4.9). Paley observes in [49, Lemma 7] that for each $2 \leq p \leq \infty$, for all $f \in L^p$,

$$\left\| \left(\sum_{n=0}^{\infty} |f_n|^p \right)^{1/p} \right\|_{L^p[0,1]} \ll_p \|f\|_{L^p[0,1]}.$$

This holds for $L^2(\ell^2)$ (applying both (2.2) and the fact that $\{w_m\}$ is a complete orthonormal system) and for $L^\infty(\ell^\infty)$ (deduced from the normalized average observation above), and the general result follows by interpolation. Now for even p , we may truncate the sum on the left-hand side to $0 \leq n \leq N$ and still obtain the inequality, by positivity. If we apply this truncated inequality with $S_{2N}f$ in place of f , the right-hand side is $\|S_{2N}f\|_{L^p}$, while the summands on the left-hand side are still f_n , since for $n \leq N$, inside each difference defining f_n , $S_{2^n}(S_{2N}f) = S_{2^n}f$. This verifies (4.9).

The formal argument now applies, and we conclude that for each $p = 2r$ an even integer, there exists constants c_p, c'_p such that uniformly for all $N \geq 1$,

$$\left\| \left(\sum_{n=0}^N f_n^2 \right)^{1/2} \right\|_{L^p} \leq c'_p \left\| \sum_{n=0}^N f_n \right\|_{L^p} \leq c_p \left\| \left(\sum_{n=0}^N f_n^2 \right)^{1/2} \right\|_{L^p}. \quad (4.21)$$

In order to obtain the full inequality (4.4) for $p = 2r$ from this truncated version, one must apply a limiting argument; we remark on this in Appendix A. There we also mention a further use of the Rademacher functions to then deduce the full case $1 < p < \infty$ from the even integer case.

This concludes our discussion of the Walsh–Paley setting as an example of Type III superorthogonality; we now turn briefly to a natural variant.

4.5 Type III' Superorthogonality for Fourier Multipliers

A variant of Type III superorthogonality is the property that for a sequence of functions $\{f_n\}$ indexed by integers n , there exists an integer $c \geq 1$ such that

$$\int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} = 0 \quad (4.22)$$

as long as:

Type III': the tuple (n_1, \dots, n_{2r}) has the property that there is an $n_j \geq n_\ell + c$ for all $\ell \neq j$. Any sequence that satisfies Type III superorthogonality also satisfies Type III' superorthogonality (with $c = 1$). For a sequence with the Type III' property, an L^2 identity such as (2.2) is no longer a simple consequence. Also, the Type III' condition is not invariant if the functions are re-ordered.

Let us describe a case in which Type III' superorthogonality holds, involving multiplier operators T , such that $(Tf)\widehat{\gamma}(\xi) = m(\xi)\widehat{f}(\xi)$, with m satisfying the usual hypotheses of the Marcinkiewicz–Mikhlin–Hörmander theorem (e.g. [61, Chap. 4] or [62, Chap. VI, §4.4 and §7.6]). First we need a standard dyadic decomposition of the ξ -space:

$$1 = \sum_j \Psi_j(\xi),$$

where $\Psi_j(\xi) = \Psi(2^j \xi)$, and Ψ is smooth, compactly supported in $1/4 \leq |\xi| \leq 4$. Then by Plancherel's identity, Type III' superorthogonality holds ($c = 4$ will do) for

the sequence of functions $f_j = T_j f$, defined by

$$(T_j f) \widehat{}(\xi) = m(\xi) \Psi(2^j \xi) \widehat{f}(\xi).$$

The Type III condition fails. Nevertheless, in general for a sequence $\{f_j\}$ that satisfies Type III' superorthogonality with a constant c , then for each $1 \leq m \leq c$ we can define a sequence by taking $f_j^{(m)} = f_{cj+m}$ as j varies, and then for each m the sequence $f_1^{(m)}, f_2^{(m)}, \dots, f_n^{(m)}, \dots$ satisfies the Type III condition.

It would be interesting to prove that $\|Tf\|_{L^p} \leq c_p \|f\|_{L^p}$ via superorthogonality. Construct the c sequences $\{f_j^{(m)}\}_j$ as above. By suitably adapting Paley's arguments for the direct inequality (say for $p = 2r$ with $r \geq 1$ an integer), one could obtain that for each $1 \leq m \leq c$,

$$\left\| \sum_j f_j^{(m)} \right\|_{L^p} \leq c_p \left\| \left(\sum_j |f_j^{(m)}|^2 \right)^{1/2} \right\|_{L^p}.$$

Adding these inequalities would then provide the direct inequality in full, since

$$\begin{aligned} \left\| \sum_j f_j \right\|_{L^p} &\leq \sum_{1 \leq m \leq c} \left\| \sum_j f_j^{(m)} \right\|_{L^p} \\ &\leq c_p \sum_{1 \leq m \leq c} \left\| \left(\sum_j |f_j^{(m)}|^2 \right)^{1/2} \right\|_{L^p} \\ &\leq c \cdot c_p \left\| \left(\sum_j |f_j|^2 \right)^{1/2} \right\|_{L^p}. \end{aligned}$$

In fact, reasoning of this type appeared in a direct inequality proved by Córdoba in the study of Bochner–Riesz operators [18, p. 507].

Paley proved his converse inequality by again exploiting the Type III condition. Suitably adapting such arguments, one could obtain that for each fixed $1 \leq m \leq c$,

$$\left\| \left(\sum_j |f_j^{(m)}|^2 \right)^{1/2} \right\|_{L^p} \leq c_p \|F^{(m)}\|_{L^p},$$

in which $F^{(m)}$ is defined by

$$(F^{(m)}) \widehat{}(\xi) = \sum_j \Psi_{cj+m}(\xi) \widehat{f}(\xi).$$

Thus $F^{(1)} + F^{(2)} + \dots + F^{(c)} = f$. However one cannot add the converse inequalities above to get the desired converse inequality $\left\| \left(\sum_j |f_j|^2 \right)^{1/2} \right\|_{L^p} \leq c_p \|f\|_{L^p}$, so this approach fails.

If instead one hoped to adapt Paley's approach to accommodate Type III' superorthogonality within the proof, a critical point is that the nonconcentration inequality implies (4.16) so that (4.18) suffices. In the case of Type III' superorthogonality, such an approach seems to require a stronger nonconcentration inequality. There are many questions in this area, such as: in what circumstances is it true that the dominant off-diagonal terms in an expansion $(\sum_{n \in I} a_n)^r$ do not even occur close (within a c -neighborhood) to the zero set of the function (4.15); or what other nonconcentration inequalities arise when we replace (4.15) by some other function?

4.6 Proof of Lemma 4.1: Nonconcentration Inequality

The nonconcentration inequality of Lemma 4.1 has also appeared explicitly in other works such as [38, Lemma 2.3] or [48, Lemma 2.35], whose proofs we follow here. The claim is true if $r = 1$, and hence we suppose $r \geq 2$. Note that if

$$\left(\sum_{n \in I} a_n \right)^r \leq 2 \sum_{(n_1, \dots, n_r) \in I^r}^{\sharp} a_{n_1} \cdots a_{n_r}, \quad (4.23)$$

then the nonconcentration inequality holds, and so we next assume that this condition fails, and show that

$$\left(\sum_{n \in I} a_n \right)^r \leq (r(r-1))^{r-1} \sum_{n \in I} a_n^r. \quad (4.24)$$

In terms of the sequence $\mathbf{a} = \{a_n\}_n$, this is the claim that $\|\mathbf{a}\|_{\ell^1} \leq (r(r-1))^{1-1/r} \|\mathbf{a}\|_{\ell^r}$.

In general we can expand the left-hand side of (4.24) as $A_1 + A_2$ in which A_1 is the contribution from ordered tuples in which all indices are distinct, while A_2 is the remaining contribution, so that $A_2 = \binom{r}{2} \left(\sum_{n \in I} a_n^2 \right) \left(\sum_{n \in I} a_n \right)^{r-2}$. Now by the assumed failure of (4.23), $\left(\sum_{n \in I} a_n \right)^r > 2A_1$ so that

$$\frac{1}{2} \left(\sum_{n \in I} a_n \right)^r \leq \left(\sum_{n \in I} a_n \right)^r - A_1 = A_2.$$

Recalling the expression for A_2 (and using non-negativity of the a_n), we learn that

$$\left(\sum_{n \in I} a_n \right)^2 \leq r(r-1) \left(\sum_{n \in I} a_n^2 \right).$$

We recognize this as the statement that $\|\mathbf{a}\|_{\ell^1} \leq (r(r-1))^{1/2} \|\mathbf{a}\|_{\ell^2}$. Since $1 \leq 2 \leq r$, by the logarithmic convexity of ℓ^p norms, $\|\mathbf{a}\|_{\ell^2} \leq \|\mathbf{a}\|_{\ell^1}^{1-\theta} \|\mathbf{a}\|_{\ell^r}^\theta$ for that $\theta \in [0, 1]$ defined by $1/2 = (1-\theta)/1 + \theta/r$. We apply this to bound the ℓ^2 norm, and conclude that $\|\mathbf{a}\|_{\ell^1} \leq (r(r-1))^{\frac{1}{2\theta}} \|\mathbf{a}\|_{\ell^r}$, which is the desired inequality.

5 Type II Superorthogonality: Discrete Operators

We now examine the role of Type II superorthogonality in a new setting, that of discrete arithmetic operators acting on functions of \mathbb{Z} . Discrete operators gained widespread attention with work of Bourgain [7–10] on discrete maximal Radon transforms, such as the operator defined for a fixed integer $k \geq 2$ by

$$Mf(n) = \sup_{r \geq 1} \left| \frac{1}{r} \sum_{1 \leq m \leq r} f(n - m^k) \right|.$$

Bourgain's motivation was that proving such an operator is bounded on ℓ^p for a certain p implies a pointwise ergodic theorem for $\frac{1}{r} \sum_{1 \leq m \leq r} T^{m^k} f$ as $r \rightarrow \infty$, for T a measure-preserving transformation acting on functions in the relevant ℓ^p space. (More generally \mathbb{Z} can be replaced by \mathbb{Z}^d and m^k can be replaced by any integer-valued polynomial mapping.)

Bourgain's initial work stimulated further investigation of discrete operators. Many singular and maximal integral operators initially defined in the real-variable setting have a clear discrete analogue, but the discrete analogue is often surprisingly difficult to handle, because arithmetic comes into play. One natural and interesting class of operators is the family of discrete singular Radon transforms, defined for example in a one-dimensional setting by

$$Rf(n) = \sum_{\substack{m \in \mathbb{Z} \\ m \neq 0}} f(n - P(m)) \frac{1}{m} \tag{5.1}$$

for a fixed integer-valued polynomial P (and more generally with $1/m$ replaced by $K(m)$, with K an appropriate Calderón–Zygmund kernel, e.g. [38, §1]). The real-variable analogue suggests that this discrete operator should be bounded on ℓ^p for $1 < p < \infty$, but this remained out of reach until *tour de force* work of Ionescu and Wainger [38], which cleverly combined many analytic and arithmetic ideas.

The Ionescu–Wainger method has been extremely influential, appearing in many subsequent papers on discrete operators. We show here that their ideas can be framed in terms of direct and converse inequalities for a certain family of discrete operators, using Type II superorthogonality. We focus on a simplified setting that highlights the aspects of their work closest to our present focus.

5.1 Preliminaries

To set notation, given a function $f \in \ell^1(\mathbb{Z})$, define the Fourier transform to be the 1-periodic function

$$\widehat{f}(\xi) = \sum_{n \in \mathbb{Z}} f(n) e^{-2\pi i n \xi},$$

which we may regard on the torus, identified with $(-1/2, 1/2]$. Given a 1-periodic function $h \in L^2_{\text{loc}}(\mathbb{R})$ which we may regard on the torus identified with $(-1/2, 1/2]$, the Fourier inverse is the function defined on \mathbb{Z} by

$$\check{h}(n) = \int_{(-1/2, 1/2]} h(\xi) e^{2\pi i n \xi} d\xi.$$

A bounded 1-periodic function $m : \mathbb{R} \rightarrow \mathbb{C}$ defines an operator $f \mapsto (m\widehat{f})^\vee$, which is bounded on $\ell^2(\mathbb{Z})$ by Plancherel's theorem. We will also use the Euclidean Fourier transform $(\mathcal{F}f)(\xi) = \int_{\mathbb{R}} f(x) e^{-2\pi i x \xi} dx$ and its corresponding inverse $(\mathcal{F}^{-1}g)(x) = \int_{\mathbb{R}} g(\xi) e^{2\pi i x \xi} d\xi$.

We say that a bounded, measurable function m is an $L^p(\mathbb{R})$ multiplier of norm B_p if the operator T defined by $Tf = \mathcal{F}^{-1}(m \cdot \mathcal{F}f)$ satisfies $\|Tf\|_{L^p} \leq B_p \|f\|_{L^p}$ for all $f \in L^p(\mathbb{R})$. Now let us assume that m is an $L^p(\mathbb{R})$ multiplier of norm B_p that in addition is compactly supported in $(-1/2, 1/2]$. Then the operator T is a convolution operator given by $Tf = f * K$, where $K(x) = (\mathcal{F}^{-1}m)(x) = \int_{\mathbb{R}} m(\xi) e^{2\pi i x \xi} d\xi$, and since we assume m is compactly supported in $(-1/2, 1/2]$, K is C^∞ and in particular its restriction $K|_{\mathbb{Z}}$ to integers is well-defined. Thus we can obtain from T an operator acting on functions of \mathbb{Z} by defining

$$T_{\text{dis}}f(n) = \sum_{m \in \mathbb{Z}} f(n - m) K(m).$$

Alternatively, since $m(\xi)$ is supported in $(-1/2, 1/2]$, we may naturally 1-periodize it by setting

$$m_{\text{per}}(\xi) = \sum_{\ell \in \mathbb{Z}} m(\xi - \ell),$$

and then we can define a discrete operator $f \mapsto (m_{\text{per}}\widehat{f})^\vee$ acting on functions f of \mathbb{Z} . These two procedures result in the same discrete operator T_{dis} , and in particular $m_{\text{per}}(\xi)$ is the Fourier multiplier of T_{dis} , that is $(T_{\text{dis}}f)^\vee = m_{\text{per}}\widehat{f}$, and $m_{\text{per}} = (K|_{\mathbb{Z}})^\vee$. See [46, §2] for these deductions. We now apply these formal notions to a specific setting.

5.2 The Discrete Operator

Let m be an $L^p(\mathbb{R})$ multiplier that is compactly supported in $(-1/2, 1/2]$. Fix a finite set Z of positive integers, and let $\mathcal{R}(Z)$ denote the set of irreducible fractions with denominators in Z , namely

$$\mathcal{R}(Z) = \{a/q : q \in Z, 1 \leq a \leq q, (a, q) = 1\}.$$

(If $Z = \{q\}$ is a singleton set, we will denote $\mathcal{R}(Z)$ by $\mathcal{R}(q)$.) Fix $\varepsilon > 0$. Given $f \in \ell^1(\mathbb{Z})$, for each $a/q \in \mathcal{R}(Z)$ define $f_{a/q}$ by

$$\widehat{f}_{a/q}(\xi) = \sum_{\ell \in \mathbb{Z}} m(\varepsilon^{-1}(\xi - \ell - a/q)) \widehat{f}(\xi) = m_{\text{per}}(\varepsilon^{-1}(\xi - a/q)) \widehat{f}(\xi), \quad (5.2)$$

which is well-defined by the discussion above. We will focus on the operator

$$f \mapsto \sum_{a/q \in \mathcal{R}(Z)} f_{a/q}. \quad (5.3)$$

Ionescu and Wainger's main result [38, Theorem 1.5] leading to a proof of the ℓ^p boundedness of the operator (5.1) is as follows. They show that for any $\delta_0 > 0$ and $N \geq 1$, there exists an enlargement Z_N of the set $\{1, 2, 3, \dots, N\}$, obtained by including certain additional integers of size at most $e^{N^{\delta_0}}$ so that the operator (5.3), summed over $a/q \in \mathcal{R}(Z_N)$ and with $\varepsilon < e^{-N^{2\delta_0}}$, is bounded on $\ell^p(\mathbb{Z})$ for every $1 < p < \infty$, with operator norm at most $C_{p, \delta_0} (\log N)^{2/\delta_0}$. The most difficult aspects of the proof are (i) allowing any $0 < \delta_0 < 1$, and (ii) achieving at most logarithmic dependence on N in the operator norm.

We will focus on a key building block that underlies this theorem: the case where Z is a *relatively prime set*, namely $\gcd(q, q') = 1$ for all $q \neq q' \in Z$. (To rule out certain vacuous cases, we also assume that $q > 1$ for all $q \in Z$; this is no limitation in applications of the method.)

In this section, we present a proof of the following main result, in which for each fixed even $p = 2r$ we assume that $f_{a/q}$ has been defined according to an $L^{2r}(\mathbb{R})$ multiplier m supported in $(-1/2, 1/2]$, as above. We require the notion of $\omega(q)$, the number of distinct prime divisors of an integer q . Given any set Z of integers, we define

$$\mathcal{Q}(Z) = \max\{\omega(q) : q \in Z\}.$$

Theorem 5.1 *Let Z be a relatively prime set of integers contained in $(1, q(Z)]$. Then for any integer $r \geq 1$, as long as $\varepsilon < r^{-1}q(Z)^{-2r}$, for all $f \in \ell^{2r}(\mathbb{Z})$,*

$$\left\| \sum_{a/q \in \mathcal{R}(Z)} f_{a/q} \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_{2r} (2^{\mathcal{Q}(Z)})^{1-1/r} \|f\|_{\ell^{2r}(\mathbb{Z})}, \quad (5.4)$$

in which the constant C_{2r} is independent of Z , ε , and f .

We have isolated this theorem as a special case underlying [38, Thm. 1.5] that best illuminates the role that direct and converse inequalities play in their method. See Sect. 5.9 for a few remarks on the general setting.

5.3 Overview of the Proof: Direct and Converse Inequalities

5.3.1 Direct Inequality

Given a set Z of integers, proving that the set of functions $\{f_{a/q}\}_{a/q \in \mathcal{R}(Z)}$ satisfies some notion of superorthogonality requires Diophantine properties of the irreducible fractions in $\mathcal{R}(Z)$. In general this assumes some arithmetic structure on Z , and in our special case we will exploit the assumption that Z is a relatively prime set.

Suppose we could show that for any tuple $(a_1/q_1, \dots, a_{2r}/q_{2r})$ of elements $a_i/q_i \in \mathcal{R}(Z)$ that has the uniqueness property,

$$\sum_{x \in \mathbb{Z}} f_{a_1/q_1}(x) \overline{f}_{a_2/q_2}(x) \cdots f_{a_{2r-1}/q_{2r-1}}(x) \overline{f}_{a_{2r}/q_{2r}}(x) = 0. \quad (5.5)$$

Then the formal argument in Sect. 3 would immediately imply a direct inequality for the functions $\{f_{a/q}\}_{a/q \in \mathcal{R}(Z)}$. However, this strong property does not hold (see Remark 5.7), and as a whole the collection $\{f_{a/q}\}_{a/q \in \mathcal{R}(Z)}$ does not exhibit Type II superorthogonality. Instead we proceed in two steps: we first show that (5.5) vanishes if the tuple of denominators $(q_1, q_2, \dots, q_{2r-1}, q_{2r})$ satisfies the uniqueness property. Second, we develop a multilinear direct inequality that exploits a uniqueness property amongst numerators. This two-step process results in a more complicated direct inequality, which we now state:

Proposition 5.2 (Direct inequality) *Let Z be a relatively prime set of integers contained in $(1, q(Z)]$. Then as long as $\varepsilon < r^{-1}q(Z)^{-2r}$,*

$$\begin{aligned} \left\| \sum_{a/q \in \mathcal{R}(Z)} f_{a/q} \right\|_{\ell^{2r}(\mathbb{Z})} &\leq C_{2r} \left\| \left(\sum_{a/q \in \mathcal{R}(Z)} |f_{a/q}|^2 \right)^{1/2} \right\|_{\ell^{2r}(\mathbb{Z})} \\ &\quad + C_{2r} \left\| \left(\sum_{q \in Z} \left| \sum_{a/q \in \mathcal{R}(q)} f_{a/q} \right|^{2r} \right)^{1/2r} \right\|_{\ell^{2r}(\mathbb{Z})}, \end{aligned}$$

for a constant C_{2r} independent of Z , ε and f .

Next, we require a converse inequality for each of the terms on the right-hand side. While we have seen superorthogonality play a role in the proof of Khintchine's converse inequality (by duality), and in Paley's converse inequality, superorthogonality seems to be of no help for the converse inequality for the functions $\{f_{a/q}\}$. Instead,

for a converse inequality for the first term, we use “uniform spacing” in the Fourier transform, which enables a square function estimate that is adapted to frequency projections onto arbitrary intervals that are regularly (rather than dyadically) spaced. For the second term, we use the “method of sampling,” and arithmetic properties of the set Z of denominators.

5.3.2 The First Converse Inequality

In general, we say a countable collection of real numbers $\{\xi_j\}$ is δ -separated if any open interval of length δ contains at most one point of $\{\xi_j\}$. We now state a general result: a converse inequality in ℓ^p that holds for a sequence of functions $\{f_j\}$ with $f_j = T_j f$ where T_j has multiplier $m(\xi - \xi_j)$, as long as $\{\xi_j\}$ is a δ -separated set, and m is an L^p multiplier supported on a subinterval of $(-1/2, 1/2]$ of diameter sufficiently small relative to δ . (In particular, there can be at most $O(\delta^{-1})$ points in a δ -separated set contained in $(-1/2, 1/2]$, so in what follows, the indices j lie in an appropriate finite set.)

To be precise, if $Tf = f * K$ is a convolution operator bounded on $L^p(\mathbb{R})$ with distribution kernel K , then $\mathcal{F}(K)(\xi) = m(\xi) = \int K(x)e^{-2\pi i x \xi} dx$ is a bounded function, and so m is the $L^p(\mathbb{R})$ multiplier such that $\mathcal{F}(Tf)(\xi) = m(\xi)\mathcal{F}(f)(\xi)$; if T has norm A_p on $L^p(\mathbb{R})$, m has multiplier norm A_p . If in addition we assume m is supported in $(-1/2, 1/2]$, then as remarked before we can periodize it to $m_{\text{per}}(\xi)$ and define the discrete operator T_{dis} with Fourier multiplier m_{per} ; then Parseval–Plancherel states that $\|T_{\text{dis}}f\|_{\ell^2(\mathbb{Z})}^2 = \|m \widehat{f}\|_{L^2(-1/2, 1/2]}^2$. In what follows, we also consider for each shift ξ_j in a well-separated set, an operator T_j with multiplier $m(\xi - \xi_j)$. In order to regard either T or T_j as an operator on discrete functions, we must periodize $m(\xi)$ and $m(\xi - \xi_j)$ and define the corresponding discrete operators. However, in order to simplify notation in the following theorem, we also denote the discretization of T_j by T_j .

Theorem 5.3 *Let $0 < \delta < 1$ and $2 \leq p < \infty$ be given. Let m be an $L^p(\mathbb{R})$ multiplier of norm A_p and assume that m is supported in $|\xi| \leq c_0 \delta$ for a constant $c_0 < 1/2$. Given a point $\xi_j \in (-1/2, 1/2]$, let T_j be the operator with multiplier $m(\xi - \xi_j)$. If a set $\{\xi_j\}$ of points in $(-1/2, 1/2]$ is δ -separated, then the corresponding discrete operator T_j has the property that for every $f \in \ell^p(\mathbb{Z})$,*

$$\left\| \left(\sum_j |T_j f|^2 \right)^{1/2} \right\|_{\ell^p(\mathbb{Z})} \leq C_p \|f\|_{\ell^p(\mathbb{Z})},$$

for a constant C_p depending only on c_0 and A_p .

We prove this using ideas of Rubio de Francia [58]. It implies a converse inequality for the first term on the right-hand side of Proposition 5.2, once we show that the points in $\mathcal{R}(Z)$ are sufficiently well-separated.

Lemma 5.4 *If Z is a set of integers contained in $(1, q(Z))$, then $\mathcal{R}(Z)$ is δ -separated for all $\delta < q(Z)^{-2}$. Moreover, $\cup_{q \in Z} \mathcal{R}(q)$ is a disjoint union.*

Proof To show that no open interval of length δ can contain two distinct elements a/q and a'/q' in $\mathcal{R}(Z)$, suppose on the contrary that $|a/q - a'/q'| \leq \delta$. Since a/q and a'/q' are both irreducible fractions, a, q and a', q' are distinct as pairs, so that $aq' - a'q$ is a nonzero integer, implying

$$\frac{1}{qq'} \leq \frac{|aq' - a'q|}{qq'} = \left| \frac{a}{q} - \frac{a'}{q'} \right| \leq \delta.$$

This implies $\delta \geq q(Z)^{-2}$, a contradiction. Thus indeed the set $\mathcal{R}(Z)$ is δ -separated. This argument also shows that $\cup_{q \in Z} \mathcal{R}(q)$ is a disjoint union, since arguing as above shows that $a/q \notin \mathcal{R}(q')$ for any $q' \neq q$. \square

As a result, Theorem 5.3 immediately implies the first converse inequality we require, as long as ε is sufficiently small.

Proposition 5.5 (First converse inequality) *Let an integer $r \geq 1$ be fixed. Let Z be a set of integers contained in $(1, q(Z)]$, and suppose $\varepsilon < q(Z)^{-2}$. Then*

$$\left\| \left(\sum_{a/q \in \mathcal{R}(Z)} |f_{a/q}|^2 \right)^{1/2} \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_{2r} \|f\|_{\ell^{2r}(\mathbb{Z})},$$

for a constant C_{2r} depending only on the L^{2r} norm of the multiplier m .

Note that for this converse inequality and the one below, we no longer require Z to be a relatively prime set, although we did require this for the direct inequality.

5.3.3 The Second Converse Inequality

Treating the second term on the right-hand side of Proposition 5.2 requires a different approach; here we apply the “method of sampling” developed in another seminal paper on discrete operators, by Magyar et al. [46]. We record the outcome of the method of sampling later in Theorem 5.16, and state the relevant consequence here; we still call it a converse inequality although it is not strictly speaking for a square function.

Proposition 5.6 (Second converse inequality) *Let an integer $r \geq 1$ be fixed. Let Z be a set of integers contained in $(1, q(Z)]$, and suppose $\varepsilon < q(Z)^{-2}$. Then*

$$\left\| \left(\sum_{q \in Z} \left| \sum_{a/q \in \mathcal{R}(q)} f_{a/q} \right|^{2r} \right)^{1/2r} \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_{2r} (2^{\Omega(Z)})^{1-1/r} \|f\|_{\ell^{2r}(\mathbb{Z})},$$

for a constant C_{2r} depending only on the L^{2r} norm of the multiplier m .

These three main propositions directly imply Theorem 5.1. We now begin the proof of each, starting with the direct inequality.

5.4 Direct Inequality (Step 1): Type II Superorthogonality Among Denominators

Proof of the direct inequality in Proposition 5.2 requires Type II superorthogonality in two steps. In Step 1, we apply Type II superorthogonality amongst tuples of functions

$$f_{a_1/q_1}, f_{a_2/q_2}, \dots, f_{a_{2r-1}/q_{2r-1}}, f_{a_{2r}/q_{2r}}$$

in which the tuple of denominators $(q_1, q_2, \dots, q_{2r})$ satisfies the uniqueness property. In Step 2, a multilinear direct inequality follows from Type II superorthogonality amongst tuples in which the numerators in $(a_1/q_1, a_2/q_2, \dots, a_{2r}/q_{2r})$ satisfy the uniqueness property (and at most two denominators take any given value).

For each $q \in Z$, define

$$F_q = \sum_{u \in \mathcal{R}(q)} f_u. \quad (5.6)$$

The goal of Step 1 is to prove the direct inequality

$$\left\| \sum_{q \in Z} F_q \right\|_{\ell^{2r}} \leq C_r \left\| \left(\sum_{q \in Z} |F_q|^2 \right)^{1/2} \right\|_{\ell^{2r}}. \quad (5.7)$$

It suffices to verify Type II superorthogonality holds for the functions $\{F_q\}_{q \in Z}$. We need only show that for any tuple $(q_1, q_2, \dots, q_{2r-1}, q_{2r})$ that has the uniqueness property,

$$\sum_{x \in \mathbb{Z}} F_{q_1}(x) \overline{F_{q_2}(x)} \cdots F_{q_{2r-1}}(x) \overline{F_{q_{2r}}(x)} = 0.$$

In fact we can show a stronger property holds term by term: for any tuple of denominators (q_1, \dots, q_{2r}) with the uniqueness property, for each tuple (u_1, \dots, u_{2r}) with $u_i = a_i/q_i \in \mathcal{R}(q_i)$,

$$\sum_{x \in \mathbb{Z}} f_{u_1} \overline{f_{u_2}} \cdots f_{u_{2r-1}} \overline{f_{u_{2r}}}(x) = 0. \quad (5.8)$$

Upon defining

$$G_{u_1, \dots, u_{2r}}(\xi) = (f_{u_1} \overline{f_{u_2}} \cdots f_{u_{2r-1}} \overline{f_{u_{2r}}})\widehat{ }(\xi),$$

the identity (5.8) is the statement that $G_{u_1, \dots, u_{2r}}(0) = 0$, so that it suffices to show that the support of $G_{u_1, \dots, u_{2r}}$ does not contain the origin.

We recall that Z is a relatively prime set of integers contained in $(1, q(Z)]$, and $\varepsilon < r^{-1}q(Z)^{-2r}$. Let $\varepsilon\mathbb{Q}$ denote the periodization of the scaled unit interval $\varepsilon(-1/2, 1/2]$,

that is,

$$\varepsilon \mathbf{Q} = \bigcup_{\ell \in \mathbb{Z}} (\ell - \varepsilon/2, \ell + \varepsilon/2].$$

For each u , the support of $(f_u) \widehat{\wedge} (\xi)$ is contained in $\varepsilon \mathbf{Q} + u$ and the support of $(\overline{f_u}) \widehat{\wedge} (\xi) = (f_u) \widehat{\wedge} (-\xi)$ is contained in $\varepsilon \mathbf{Q} - u$. The function $G_{u_1, \dots, u_{2r}}(\xi)$ is a convolution of $2r$ such functions and has support contained in

$$2r\varepsilon \mathbf{Q} + u_1 - u_2 + \dots + u_{2r-1} - u_{2r}. \quad (5.9)$$

Recall that each $u_i = a_i/q_i \in \mathcal{R}(q_i)$. Under the uniqueness assumption, we may assume without loss of generality that q_1 is distinct from q_2, \dots, q_{2r} . Let a'/q' denote the (signed) reduced fraction such that $a_1/q_1 - a'/q' = u_1 - (u_2 - u_3 + \dots - u_{2r-1} + u_{2r}) \pmod{1}$. Then $q' \leq q(Z)^{2r-1}$, and since Z is a relatively prime set, $(q_1, q') = 1$; since $q_1 > 1$ this implies $q_1 \neq q'$. In particular, the reduced fractions a_1/q_1 and a'/q' are distinct.

Now supposing that the set (5.9) does contain the origin, we would have $|a_1/q_1 - a'/q'| \leq r\varepsilon$. But since $a_1q' - a'q_1$ is a nonzero integer, this would imply that

$$\frac{1}{q_1 q'} \leq \left| \frac{a_1 q' - a' q_1}{q_1 q'} \right| = \left| \frac{a_1}{q_1} - \frac{a'}{q'} \right| \leq r\varepsilon \quad (5.10)$$

and hence $r\varepsilon > q(Z)^{-2r}$, which contradicts our assumption that $\varepsilon < r^{-1}q(Z)^{-2r}$. We conclude that 0 does not lie in the support of $G_{u_1, \dots, u_{2r}}$. This verifies the superorthogonality property, and completes the proof of the direct inequality (5.7) in Step 1.

Remark 5.7 Here we can see that we cannot verify (5.5) if we merely assume the tuple of rationals $(a_1/q_1, \dots, a_{2r}/q_{2r})$ has the uniqueness property. Indeed, if $q_i = q$ for all $i = 1, \dots, 2r$ but $a_1 = a_2 - a_3 + \dots - a_{2r-1} + a_{2r}$ with $a_1 \notin \{a_2, a_3, \dots, a_{2r-1}, a_{2r}\}$, then (5.9) could contain the origin. Compare this to Step 2 below, in which we use an r -linear formulation to ensure that no more than two denominators can share the same value.

The direct inequality (5.7) in terms of the functions $\{F_q\}$ is not yet sufficient for the purposes of proving Theorem 5.1, since our converse inequality in Theorem 5.3 does not apply directly to operators such as F_q . (This is because there is no single multiplier $M(\xi)$ such that for every q , F_q can be defined according to a multiplier that is a shift of $M(\xi)$. We can for example see this from the basic observation that as q varies, the number of summands in F_q varies.)

Thus we proceed with a second step: we expand the right-hand side of (5.7) and apply the non-concentration inequality of Lemma 4.1. This yields

$$\left\| \left(\sum_{q \in Z} |F_q|^2 \right)^{1/2} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} = \sum_x \left(\sum_{q \in Z} |F_q|^2 \right)^r$$

$$\leq C_r \sum_x \sum_{q \in Z} |F_q|^{2r} + C_r \sum_x \sum_{(q_1, \dots, q_r) \in Z^r}^{\#} |F_{q_1}|^2 \cdots |F_{q_r}|^2, \quad (5.11)$$

in which $\sum^{\#}$ indicates that the sum restricts to those ordered tuples (q_1, \dots, q_r) with all pairwise distinct entries. The first “diagonal” term we recognize as the second term on the right-hand side in Proposition 5.2. The second “off-diagonal” term we will treat further, by applying a multilinear direct inequality for functions with Type II superorthogonality.

5.5 A Multilinear Direct Inequality via Type II Superorthogonality

We now show that Type II superorthogonality implies an r -multilinear direct inequality in L^{2r} . To work in full generality, we let \mathcal{U} be a finite index set, and for each of $j = 1, \dots, r$ we suppose we are given a set $\{g_u^{(j)}\}_{u \in \mathcal{U}}$ of functions in L^{2r} ; as usual in such formal arguments we refer to $L^{2r}(X, d\mu)$, which we could take for example to be $X = \mathbb{R}$ or $(-1/2, 1/2]$ with Lebesgue measure, or \mathbb{Z} with counting measure.

Proposition 5.8 (Multilinear direct inequality)

For every integer $r \geq 1$ there exists a constant C_r such that the following holds. For each $1 \leq j \leq r$, let $\{g_u^{(j)}\}_{u \in \mathcal{U}}$ be a sequence of functions in L^{2r} . Suppose that for every $2r$ -tuple of indices $(u_1, u_2, \dots, u_{2r}) \in \mathcal{U}^{2r}$ that has the uniqueness property,

$$\int g_{u_1}^{(1)} \bar{g}_{u_2}^{(1)} \cdots g_{u_{2r-1}}^{(r)} \bar{g}_{u_{2r}}^{(r)} = 0.$$

Then

$$\left\| \prod_{j=1}^r \left(\sum_{u \in \mathcal{U}} g_u^{(j)} \right)^{1/r} \right\|_{L^{2r}} \leq C_r \left\| \prod_{j=1}^r \left(\left(\sum_{u \in \mathcal{U}} |g_u^{(j)}|^2 \right)^{1/2} \right)^{1/r} \right\|_{L^{2r}}.$$

In the proof, it will be useful to have a notation for the tuple $(u_1, u_2, \dots, u_{2r})$ that makes it more visible which of these indices are applied to the j th collection of functions $g_u^{(j)}$, for $j = 1, \dots, r$. Thus we will now denote any such tuple with the notation

$$(u_1(0), u_1(1), u_2(0), u_2(1), \dots, u_r(0), u_r(1)).$$

We will again use the convention that a tuple is an ordered sequence of entries, while the set $\{u_1(0), u_1(1), u_2(0), u_2(1), \dots, u_r(0), u_r(1)\}$ denotes the unordered set of distinct elements appearing in the tuple.

We require a sorting lemma based on the uniqueness property.

Lemma 5.9 *Let $r \geq 1$ be a fixed integer, and let $(u_1(0), u_1(1), \dots, u_r(0), u_r(1))$ be a $2r$ -tuple of integers that does not have the uniqueness property. Then there exists a*

function $\kappa : \{1, \dots, r\} \mapsto \{0, 1\}$ so that as sets,

$$\begin{aligned} \{u_1(0), u_1(1), \dots, u_r(0), u_r(1)\} &= \{u_1(\kappa(1)), \dots, u_r(\kappa(r))\} \\ &= \{u_1(1 - \kappa(1)), \dots, u_r(1 - \kappa(r))\}. \end{aligned}$$

Let us defer the proof of this momentarily, and see why it suffices for proving the multilinear direct inequality. We raise both sides of the claimed inequality to the $2r$ -th power; then the left-hand side may be expanded as

$$\sum_{(u_1(0), u_1(1), \dots, u_r(0), u_r(1)) \in \mathcal{U}^{2r}} \int \prod_{j=1}^r \left(g_{u_j(0)}^{(j)} \bar{g}_{u_j(1)}^{(j)} \right). \quad (5.12)$$

For any tuple $(u_1(0), u_1(1), \dots, u_r(0), u_r(1))$ with the uniqueness property, the corresponding integral vanishes, by the assumed superorthogonality. Define for any subset $A \subseteq \mathcal{U}$ the function

$$S_A(x) = \sum_{\substack{(u_1(0), u_1(1), \dots, u_r(0), u_r(1)) \\ \{u_1(0), u_1(1), \dots, u_r(0), u_r(1)\} = A}} g_{u_1(0)}^{(1)}(x) \bar{g}_{u_1(1)}^{(1)}(x) \cdots g_{u_r(0)}^{(r)}(x) \bar{g}_{u_r(1)}^{(r)}(x).$$

Thus the left-hand side contribution (5.12) is equal to

$$\sum_{|A| \leq r} \int S_A, \quad (5.13)$$

in which we need only consider $|A| \leq r$ since any $2r$ -tuple without the uniqueness property contains at most r distinct values.

On the other hand, for any set $A \subseteq \mathcal{U}$ with $|A| \leq r$, define the function

$$T_A(x) = \sum_{\substack{(u_1, \dots, u_r) \\ \{u_1, \dots, u_r\} = A}} \left| g_{u_1}^{(1)}(x) \right|^2 \cdots \left| g_{u_r}^{(r)}(x) \right|^2.$$

The multilinear direct inequality will be proved if we can verify that

$$\sum_{|A| \leq r} \int S_A \leq C_r^{2r} \sum_{|A| \leq r} \int T_A.$$

Note that once a fixed subset $|A| \leq r$ is chosen, there are at most d_r $2r$ -tuples such that the set $\{u_1(0), u_1(1), \dots, u_r(0), u_r(1)\}$ is equal to A , for some combinatorial constant d_r . Thus the inequality above will hold (with $C_r^{2r} = d_r$) if we can show that for each set A with $|A| \leq r$, for each tuple with set $\{u_1(0), u_1(1), \dots, u_r(0), u_r(1)\} = A$,

$$\int \left| g_{u_1(0)}^{(1)} \bar{g}_{u_1(1)}^{(1)} \cdots g_{u_r(0)}^{(r)} \bar{g}_{u_r(1)}^{(r)} \right| \leq \int T_A.$$

We apply Lemma 5.9. to rewrite the left-hand side as

$$\begin{aligned} & \int \left| g_{u_1(\kappa(1))}^{(1)} \cdots g_{u_r(\kappa(r))}^{(r)} \right| \cdot \left| g_{u_1(1-\kappa(1))}^{(1)} \cdots g_{u_r(1-\kappa(r))}^{(r)} \right| \\ & \leq \frac{1}{2} \int \left| g_{u_1(\kappa(1))}^{(1)} \cdots g_{u_r(\kappa(r))}^{(r)} \right|^2 + \frac{1}{2} \int \left| g_{u_1(1-\kappa(1))}^{(1)} \cdots g_{u_r(1-\kappa(r))}^{(r)} \right|^2. \end{aligned}$$

Here we also used the fact that $AB \leq (1/2)(A^2 + B^2)$ for A, B non-negative real numbers. By the lemma, each of the tuples $(u_1(\kappa(1)), \dots, u_r(\kappa(r)))$ and $(u_1(1 - \kappa(1)), \dots, u_r(1 - \kappa(r)))$ is a term represented in the sum defining $T_A(x)$, and thus in particular the right-hand side is bounded above by $\int T_A$, as desired.

We now return to the proof of the sorting property in Lemma 5.9, using an argument appearing in [48, Lemma 2.22]. We will denote the set $\{u_1(0), u_1(1), \dots, u_r(0), u_r(1)\}$ by A ; since the tuple does not have the uniqueness property, we know that $|A| \leq r$. Let us first see that we need only prove the lemma in the case $|A| = r$. In fact, if for some $s \leq r$ the lemma holds for all sets of cardinality s , then the lemma is also proved for all sets with cardinality $s - 1$. For suppose that the set of values appearing in the tuple is $A = \{a_1, \dots, a_{s-1}\}$, with $s - 1 < r$. Then in the $2r$ -tuple $(u_1(0), u_1(1), \dots, u_r(0), u_r(1))$, one value (say a_i) must appear at least four times, or two distinct values (say a_i and a_j) must each appear at least three times. We construct a new $2r$ -tuple in the first case by changing two occurrences of a_i to a new value $a_s \notin A$, and in the second case by changing one occurrence of a_i to a_s and one occurrence of a_j to a_s . This new tuple $(u_1(0)', u_1(1)', \dots, u_r(0)', u_r(1)')$ does not have the uniqueness property, and takes s distinct values in the set $A' = A \cup \{a_s\}$. The version of the lemma assumed to hold for cardinality s sets now applies, and the map κ it provides shows that $\{u_1(\kappa(1))', \dots, u_1(\kappa(1))'\} = A'$ and $\{u_1(1 - \kappa(1))', \dots, u_1(1 - \kappa(1))'\} = A'$. As a consequence, we deduce that $\{u_1(\kappa(1)), \dots, u_1(\kappa(1))\} = A$ and $\{u_1(1 - \kappa(1)), \dots, u_1(1 - \kappa(1))\} = A$, as desired.

Now we prove the lemma in the case $|A| = r$, so that each value in A is taken by precisely two elements in the tuple. We can construct a bipartite graph as follows. One set of vertices represents the set of indices $\{1, \dots, r\}$ and the other set of vertices represents the set of values $\{a_1, \dots, a_r\}$. We will connect a vertex i and a vertex a_i with an edge if $u_i(0) = a_j$, and with another edge if $u_i(1) = a_j$. In particular, every vertex in this finite bipartite graph is associated to precisely 2 edges. It follows that the graph is a union of finite cycles, each with an even number of edges. In each such cycle, we color the edges red and blue, alternately. In particular, each vertex corresponding to an index $i \in \{1, \dots, r\}$ has a red edge and a blue edge. We will define $\kappa(i)$ to be the value in $\{0, 1\}$ such that the edge between the vertex representing the index i and the vertex representing the value $u_i(\kappa(i))$ is red. Since each vertex corresponding to a value a_i has a red edge and a blue edge, this map has the desired property, and the lemma is proved.

This completes the verification of the lemma, and hence of the multilinear direct inequality.

5.6 Direct Inequality (Step 2): Type II Superorthogonality Among Numerators

We now apply the multilinear direct inequality to the setting of our functions $\{f_{a/q}\}$. For any integer $q \in \mathbb{Z}$, define the square function

$$S_q(f) = \left(\sum_{a/q \in \mathcal{R}(q)} |f_{a/q}|^2 \right)^{1/2}.$$

Lemma 5.10 (Multilinear direct inequality) *Let (q_1, \dots, q_r) be a tuple of distinct integers that are all pairwise relatively prime. Then as long as $\varepsilon < r^{-1} \max\{q_1, \dots, q_r\}^{-2r}$,*

$$\left\| (F_{q_1})^{1/r} \cdots (F_{q_r})^{1/r} \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_r \left\| (S_{q_1}(f))^{1/r} \cdots (S_{q_r}(f))^{1/r} \right\|_{\ell^{2r}(\mathbb{Z})}.$$

This will follow immediately from the general inequality in Proposition 5.8 after we set some notation and verify the appropriate superorthogonality condition. Define the set $Z' = \{q_1, \dots, q_r\}$. For each $i = 1, \dots, r$, and for each $u \in \mathcal{R}(Z')$, define

$$g_u^{(i)}(x) = \mathbf{1}_{\mathcal{R}(q_i)}(u) f_u(x),$$

so that it detects whether the denominator is q_i . Then

$$\begin{aligned} \left\| (F_{q_1})^{1/r} \cdots (F_{q_r})^{1/r} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} &= \sum_{x \in \mathbb{Z}} |F_{q_1}|^2 \cdots |F_{q_r}|^2 \\ &= \sum_{x \in \mathbb{Z}} \left| \sum_{u_1 \in \mathcal{R}(Z')} g_{u_1}^{(1)}(x) \right|^2 \cdots \left| \sum_{u_r \in \mathcal{R}(Z')} g_{u_r}^{(r)}(x) \right|^2. \end{aligned}$$

Thus Proposition 5.8 provides the inequality claimed in our lemma, as long as we can verify that for every tuple $(u_1(0), u_1(1), \dots, u_r(0), u_r(1))$ of elements in $\mathcal{R}(Z')$ with the uniqueness property,

$$\sum_{x \in \mathbb{Z}} g_{u_1(0)}^{(1)} \bar{g}_{u_1(1)}^{(1)} \cdots g_{u_r(0)}^{(r)} \bar{g}_{u_r(1)}^{(r)}(x) = 0.$$

Arguing as in Step 1, this holds as long as the origin is not contained in the set

$$2r\varepsilon\mathbf{Q} + u_1(0) - u_1(1) + \cdots + u_r(0) - u_r(1). \quad (5.14)$$

Recall that for each $i = 1, \dots, r$, q_i is the denominator of $u_i(0)$ and of $u_i(1)$. Without loss of generality, assume that $u_1(0)$ is distinct from all the others. If we denote $u_1(0) = a_1/q_1$ and $u_1(1) = a_2/q_1$, in particular this means that $a_0/q_1 := a_1/q_1 - a_2/q_1 \neq 0$. Let a'/q' be the (signed) reduced fraction such that $a_0/q_1 - a'/q' = u_1(0) - u_1(1) + (u_2(0) - u_2(1) + \cdots + u_r(0) - u_r(1)) \pmod{1}$. Note that

$q' \leq q(Z)^{2r-1}$ and $(q_1, q') = 1$. Thus, a_0/q_1 is distinct from the reduced fraction a'/q' , and $a_0q' - a'q_1$ is a nonzero integer. Supposing that (5.14) does contain the origin, then we would have

$$\frac{1}{q_1 q'} \leq \left| \frac{a_0 q' - a' q_1}{q_1 q'} \right| = \left| \frac{a_0}{q_1} - \frac{a'}{q'} \right| \leq r\varepsilon.$$

This cannot occur if we have chosen $\varepsilon < r^{-1} \max\{q_1, \dots, q_r\}^{-2r}$. Thus the super-orthogonality property holds, and this concludes the proof of Lemma 5.10.

Remark 5.11 Note that here it was critical that at most two of the rationals $u_i(j)$ shared the same denominator; pairwise distinct fractions $a_1/q, \dots, a_j/q$ with $j \geq 3$ could have signed sum $a_1/q - a_2/q + \dots + (-1)^{j+1}a_j/q$ equal to zero, in which case the above argument would fail. This is why the application of the non-concentration inequality, and the r -linear formulation, is required.

Now we may complete the proof of the direct inequality in Proposition 5.2. Recall from our application of the non-concentration inequality in (5.11) that

$$\left\| \left(\sum_{q \in Z} |F_q|^2 \right)^{1/2} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} \leq C_r \sum_x \sum_{q \in Z} |F_q|^{2r} + C_r \sum_{(q_1, \dots, q_r) \in Z^r}^{\sharp} \sum_x |F_{q_1}|^2 \cdots |F_{q_r}|^2.$$

Since Z is a relatively prime set, we may apply Lemma 5.10 to each term in the restricted sum over q_1, \dots, q_r , so that

$$\begin{aligned} \sum_{(q_1, \dots, q_r) \in Z^r}^{\sharp} \sum_x |F_{q_1}|^2 \cdots |F_{q_r}|^2 &\leq C_r \sum_{(q_1, \dots, q_r) \in Z^r}^{\sharp} \sum_x S_{q_1}(f)(x)^2 \cdots S_{q_r}(f)(x)^2 \\ &\leq C_r \sum_x \left(\sum_{q \in Z} \sum_{a/q \in \mathcal{R}(q)} |f_{a/q}|^2 \right)^r \\ &= C_r \left\| \left(\sum_{q \in Z} \sum_{a/q \in \mathcal{R}(q)} |f_{a/q}|^2 \right)^{1/2} \right\|_{\ell^{2r}}^{2r} \\ &= C_r \left\| \left(\sum_{a/q \in \mathcal{R}(Z)} |f_{a/q}|^2 \right)^{1/2} \right\|_{\ell^{2r}}^{2r}. \end{aligned}$$

We have proved Proposition 5.2, the direct inequality in ℓ^{2r} for the functions $\{f_{a/q}\}$.

5.7 The First Converse Inequality

We now turn to the first converse inequality of Theorem 5.3, which we have seen immediately implies Proposition 5.5. We first prove a version in which the multiplier is a C^∞ function supported in $(-1/2, 1/2]$, which we will call $\Psi(\xi)$, with corresponding operator denoted by S_j . As mentioned before Theorem 5.3, in order to define the discrete operator associated to S_j , we must first periodize the multiplier $\Psi(\xi - \xi_j)$ to $\Psi_{\text{per}}(\xi - \xi_j)$. In order to simplify notation in the statement below, we denote both S_j and its associated discrete operator by S_j .

Theorem 5.12 *Let Ψ be a C^∞ function that is compactly supported in $(-1/2, 1/2]$, and fix $0 < \delta < 1$. Given a point $\xi_j \in (-1/2, 1/2]$, let S_j be the operator with multiplier $\Psi(\delta^{-1}(\xi - \xi_j))$. If a set $\{\xi_j\}$ of points in $(-1/2, 1/2]$ is δ -separated, then the corresponding discrete operator S_j has the property that for each $2 \leq p \leq \infty$,*

$$\left\| \left(\sum_j |S_j f|^2 \right)^{1/2} \right\|_{\ell^p(\mathbb{Z})} \leq C_p \|f\|_{\ell^p(\mathbb{Z})}$$

for a constant C_p depending only on Ψ and p , and independent of δ or the δ -separated set $\{\xi_j\}$.

We can deduce from this the result for a general L^p multiplier via the Marcinkiewicz–Zygmund inequality, which we proved in Theorem 2.1 as a consequence of Khintchine's inequality. Let us see how this deduction goes. In Theorem 5.3, $0 < \delta < 1$ is fixed and the given L^p multiplier $m(\xi)$ is supported in $|\xi| \leq c_0 \delta$ with $c_0 < 1/2$. We choose a C^∞ function Ψ supported in $(-1/2, 1/2]$ such that $\Psi(\xi) = 1$ for $|\xi| \leq c_0$, so that $\Psi(\delta^{-1}(\xi - \xi_j)) = 1$ on the support of $m(\xi - \xi_j)$, and we define the operator S_j accordingly with multiplier $\Psi(\delta^{-1}(\xi - \xi_j))$. Then $T_j = T_j S_j$ as operators acting on functions of \mathbb{R} . Similarly, after periodizing each kernel, we obtain $T_j = T_j S_j$ for the corresponding discrete operators acting on functions of \mathbb{Z} . By the variant of the Marcinkiewicz–Zygmund inequality in part (II) of Theorem 2.1, for any sequence of functions $F_j \in \ell^p(\mathbb{Z})$,

$$\left\| \left(\sum_j |T_j(F_j)|^2 \right)^{1/2} \right\|_{\ell^p} \leq C_p A_p \left\| \left(\sum_j |F_j|^2 \right)^{1/2} \right\|_{\ell^p} \quad (5.15)$$

for a constant C_p . In particular, given a function f of \mathbb{Z} , set $F_j = S_j(f)$, and apply this inequality to $T_j(F_j) = T_j S_j(f) = T_j(f)$ to obtain

$$\left\| \left(\sum_j |T_j(f)|^2 \right)^{1/2} \right\|_{\ell^p} \leq C_p A_p \left\| \left(\sum_j |S_j(f)|^2 \right)^{1/2} \right\|_{\ell^p}.$$

Then Theorem 5.3 follows from invoking Theorem 5.12, in which the resulting constant depends on the choice of Ψ , and hence on c_0 .

It remains to prove Theorem 5.12. It claims that an operator maps $\ell^p(\mathbb{Z})$ to $\ell^p(\mathbb{Z}; \ell^2(j \in \mathbb{Z}))$, and by interpolation it suffices to prove it for $p = 2$ and $p = \infty$. The case $p = 2$ holds by the Parseval–Plancherel theorem: for each j ,

$$\begin{aligned}\|S_j(f)\|_{\ell^2(\mathbb{Z})}^2 &= \|(\Psi_{\text{per}}(\delta^{-1}(\xi - \xi_j))\widehat{f}(\xi))^\vee\|_{\ell^2(\mathbb{Z})}^2 \\ &= \int_{(-1/2, 1/2]} |\Psi(\delta^{-1}(\xi - \xi_j))|^2 |\widehat{f}(\xi)|^2 d\xi.\end{aligned}$$

Thus

$$\begin{aligned}\left\| \left(\sum_j |S_j(f)|^2 \right)^{1/2} \right\|_{\ell^2(\mathbb{Z})}^2 &= \int_{(-1/2, 1/2]} \sum_j |\Psi(\delta^{-1}(\xi - \xi_j))|^2 |\widehat{f}(\xi)|^2 d\xi \\ &\leq \|\Psi\|_{L^\infty}^2 \int_{(-1/2, 1/2]} |\widehat{f}(\xi)|^2 d\xi,\end{aligned}$$

since at most one summand $\Psi(\delta^{-1}(\xi - \xi_j))$ is non-zero for each ξ , in view of the δ -separation of the set $\{\xi_j\}$. By applying Parseval–Plancherel again, we see the rightmost side is $\|\Psi\|_{L^\infty}^2 \|f\|_{\ell^2(\mathbb{Z})}^2$, verifying the case $p = 2$.

To establish the case $p = \infty$, we use the following general observation, an application of duality. Let $\{F_j\}$ be a set of functions on \mathbb{Z} . If we can prove that $\left\| \sum_j \alpha_j F_j \right\|_{\ell^\infty(\mathbb{Z})} \leq C$ for all sequences of complex numbers α_j with $\sum_j |\alpha_j|^2 = 1$, then it follows that

$$\left\| \left(\sum_j |F_j|^2 \right)^{1/2} \right\|_{\ell^\infty(\mathbb{Z})} \leq C,$$

with the same constant C . To see this, fix $x \in \mathbb{Z}$. By assumption, the sequence of values $\{F_j(x)\}_j$ satisfies $\left| \sum_j \alpha_j F_j(x) \right| \leq C$ for all sequences $\{\alpha_j\} \in \ell^2(j \in \mathbb{Z})$ with ℓ^2 norm 1. By duality, the sequence $\{F_j(x)\}_j$ thus lies in $\ell^2(j \in \mathbb{Z})$, with $\left(\sum_j |F_j|^2(x) \right)^{1/2} \leq C$. Since this holds uniformly for every x , the claim follows.

Thus in order to prove the ℓ^∞ case of Theorem 5.12, it suffices to prove that there is a constant C such that for every $f \in \ell^\infty$ with $\|f\|_\infty \leq 1$, for every sequence $\{a_j\}$ with $\sum_j |a_j|^2 = 1$,

$$\left| \sum_j a_j S_j(f)(n) \right| \leq C \tag{5.16}$$

for every $n \in \mathbb{Z}$. Recall that by S_j we denote the discrete operator with Fourier multiplier $\Psi_{\text{per}}(\delta^{-1}(\xi - \xi_j))$. Let K denote the convolution kernel of the operator $\sum_j a_j S_j$. Then by Young's inequality, (5.16) would follow from the estimate

$$\sum_{n \in \mathbb{Z}} |K(n)| \leq C. \quad (5.17)$$

Let K_0 denote the convolution kernel of the discrete operator with multiplier $\Psi_{\text{per}}(\delta^{-1}\xi)$, so that

$$K(n) = \left(\sum_j a_j e^{2\pi i \xi_j n} \right) K_0(n).$$

Precisely

$$K_0(n) = \int_{(-1/2, 1/2]} \Psi(\delta^{-1}\xi) e^{2\pi i \xi n} d\xi,$$

and consequently $|K_0(n)| \leq c\delta(1+|\delta n|)^{-2}$. Indeed, due to the support of Ψ we have $|K_0(n)| \leq \delta \|\Psi\|_{L^\infty}$ for all n . On the other hand, integrating twice by parts provides the bound $c\delta|\delta n|^{-2}$.

In combination with this bound for $K_0(n)$ we require a lemma about exponential sums.

Lemma 5.13 *Given a sequence $\{a_j\}$ of complex numbers and a set $\{\xi_j\}$ of real numbers in $(-1/2, 1/2]$, define for every $n \in \mathbb{Z}$,*

$$\mathbf{S}(n) = \sum_j a_j e^{2\pi i \xi_j n}. \quad (5.18)$$

Fix $0 < \delta < 1$. If $\{\xi_j\}$ is a δ -separated set, then for any interval J of length $1/\delta$, we have

$$\sum_{n \in J} |\mathbf{S}(n)|^2 \leq \frac{c}{\delta} \sum_j |a_j|^2 \quad (5.19)$$

for a constant c that is independent of δ , the sequences $\{a_j\}$ and $\{\xi_j\}$, and of the interval J .

Remark 5.14 Let a positive integer N be given. If we take $\xi_j = j/N$ for $j = 1, \dots, N$, then $\{\xi_j\}$ is a δ -separated set in $(-1/2, 1/2]$ (identified with the torus) with $\delta = 1/N$. In this case (5.19) becomes the identity

$$\sum_{j=1}^N |\mathbf{S}(n)|^2 = N \sum_{j=1}^N |a_j|^2,$$

which is the Parseval–Plancherel identity for the group $\mathbb{Z}/N\mathbb{Z}$.

Proof of Lemma 5.13 We will prove (5.19) by inserting a smooth weight. We fix an auxiliary function ϕ , such that $\phi(x) \geq 0$ for all $x \in \mathbb{R}$, $\phi(x) \geq 1$ for $|x| \leq c_1$ for some $c_1 > 0$, and $\phi(x) = \widehat{\Phi}(x)$, where Φ is C^∞ and is supported in $(-1/2, 1/2]$. (To construct ϕ , let $\Phi_1 \in C^\infty$ be supported in $|x| < 1/4$ with $\int \Phi_1(x)dx > 1$. Then let $\Phi_1^*(x) = \widehat{\Phi_1}(-x)$ and define $\Phi = \Phi_1 * (\Phi_1^*)$, so that $\phi = |\widehat{\Phi_1}|^2$. In particular, $\phi(0) = |\widehat{\Phi_1}(0)|^2 > 1$, so that this inequality also holds in a small neighborhood of the origin.) With this definition, we claim

$$\sum_{n \in \mathbb{Z}} e^{2\pi i n u} \phi(n\delta) = \delta^{-1} \Phi(\delta^{-1} u). \quad (5.20)$$

Indeed, the property $\phi = \widehat{\Phi}$ yields that for any $u \in \mathbb{T}$,

$$\begin{aligned} \sum_{n \in \mathbb{Z}} e^{2\pi i n u} \phi(n\delta) &= \sum_{n \in \mathbb{Z}} e^{2\pi i n u} \int_{\mathbb{R}} \Phi(x) e^{-2\pi i n x \delta} dx \\ &= \sum_{n \in \mathbb{Z}} e^{2\pi i n u} \int_{\mathbb{R}} \delta^{-1} \Phi(\delta^{-1} x) e^{-2\pi i n x} dx. \end{aligned}$$

However, for $\delta \leq 1$, then $\Phi(\delta^{-1} x)$ is supported in $(-1/2, 1/2]$, and the last sum is the Fourier series expansion of the function $\delta^{-1} \Phi(\delta^{-1} \cdot)$ in the interval $(-1/2, 1/2]$, and so by the Fourier inversion formula the quantities on each side of the identity are equal to $\delta^{-1} \Phi(\delta^{-1} u)$, as claimed.

We turn to the proof of (5.19). It suffices to consider the case in which the interval J is taken to be $\{n : |n| \leq c_1/\delta\}$ with c_1 as above. Indeed, once we have proved the result for such an interval J , it automatically holds for every translate $J + h$, because the coefficients a_j are then simply replaced by $a_j e^{2\pi i \xi_j h}$, which have the same ℓ^2 norm. Moreover any interval of length $1/\delta$ is covered by at most a bounded number of such translates (depending only on c_1).

Having reduced to this case, we observe that

$$\sum_{|n| \leq c_1/\delta} |\mathbf{S}(n)|^2 \leq \sum_{n \in \mathbb{Z}} |\mathbf{S}(n)|^2 \phi(n\delta). \quad (5.21)$$

On the other hand, squaring gives

$$|\mathbf{S}(n)|^2 = \sum_{j, j'} a_j \overline{a_{j'}} e^{2\pi i (\xi_j - \xi_{j'}) n}.$$

We insert this in (5.21) and then apply (5.20) with $u = \xi_j - \xi_{j'}$, to conclude that

$$\sum_{|n| \leq c_1/\delta} |\mathbf{S}(n)|^2 \leq \delta^{-1} \sum_{j, j'} a_j \overline{a_{j'}} \Phi(\delta^{-1} (\xi_j - \xi_{j'})) = c \delta^{-1} \sum_j |a_j|^2 \quad (5.22)$$

with $c = \Phi(0)$, since $\Phi(\delta^{-1}(\xi_j - \xi_{j'})) = 0$ for all $j \neq j'$, by the assumed δ -separation of the set $\{\xi_j\}$. The lemma is proved. \square

We apply Lemma 5.13 to prove the upper bound (5.17) for $\|K\|_{\ell^1}$. Recall that we are given a sequence $\{a_j\}$ with $\sum_j |a_j|^2 = 1$, and we define K as before to be the kernel of the operator $\sum_j a_j S_j$, so that $K(n) = \mathbf{S}(n) K_0(n)$. By the upper bound for $K_0(n)$, $|K(n)| \leq c|\mathbf{S}(n)|\delta(1+|\delta n|)^{-2}$, and we will apply Lemma 5.13 to bound $\mathbf{S}(n)$. We break the summation in (5.17) over \mathbb{Z} into intervals of length $1/\delta$, according to a disjoint union $\mathbb{Z} = \bigcup_{k \in \mathbb{Z}} I_k$ with

$$I_k = \left\{ n : \frac{k-1/2}{\delta} < n \leq \frac{k+1/2}{\delta} \right\}.$$

Applying Cauchy–Schwarz to each sum over $n \in I_k$, the left-hand side of (5.17) is majorized by

$$c \sum_{k \in \mathbb{Z}} A_k B_k,$$

where

$$A_k = \left(\sum_{n \in I_k} |\mathbf{S}(n)|^2 \right)^{1/2}, \quad B_k = \delta \left(\sum_{n \in I_k} (1 + |\delta n|)^{-4} \right)^{1/2}. \quad (5.23)$$

However, $A_k \leq c\delta^{-1/2}$ by Lemma 5.13, while $B_k \leq c\delta^{1/2}$ if $k = 0$ and $B_k \leq c\delta^{1/2}|k|^{-2}$ if $k \neq 0$. As a result the sum is majorized by $c \left(1 + \sum_{k \neq 0} |k|^{-2} \right) \leq c'$ and (5.17) is proved. This concludes the proof of Theorem 5.12 in the case $p = \infty$. Consequently we have also completed the proof of the first converse inequality in Theorem 5.3.

5.8 The Second Converse Inequality

The final step is to prove the second converse inequality in Proposition 5.6, an ℓ^{2r} bound for the operator

$$f \mapsto \left(\sum_{q \in Z} \left| \sum_{a/q \in \mathcal{R}(q)} f_{a/q} \right|^{2r} \right)^{1/2r}.$$

This will require not just separation properties of elements in $\mathcal{R}(Z)$, but more intricate arithmetic information as well. In particular, we recall the notation

$$\mathcal{Q}(Z) = \max\{\omega(q) : q \in Z\},$$

in which $\omega(q)$ is the number of distinct prime divisors of an integer q . We state a general theorem that implies the second converse inequality of Proposition 5.6.

Theorem 5.15 *Let an integer $r \geq 1$ be fixed. Let Z be a finite set of integers contained in $(1, q(Z)]$ and fix $\delta < q(Z)^{-2}$. Let m be an $L^{2r}(\mathbb{R})$ multiplier of norm A_{2r} and assume furthermore that $m(\xi)$ is supported in $|\xi| \leq c_0\delta$ for a constant $c_0 < 1/2$. Given a point $u \in (-1/2, 1/2]$, let T_u be the operator with multiplier $m(\xi - u)$. Then the corresponding discrete operators T_u have the property that for all $f \in \ell^{2r}(\mathbb{Z})$,*

$$\left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} T_u f \right|^{2r} \right)^{\frac{1}{2r}} \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_{2r} (2^{\Omega(Z)})^{1-1/r} \|f\|_{\ell^{2r}(\mathbb{Z})},$$

in which C_{2r} is a constant depending only on c_0 and A_{2r} .

Proposition 5.6 immediately follows, as long as ε is sufficiently small that $m(\varepsilon^{-1}(\cdot))$ satisfies the hypotheses of the theorem; $\varepsilon < q(Z)^{-2}$ suffices.

Theorem 5.15 is a consequence of the “method of sampling,” as developed in seminal work of [46, §2] on the discrete spherical maximal function. Let us recall the main consequence of this principle. In the notation introduced at the beginning of the section, the method of sampling shows how the norm of the real-variable operator T with L^p multiplier m controls the norm of the corresponding discrete operator T_{dis} , as long m is supported in $(-1/2, 1/2]$. The variant we state here is an arithmetic consequence of this general result when the multiplier is shifted by b/Q for all $1 \leq b \leq Q$, valid in the case that the multiplier has an even smaller support in $(-1/(2Q), 1/(2Q)]$.

Theorem 5.16 (The method of sampling) *Let $1 \leq p \leq \infty$ be fixed. Let μ be an $L^p(\mathbb{R})$ multiplier of norm M_p that is compactly supported in $(-1/2, 1/2]$. Fix an integer $Q \geq 1$ and $\varepsilon < Q^{-1}$. Then the discrete operator S with Fourier multiplier*

$$\sum_{b=1}^Q \mu_{\text{per}}(\varepsilon^{-1}(\xi - b/Q))$$

extends to a bounded operator on $\ell^p(\mathbb{Z})$, with $\|Sf\|_{\ell^p(\mathbb{Z})} \leq C_p \|f\|_{\ell^p(\mathbb{Z})}$, in which the constant C_p may depend on p and M_p but is independent of Q and ε .

A key accomplishment of this result is that the discrete operator norm is independent of both Q and ε . Giving a full proof would take us too far afield, so we refer to [46, Prop. 2.1 and Cor. 2.1].

Note that Theorem 5.16 considers *all* fractions of denominator Q when defining the multiplier, but in our application we consider only the *irreducible* fractions $\mathcal{R}(Q)$. As a first observation, we deduce a corollary for multipliers defined with only irreducible fractions, albeit with a norm that depends on Q .

Corollary 5.17 Let $1 \leq p \leq \infty$ be fixed. Let μ be an $L^p(\mathbb{R})$ multiplier of norm M_p that is compactly supported in $(-1/2, 1/2]$. Fix an integer $Q \geq 1$ and $\varepsilon < Q^{-1}$. Then the discrete operator R with Fourier multiplier

$$\sum_{u \in \mathcal{R}(Q)} \mu_{\text{per}}(\varepsilon^{-1}(\xi - u))$$

extends to a bounded operator on $\ell^p(\mathbb{Z})$, with $\|Rf\|_{\ell^p(\mathbb{Z})} \leq C_p 2^{\omega(Q)} \|f\|_{\ell^p(\mathbb{Z})}$, in which the constant C_p is the constant in Theorem 5.16.

Let us see how to deduce this corollary from the theorem. It is convenient to define the counterpart to $\mathcal{R}(q)$, namely the “full” set of fractions

$$\mathcal{F}(q) = \{a/q : 1 \leq a \leq q\}.$$

The key to deducing the corollary is a simple identity.

Lemma 5.18 Let h be the periodization of a function compactly supported in $(-1/2, 1/2]$. Fix an integer q with prime factorization $q = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with distinct primes p_1, \dots, p_k . Then

$$\sum_{u \in \mathcal{R}(q)} h(u) = \sum_{\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}} (-1)^{|\underline{\varepsilon}|} \sum_{w \in \mathcal{F}(p_1^{\alpha_1 - \varepsilon_1} \cdots p_k^{\alpha_k - \varepsilon_k})} h(w), \quad (5.24)$$

where for each $\underline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_k) \in \{0, 1\}^k$ we have defined $|\underline{\varepsilon}| = \sum_j \varepsilon_j$.

Notice that for a given integer Q , there are $2^{\omega(Q)}$ choices for the tuple $\underline{\varepsilon}$. Thus we can apply this identity to write the multiplier in the corollary as a signed sum of $2^{\omega(Q)}$ multipliers, each of which is of the form considered in the theorem. Since the operator norm in the theorem is independent of Q , applying the theorem to each of the $2^{\omega(Q)}$ terms then proves the corollary.

Proof of Lemma 5.18 When $q = p^\alpha$ is a prime power, (5.24) is the claim that

$$\sum_{u \in \mathcal{R}(q)} h(u) = \sum_{w \in \mathcal{F}(p^\alpha)} h(w) - \sum_{w \in \mathcal{F}(p^{\alpha-1})} h(w).$$

This holds since $\mathcal{F}(p^\alpha) = \mathcal{R}(p^\alpha) \sqcup \mathcal{F}(p^{\alpha-1})$ as a disjoint union, namely

$$\{1 \leq a \leq p^\alpha\} = \{1 \leq a \leq p^\alpha : (a, p^\alpha) = 1\} \sqcup \{pa' : 1 \leq a' \leq p^{\alpha-1}\}.$$

More generally, we will apply the facts that if q_1 and q_2 are relatively prime, then

$$\mathcal{F}(q_1 q_2) = \mathcal{F}(q_1) + \mathcal{F}(q_2), \quad \mathcal{R}(q_1 q_2) = \mathcal{R}(q_1) + \mathcal{R}(q_2).$$

These are consequences of the Chinese Remainder Theorem. Here we regard elements in the sets $\mathcal{F}(\cdot)$ and $\mathcal{R}(\cdot)$ modulo 1 (as we may in our application), and we use the notation that given sets \mathcal{S}_1 and \mathcal{S}_2 , $\mathcal{S}_1 + \mathcal{S}_2 = \{s_1 + s_2 : s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2\}$.

Thus if $q = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with distinct primes p_i , it follows that

$$\mathcal{R}(q) = \mathcal{R}(p_1^{\alpha_1} \cdots q_k^{\alpha_k}) = \mathcal{R}(p_1^{\alpha_1}) + \cdots + \mathcal{R}(p_k^{\alpha_k}),$$

so that

$$\sum_{u \in \mathcal{R}(q)} h(u) = \sum_{u_1 \in \mathcal{R}(p_1^{\alpha_1})} \cdots \sum_{u_k \in \mathcal{R}(p_k^{\alpha_k})} h(u_1 + \cdots + u_k).$$

Now we apply the prime power case to each sum over $\mathcal{R}(p_j^{\alpha_j})$, so that the right-hand side becomes

$$\sum_{\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}} (-1)^{|\varepsilon|} \sum_{\gamma_1 \in \mathcal{F}(p_1^{\alpha_1 - \varepsilon_1})} \cdots \sum_{\gamma_k \in \mathcal{F}(p_k^{\alpha_k - \varepsilon_k})} h(\gamma_1 + \cdots + \gamma_k).$$

Finally noting that $\mathcal{F}(p_1^{\alpha_1 - \varepsilon_1}) + \cdots + \mathcal{F}(p_k^{\alpha_k - \varepsilon_k}) = \mathcal{F}(p_1^{\alpha_1 - \varepsilon_1} \cdots p_k^{\alpha_k - \varepsilon_k})$, we recognize the right-hand side of (5.24), and the identity is proved. \square

While this corollary is useful, it does not immediately suffice to prove Theorem 5.15. Fix $r \geq 1$ and let T_u be the discrete operator associated to the multiplier $m(\xi - u)$, where we recall that $m(\xi)$ is supported in $|\xi| \leq c_0\delta$, with $c_0 < 1/2$, $\delta \leq q(Z)^{-2}$. Examine the norm

$$\left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} T_u f \right|^{2r} \right)^{\frac{1}{2r}} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} = \sum_{q \in Z} \left\| \sum_{u \in \mathcal{R}(q)} T_u f \right\|_{\ell^{2r}(\mathbb{Z})}^{2r}. \quad (5.25)$$

The operator $\sum_{u \in \mathcal{R}(q)} T_u$ has Fourier multiplier

$$\sum_{u \in \mathcal{R}(q)} m_{\text{per}}(\xi - u).$$

For each fixed $q \in Z$, δ is sufficiently small that we can apply Corollary 5.17 to conclude that

$$\left\| \sum_{u \in \mathcal{R}(q)} T_u f \right\|_{\ell^{2r}(\mathbb{Z})} \leq C_{2r} 2^{\omega(q)} \|f\|_{\ell^{2r}(\mathbb{Z})}$$

with C_{2r} depending on the norm A_{2r} but independent of q and δ . But this does not suffice to prove Theorem 5.15, since a trivial summation over $q \in Z$ would lead to

an unacceptably large operator norm of size $|Z|C_{2r}2^{\Omega(Z)}$. Instead, we will prove a version of Theorem 5.15 for a smooth multiplier, and then pass from the L^p multiplier to the smooth multiplier via an arithmetic factorization identity. We state the theorem for the smooth multiplier:

Theorem 5.19 *Suppose Ψ is a C^∞ function that is compactly supported in $(-1/2, 1/2]$, and fix $0 < \delta < 1$. Given a point $u \in (-1/2, 1/2]$ let S_u be the operator with multiplier $\Psi(\delta^{-1}(\xi - u))$.*

Let Z be a finite set of integers contained in $(1, q(Z)]$ and suppose the set $\bigcup_{q \in Z} \mathcal{R}(q)$ is a disjoint union and is δ -separated. Then if $\delta < q(Z)^{-2}$ the corresponding discrete operators S_u have the property that for every $2 \leq p \leq \infty$,

$$\left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} S_u f \right|^p \right)^{\frac{1}{p}} \right\|_{\ell^p(\mathbb{Z})} \leq C_p (2^{\Omega(Z)})^{1-2/p} \|f\|_{\ell^p(\mathbb{Z})},$$

in which C_p is a constant depending only on p and Ψ .

To deduce Theorem 5.15 from this, we require the following lemma.

Lemma 5.20 *Fix an integer $q > 1$ and $\delta \leq q^{-2}$. If $\mu(\xi)$ and $\phi(\xi)$ are functions compactly supported in $|\xi| \leq \delta/2$, then*

$$\sum_{u \in \mathcal{R}(q)} \mu(\xi - u) \phi(\xi - u) = \left(\sum_{w \in \mathcal{F}(q)} \mu(\xi - w) \right) \cdot \left(\sum_{u \in \mathcal{R}(q)} \phi(\xi - u) \right), \quad (5.26)$$

regarding the elements in $\mathcal{F}(q)$ and $\mathcal{R}(q)$ modulo 1. Correspondingly, this holds for the periodizations μ_{per} and ϕ_{per} as well.

Proof It is convenient to define $\mathcal{D}(q)$ to be the set of reducible fractions with denominator q ,

$$\mathcal{D}(q) = \{a/q : 1 \leq a \leq q, (a, q) > 1\}.$$

Then $\mathcal{F}(q) = \mathcal{R}(q) \sqcup \mathcal{D}(q)$ as a disjoint union. Suppose we can verify two facts: first,

$$\sum_{u \in \mathcal{R}(q)} \mu(\xi - u) \phi(\xi - u) = \left(\sum_{u \in \mathcal{R}(q)} \mu(\xi - u) \right) \cdot \left(\sum_{u' \in \mathcal{R}(q)} \phi(\xi - u') \right), \quad (5.27)$$

and second,

$$\left(\sum_{v \in \mathcal{D}(q)} \mu(\xi - v) \right) \cdot \left(\sum_{u' \in \mathcal{R}(q)} \phi(\xi - u') \right) = 0. \quad (5.28)$$

Then we could add (5.28) to the right-hand side of (5.27) and use $\mathcal{F}(q) = \mathcal{R}(q) \sqcup \mathcal{D}(q)$ to conclude the lemma holds.

To verify (5.27) it suffices to show that the only nonvanishing terms on the right-hand side occur when $u = u'$; due to the support constraints of μ, ϕ it thus suffices to show that the set $\mathcal{R}(q)$ is δ -separated. This of course holds as long as $\delta < 1/q$.

To verify (5.28), first observe that by identifying each ratio a/q in $\mathcal{D}(q)$ (as a point on the real line) with its associated reduced ratio, each element of $\mathcal{D}(q)$ lies in some set $\mathcal{R}(q')$ with $q' < q$. It then suffices to prove that as long as $\delta < q^{-2}$, any collection of intervals of length δ centered at points in $\bigcup_{1 \leq q' < q} \mathcal{R}(q')$ is disjoint from any collection of intervals of length δ centered at points in $\mathcal{R}(q)$. Assume on the contrary that two such intervals intersect; then there would be a point ξ for which

$$|a/q - a'/q'| \leq |\xi - a/q| + |\xi - a'/q'| \leq \delta/2 + \delta/2,$$

with $(a, q) = 1$ and $(a', q') = 1$, where $q' < q$. But then $aq' - a'q$ is a nonzero integer, and it would follow that

$$q^{-2} < (qq')^{-1} \leq |a/q - a'/q'| \leq \delta,$$

which is impossible, under the assumption that $\delta \leq q^{-2}$. Thus for any fixed ξ , for every pair $v \in \mathcal{D}(q)$, $u' \in \mathcal{R}(q)$ on the left-hand side of (5.28) the supports of $\mu(\xi - v)$ and $\phi(\xi - u')$ are disjoint, thus proving the identity. This proof holds for their periodization as well. \square

In the process of deducing Theorem 5.15 from Theorem 5.19, we apply Lemma 5.20 with $\mu = m$ the L^{2r} multiplier and $\phi = \Psi$ a smooth multiplier. This allows us to replace the sum of T_u over $u \in \mathcal{R}(q)$ in (5.25) by two operators, one summing T_u over $\mathcal{F}(q)$, which can be controlled by the method of sampling, and another summing a smooth multiplier operator over $\mathcal{R}(q)$, which we control using Theorem 5.19.

Precisely, fix $r \geq 1$. Recall that $\delta < Z(q)^{-2}$ is fixed and $m(\xi)$ is supported in $|\xi| \leq c_0\delta$, with $c_0 < 1/2$. Choose a smooth function Ψ supported in $(-1/2, 1/2]$ and such that $\Psi(\xi) = 1$ for $|\xi| \leq c_0$, so that $\Psi(\delta^{-1}\xi) = 1$ on the support of $m(\xi)$. Since $\delta < q(Z)^{-2}$, then for any $q \in Z$, by the choice of Ψ and Lemma 5.20,

$$\begin{aligned} \sum_{u \in \mathcal{R}(q)} m_{\text{per}}(\xi - u) &= \sum_{u \in \mathcal{R}(q)} m_{\text{per}}(\xi - u) \Psi_{\text{per}}(\delta^{-1}(\xi - u)) \\ &= \left(\sum_{w \in \mathcal{F}(q)} m_{\text{per}}(\xi - w) \right) \left(\sum_{u \in \mathcal{R}(q)} \Psi_{\text{per}}(\delta^{-1}(\xi - u)) \right). \end{aligned}$$

By the method of sampling (Theorem 5.16), the operator with Fourier multiplier corresponding to $\sum_{w \in \mathcal{F}(q)} m_{\text{per}}(\xi - w)$ is bounded on $\ell^{2r}(\mathbb{Z})$, with norm C_{2r} independent of q, δ . Let S_u denote the discrete operator with smooth Fourier multiplier

$\Psi_{\text{per}}(\delta^{-1}(\xi - u))$. Applying this in (5.25), we see that

$$\begin{aligned} & \left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} T_u f \right|^{2r} \right)^{\frac{1}{2r}} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} \\ & \leq C_{2r}^{2r} \sum_{q \in Z} \left\| \sum_{u \in \mathcal{R}(q)} S_u f \right\|_{\ell^{2r}(\mathbb{Z})}^{2r} = C_{2r}^{2r} \left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} S_u f \right|^{2r} \right)^{1/2r} \right\|_{\ell^{2r}(\mathbb{Z})}^{2r}. \end{aligned}$$

We then apply Theorem 5.19 to bound this by $C'_r \|f\|_{\ell^{2r}}^{2r}$, and we have verified Theorem 5.15.

5.8.1 Proof of Theorem 5.19

The final remaining step is to prove Theorem 5.19. We introduce the notation that for a function $g(x, q)$ of $x \in \mathbb{Z}$ and $q \in Z$, for $1 \leq p < \infty$,

$$\|g(x, q)\|_{\ell^p(\mathbb{Z} \times Z)} = \left(\sum_{x \in \mathbb{Z}} \sum_{q \in Z} |g(x, q)|^p \right)^{1/p}, \quad (5.29)$$

and for $p = \infty$,

$$\|g(x, q)\|_{\ell^\infty(\mathbb{Z} \times Z)} = \sup_{(x, q) \in \mathbb{Z} \times Z} |g(x, q)|.$$

Then the theorem claims that for each $2 \leq p \leq \infty$,

$$\left\| \sum_{u \in \mathcal{R}(q)} S_u f \right\|_{\ell^p(\mathbb{Z} \times Z)} \leq C_p (2^{\Omega(Z)})^{1-2/p} \|f\|_{\ell^p(\mathbb{Z})}. \quad (5.30)$$

It therefore suffices to prove a bound for $\ell^2(\mathbb{Z} \times Z)$ and for $\ell^\infty(\mathbb{Z} \times Z)$, and the intermediate cases follow by interpolation.

For the ℓ^2 bound, first rewrite

$$\left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} S_u f \right|^2 \right)^{\frac{1}{2}} \right\|_{\ell^2(\mathbb{Z})}^2 = \sum_{q \in Z} \left\| \sum_{u \in \mathcal{R}(q)} S_u f \right\|_{\ell^2(\mathbb{Z})}^2.$$

Applying the Parseval–Plancherel identity for each q shows that this is equal to

$$\begin{aligned} & \sum_{q \in Z} \left\| \sum_{u \in \mathcal{R}(q)} \Psi(\delta^{-1}(\xi - u)) \hat{f}(\xi) \right\|_{L^2(\mathbb{T})}^2 \\ &= \int_{(-1/2, 1/2]} |\hat{f}(\xi)|^2 \sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} \Psi(\delta^{-1}(\xi - u)) \right|^2 d\xi. \end{aligned}$$

Since $\delta < q(Z)^{-2}$, by Lemma 5.4, $\cup_q \mathcal{R}(q)$ is δ -separated (and is a disjoint union), so that for each fixed ξ at most one term is present as q, u vary. Thus we may conclude, after applying Plancherel again, that

$$\left\| \left(\sum_{q \in Z} \left| \sum_{u \in \mathcal{R}(q)} S_u \right|^2 \right)^{\frac{1}{2}} \right\|_{\ell^2(\mathbb{Z})}^2 \leq \|\Psi\|_{L^\infty(-1/2, 1/2]}^2 \|f\|_{\ell^2(\mathbb{Z})}^2.$$

(Here we used the δ -separation of the points, but no explicitly arithmetic properties.)

For the ℓ^∞ bound, it suffices to show that uniformly in $q \in Z$,

$$\left\| \sum_{u \in \mathcal{R}(q)} S_u f \right\|_{\ell^\infty(\mathbb{Z})} \leq C 2^{\mathcal{Q}(Z)} \|f\|_{\ell^\infty(\mathbb{Z})}, \quad (5.31)$$

for a constant C independent of q . Note that if q has prime factorization $q = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, by Lemma 5.18 the Fourier multiplier of this operator can be written as

$$\sum_{u \in \mathcal{R}(q)} \Psi_{\text{per}}(\delta^{-1}(\xi - u)) = \sum_{\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}} (-1)^{|\varepsilon|} \sum_{w \in \mathcal{F}(p_1^{\alpha_1 - \varepsilon_1} \cdots p_k^{\alpha_k - \varepsilon_k})} \Psi_{\text{per}}(\delta^{-1}(\xi - w)).$$

There are $2^{\omega(q)} \leq 2^{\mathcal{Q}(Z)}$ terms on the right-hand side. Thus to prove (5.31) it suffices to prove that each of the terms on the right-hand side corresponds to an operator with uniformly bounded norm. That is, it suffices to prove that for any integer $Q \geq 1$,

$$\left\| \sum_{u \in \mathcal{F}(Q)} S_u f \right\|_{\ell^\infty(\mathbb{Z})} \leq C \|f\|_{\ell^\infty(\mathbb{Z})}.$$

Let $K(n)$ denote the kernel of the operator $\sum_{u \in \mathcal{F}(Q)} S_u$, so that it suffices to show that

$$\sum_{n \in \mathbb{Z}} |K(n)| \leq C. \quad (5.32)$$

There is an analogy to the use of Lemma 5.13 to prove the ℓ^∞ case of Theorem 5.12, but now instead of using δ -separation of a collection of points $\{\xi_j\}$ we can use precise arithmetic information (compare to Remark 5.14). We compute that

$$\begin{aligned} K(n) &= \sum_{u \in \mathcal{F}(Q)} (\Psi_{\text{per}}(\delta^{-1}(\cdot - u)))^\vee(n) \\ &= \sum_{u \in \mathcal{F}(Q)} \int_{(-1/2, 1/2]} \Psi(\delta^{-1}(\xi - u)) e^{2\pi i n \xi} d\xi \\ &= \left(\sum_{u \in \mathcal{F}(Q)} e^{2\pi i n u} \right) \cdot \int_{\mathbb{R}} \Psi(\delta^{-1} \xi) e^{2\pi i n \xi} d\xi \\ &= Q \mathbf{1}_Q(n) \cdot \delta(\mathcal{F}^{-1} \Psi)(\delta n). \end{aligned}$$

We have applied first the support constraint of Ψ , followed by the fact that

$$\sum_{u \in \mathcal{F}(Q)} e^{2\pi i n u} = Q \mathbf{1}_Q(n) := \begin{cases} Q & \text{if } n \equiv 0 \pmod{Q}, \\ 0 & \text{otherwise.} \end{cases}$$

We see under the change of variables $n = Qm$ that

$$\sum_{n \in \mathbb{Z}} |K(n)| = \sum_{\substack{n \in \mathbb{Z} \\ Q|n}} |K(n)| = \sum_{m \in \mathbb{Z}} Q \delta |(\mathcal{F}^{-1} \Psi)(\delta Qm)|.$$

The last sum is uniformly bounded, so that (5.32) is confirmed. Indeed, since Ψ is C^∞ , its Fourier inverse has rapid decay, so that $|(\mathcal{F}^{-1} \Psi)(x)| \leq c(1 + |x|)^{-M}$ for any $M \geq 1$ of our choice. Breaking the sum into a contribution from small m and from large m , we see that each portion is bounded:

$$Q \delta \sum_{|m| \leq (\delta Q)^{-1}} |(\mathcal{F}^{-1} \Psi)(\delta Qm)| \leq Q \delta \sum_{|m| \leq (\delta Q)^{-1}} O(1) = O(1),$$

and

$$Q \delta \sum_{|m| > (\delta Q)^{-1}} |(\mathcal{F}^{-1} \Psi)(\delta Qm)| \leq Q \delta \sum_{|m| > (\delta Q)^{-1}} O((\delta Q|m|)^{-M}) = O(1).$$

This completes the proof of Theorem 5.19, and hence also the proof of the second converse inequality in Theorem 5.15.

5.9 Further Remarks on the General Setting

This concludes our study of direct and converse inequalities for the discrete operator

$$f \mapsto \sum_{a/q \in \mathcal{R}(Z)} f_{a/q} \quad (5.33)$$

in the case that Z is a relatively prime set. Our main result Theorem 5.1 was stated in terms of ℓ^{2r} bounds, with a constraint on ε depending on r and the maximum size $q(Z)$ of an element in Z . In the more general setting of Ionescu and Wainger, a parameter $0 < \delta_0 < 1$ is specified, and the goal is to construct a set Z_N that is an enlargement of the set $\{1, \dots, N\}$ with elements at most of size $e^{N^{\delta_0}}$, such that the resulting operator (5.33) with $Z = Z_N$ is bounded on ℓ^p with norm at most $C_{p, \delta_0} (\log N)^{2/\delta_0}$, for each $1 < p < \infty$. By specifying that $\varepsilon < e^{-N^{2\delta_0}}$, the constraint $\varepsilon < r^{-1} q(Z_N)^{-1/2r}$ holds for all $r \geq 1$ (for N sufficiently large relative to r, δ_0), and an ℓ^{2r} bound may be obtained for the operator. Then by interpolation the result of the theorem holds for all $2 \leq p < \infty$; duality then shows the result also holds for $1 < p \leq 2$. Thus the focus of Theorem 5.1 on ℓ^{2r} bounds is not unduly restrictive.

One crucial aspect of the work of Ionescu and Wainger is that they can allow $\delta_0 > 0$ to be arbitrarily small. (The case $\delta_0 > 1$ can be treated relatively simply.) To handle cases in which δ_0 is close to 0, Ionescu and Wainger construct a set Z_N that is a product set $Z_1 \cdots Z_s$ of relatively prime sets Z_j , with the further property that all elements in Z_j are relatively prime to all elements in $Z_{j'}$ if $j \neq j'$, and with s on the order of $1/\delta_0$. The setting of Theorem 5.1 illustrates the special case $s = 1$. When $s > 1$, one proves a direct inequality using an induction based on computations similar to those we exhibited here. The final direct inequality playing the role of Proposition 5.2 then has 2^s terms that are various hybrids of the two types of terms we exhibited here. To prove the converse inequalities for the hybrid terms, one combines appropriately the methods of proof we illustrated here for the first and second converse inequalities, stated as Propositions 5.5 and 5.6.

A final crucial aspect of the work of Ionescu and Wainger is that simultaneously with the considerations above, they must ensure that the factor $2^{\mathcal{Q}(Z_N)}$ appearing in the analogue of Proposition 5.6 does not exceed the allowed norm $C_{p, \delta_0} (\log N)^{2/\delta_0}$. This is difficult, since Z_N must be an enlargement of the set $\{1, \dots, N\}$ and in particular can include integers with many distinct small prime divisors. Thus as a first step, Ionescu and Wainger separate out from $\mathcal{R}(\{1, \dots, N\})$ all fractions with denominators divisible by many small prime factors. These fractions are, roughly speaking, carried along inside the multiplier to which the above method is applied, until the method of sampling is finally applied to also treat these terms. This aspect of the work of Ionescu and Wainger is very interesting from an arithmetic point of view, but the special case we focused on was designed to remove such considerations, in order to illuminate more simply the role that superorthogonality plays.

6 A Return to Type I Superorthogonality: Diagonal Behavior

A refinement of Type I superorthogonality arises naturally in a question related to decoupling. This refinement is the condition that for every $2r$ -tuple $f_{n_1}, \dots, f_{n_{2r}}$ of (complex-valued) functions from a sequence $\{f_n\}$,

$$\int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} = 0 \quad (6.1)$$

as long as

Type I*: the tuple $(n_1, n_3, \dots, n_{2r-1})$ is not a permutation of the tuple $(n_2, n_4, \dots, n_{2r})$.

In particular, if a sequence $\{f_n\}$ is of Type I*, it is certainly of Type I. Under the Type I condition, a direct inequality holds for any sequence $\{f_n\}$, by the argument given in Sect. 2 (suitably modified for complex-valued f_n). But for Type I* this argument can be refined to show that for any integer $r \geq 1$,

$$\left\| \left(\sum_n |f_n|^2 \right)^{1/2} \right\|_{L^{2r}}^{2r} \leq \left\| \sum_n f_n \right\|_{L^{2r}}^{2r} \leq r! \left\| \left(\sum_n |f_n|^2 \right)^{1/2} \right\|_{L^{2r}}^{2r}. \quad (6.2)$$

Indeed, after expanding the middle term, (6.1) shows that the only nonvanishing terms can be written as

$$\int \left(\sum_n f_n \right)^r \left(\sum_{n'} \bar{f}_{n'} \right)^r = \sum_{(a_1, \dots, a_s)} C(a_1, \dots, a_s)^2 \int |f_{n_1}|^{2a_1} \cdots |f_{n_s}|^{2a_s},$$

in which the sum on the right-hand side is over all $s \leq r$, all pairwise distinct n_1, \dots, n_s in the (finite) index set, and all (a_1, \dots, a_s) with $a_1 + \cdots + a_s = r$. Here, as before, $C(a_1, \dots, a_s) = (a_1 + \cdots + a_s)! / (a_1! \cdots a_s!)$. On the other hand,

$$\int \left(\sum_n |f_n|^2 \right)^r = \sum_{(a_1, \dots, a_s)} C(a_1, \dots, a_s) \int |f_{n_1}|^{2a_1} \cdots |f_{n_s}|^{2a_s},$$

in which the sum varies over the same parameters as described above. The claim follows, since $\max_{(a_1, \dots, a_s)} C(a_1, \dots, a_s) \leq r!$ and $\min_{(a_1, \dots, a_s)} C(a_1, \dots, a_s) \geq 1$.

6.1 An Extension Operator Associated to a Nondegenerate Curve

In this section we demonstrate a family $\{f_n\}$ with Type I* superorthogonality that relates to both harmonic analysis and number theory. Let $\gamma : [0, 1] \rightarrow \mathbb{R}^n$ be a nondegenerate curve, that is,

$$\det(\gamma'(t), \gamma''(t), \dots, \gamma^{(n)}(t)) \neq 0 \quad \text{for every } t \in [0, 1].$$

The prototypical example is the moment curve, $\gamma(t) = (t, t^2, \dots, t^n)$. We may associate to the curve γ an extension operator that maps functions on an interval $I \subset [0, 1]$ to functions of \mathbb{R}^n , by

$$E_I f(x) = \int_I e^{2\pi i x \cdot \gamma(t)} f(t) dt.$$

Then $E_I f$ can be thought of as a function whose Fourier transform is supported as a distribution on a portion of the curve $\{\gamma(t) : t \in [0, 1]\}$.

Suppose that we dissect $[0, 1]$ into a set of disjoint intervals $\{I_n\}_n$. Then we can ask whether the sequence of functions $\{E_{I_n} f\}_n$ satisfies a direct inequality in L^p ; if it does, this also implies an $\ell^2 L^p$ decoupling inequality (in an appropriate range of p). This setting has been considered in recent work of Gressman, Guo, Roos, Yung and the author [30]. As explained there, to state the relevant direct inequality precisely (so that both sides may be finite), we must define the L^p norms with an appropriate weight. There are many choices for such a weight (with comparable outcomes in the setting of decoupling, see e.g. [5, Lemma 4.1]), and we will make a particularly convenient choice here.

Let ϕ be a non-negative Schwartz function on \mathbb{R}^n with the property that $\phi \geq 1$ on the unit ball centered at the origin, and $\widehat{\phi}$ is supported on the unit ball centered at the origin (see the proof of Lemma 5.13 for a construction). Define $\phi_R(x) = \phi(R^{-n}x)$, and define the weighted norm

$$\|f\|_{L^p(\phi_R)} = \left(\int_{\mathbb{R}^n} |f(x)|^p \phi_R(x) dx \right)^{1/p}.$$

We may think of this weighted norm as capturing the average behavior of f over at least a ball of radius R^n ; the weight $\phi_R(x)$ has the effect of “blurring” the support of the Fourier transform of $|f(x)|^p$ on the scale of an $O(R^{-n})$ neighborhood; see e.g. [53, §8.1.3].

The main result of Guo et al. [30] is the following direct inequality: there exists a constant $C(\gamma, n) \in (0, \infty)$ such that for each integer $1 \leq r \leq n$, for every $R \geq 1$, for every $f \in L^{2r}(\phi_R)$,

$$\|E_{[0,1]} f\|_{L^{2r}(\phi_R)} \leq C(\gamma, n) \left\| \left(\sum_{|I|=R^{-1}} |E_I f|^2 \right)^{1/2} \right\|_{L^{2r}(\phi_R)}. \quad (6.3)$$

Here the summation is over the intervals I in a dissection of $[0, 1]$ into subintervals of length R^{-1} .

For any fixed $r \geq 1$, such a direct inequality is stronger than the corresponding $\ell^2 L^{2r}$ decoupling inequality, which would replace the norm on the right-hand side by $\left(\sum_{|I|=R^{-1}} \|E_I f\|_{L^{2r}(\phi_R)}^2 \right)^{1/2}$ (see e.g. [53, §5.3.2] for a formal comparison). The celebrated work [6] shows that the $\ell^2 L^{2r}$ decoupling inequality is valid in the much

larger range of any real $r \leq n(n + 1)/2$. See further remarks below, on barriers to extending the current proof of the direct inequality to values $r > n$.

6.2 Type I* Superorthogonality for Extension Operators

An advantage of the direct inequality (6.3) for integers $r \leq n$ is its comparatively simple proof. Fundamentally, the argument is an application of Type I* superorthogonality: if the Type I* condition holds for functions $\{E_I f\}_I$ as I varies over a finite set \mathcal{I} , then (6.2) shows that

$$\left\| \sum_{I \in \mathcal{I}} E_I f \right\|_{L^{2r}(\phi_R)} \leq C_r \left\| \left(\sum_{I \in \mathcal{I}} |E_I f|^2 \right)^{1/2} \right\|_{L^{2r}(\phi_R)}. \quad (6.4)$$

From this inequality, certain reductions (reviewed momentarily) show that (6.3) holds.

In this weighted context, the Type I* criterion is the statement that for any tuple $(I_1, I_2, \dots, I_{2r})$ of intervals in the collection \mathcal{I} ,

$$\int_{\mathbb{R}^n} E_{I_1} f(x) \overline{E_{I_2} f}(x) \cdots E_{I_{2r-1}} f(x) \overline{E_{I_{2r}} f}(x) \phi_R(x) dx = 0 \quad (6.5)$$

unless $(I_1, I_3, \dots, I_{2r-1})$ is a permutation of $(I_2, I_4, \dots, I_{2r})$. Upon expanding the definition of the extension operators, the integral (6.5) is identical to the expression

$$\int_{I_{\text{odd}}} \int_{I_{\text{even}}} R^{n^2} \widehat{\phi} \left(R^n \sum_{i=1}^r (\gamma(t_i) - \gamma(s_i)) \right) \cdot f(t_1) \cdots f(t_r) \overline{f(s_1) \cdots f(s_r)} dt_1 \cdots dt_r ds_1 \cdots ds_r;$$

here we let $(t_1, \dots, t_r) \in I_{\text{odd}} := I_1 \times I_3 \times \cdots \times I_{2r-1}$, and analogously for $(s_1, \dots, s_r) \in I_{\text{even}} := I_2 \times I_4 \times \cdots \times I_{2r}$. This integral will vanish unless $R^n \sum_{i=1}^r (\gamma(t_i) - \gamma(s_i))$ lies in the support of $\widehat{\phi}(\xi)$, which requires that

$$\left| \sum_{i=1}^r (\gamma(t_i) - \gamma(s_i)) \right| \leq R^{-n}. \quad (6.6)$$

The central technical result of [30, Prop. 1.3] is that nondegeneracy of the curve γ guarantees that for each integer $1 \leq r \leq n$, as long as the intervals in $I \in \mathcal{I}$ are sufficiently well-spaced, (6.6) can only occur if $(I_1, I_3, \dots, I_{2r-1})$ is a permutation of $(I_2, I_4, \dots, I_{2r})$. This verifies that the Type I* condition holds as long as the intervals $I \in \mathcal{I}$ are sufficiently well-spaced.

For completeness, we recall a few details of this result, to confirm that it reduces the full proof of (6.3) to the case of (6.4). Precisely, the nondegeneracy of γ guarantees the existence of constants $\delta_0(\gamma, n) \leq 1$ and $c_0(\gamma, n) \geq 10$ (with $\delta_0^{-1}, c_0 \in \mathbb{Z}$) such

that for any collection \mathcal{I} of intervals from a dissection of $[0, 1]$ into pairwise disjoint intervals of length R^{-1} with the property that

$$\text{dist}(I, I') \geq c_0(\gamma, n)R^{-1} \quad \text{for } I \neq I' \in \mathcal{I}, \quad \text{and} \quad \text{diam} \left(\bigcup_{I \in \mathcal{I}} I \right) \leq \delta_0(\gamma, n), \quad (6.7)$$

then (6.6) can only hold if $(t_1, \dots, t_r) \in I_{n_1} \times \dots \times I_{n_r}$ and $(s_1, \dots, s_r) \in I'_{n_1} \times \dots \times I'_{n_r}$ where $(I_{n_1}, \dots, I_{n_r})$ is a permutation of $(I'_{n_1}, \dots, I'_{n_r})$. We conclude that for any collection \mathcal{I} of intervals satisfying (6.7), the integral (6.5) vanishes unless $(I_1, I_3, \dots, I_{2r-1})$ is a permutation of $(I_2, I_4, \dots, I_{2r})$. Thus to prove (6.3), one begins with a dissection of $[0, 1]$ into intervals of length R^{-1} , and then cuts this dissection into $\leq \delta_0^{-1}$ subcollections, each lying in a subinterval of length at most δ_0 . Then one cuts each such subcollection further, taking every $(c_0 + 1)$ th interval in the subcollection to make one of the desired collections \mathcal{I} to which we can apply (6.4). This verifies (6.3) with the constant $(c_0 + 1)\delta_0^{-1}$.

6.3 Further Remarks: Diagonal vs. Off-diagonal Solutions

What about direct inequalities like (6.3) in $L^{2r}(\phi_R)$ for a curve in \mathbb{R}^n , for $r > n$? The essential ingredient in the argument above is that for integers $r \leq n$ and a non-degenerate curve $\gamma : [0, 1] \rightarrow \mathbb{R}^n$, the $2r$ -iterated system of equations

$$\gamma(x_1) + \gamma(x_3) + \dots + \gamma(x_{2r-1}) = \gamma(x_2) + \gamma(x_4) + \dots + \gamma(x_{2r}) \quad (6.8)$$

has the property that its only solutions (or near solutions) are “essentially diagonal,” in the sense that $x_1, x_3, \dots, x_{2r-1}$ is a permutation of x_2, x_4, \dots, x_{2r} , or at least very nearly. This can fail to be true for $r > n$.

We can gain an intuition for this obstacle from the case of the moment curve $\gamma(t) = (t, t^2, \dots, t^n) \subset \mathbb{R}^n$ by studying integral solutions to the system of equations (6.8). This is the Vinogradov system of degree n in $2r$ variables,

$$x_1^d + x_3^d + \dots + x_{2r-1}^d = x_2^d + x_4^d + \dots + x_{2r}^d, \quad 1 \leq d \leq n.$$

Integral solutions with $1 \leq x_i \leq X$ correspond to X^{-1} -separated points on γ . The Vinogradov system is known to have only diagonal integral solutions as long as $r \leq n$; for all large n it is an open problem to determine the least $r > n$ for which an off-diagonal integral solution exists (the Prouhet–Tarry–Escott problem). For $1 \leq n \leq 9$ and $n = 11$, an off-diagonal integral solution has been exhibited for $r = n + 1$. Moreover it is known that for $r > n$, as soon as one off-diagonal integral solution with all $|x_i| \ll X$ exists, at least $\gg X^2$ off-diagonal integral solutions exist. Thus if a direct inequality in L^{2r} (if true) is to be obtained for some $r > n$, the method of proof must be able to accommodate a profusion of off-diagonal solutions. We refer to [30, §2] for details, and a summary of literature related to counts for off-diagonal integral solutions.

7 Quasi-superorthogonality and Trace Functions

We now introduce the notion of quasi-superorthogonality: we no longer assume that the integral of $f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}}$ vanishes, but that it exhibits cancellation relative to a trivial bound. This will lead us to central questions in number theory.

Let (M, μ) be a finite-measure space and denote $|M| = \mu(M) \geq 1$. Let $\{f_n\}$ be a sequence of uniformly bounded functions with finite index set \mathcal{I} ; for simplicity we assume that $\|f_n\|_{L^\infty} \leq 1$ for all n . We suppose that there is a real number $0 < \nu < 1$ such that for every $r \geq 1$, for every $2r$ -tuple of functions in $\{f_n\}$,

$$\left| \int_M f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} d\mu \right| \leq C_r |M|^\nu \quad (7.1)$$

as long as:

Type I quasi-superorthogonality: the tuple $(n_1, n_2, \dots, n_{2r})$ has the property that some value n_j appears an odd number of times.

Type II quasi-superorthogonality: the tuple $(n_1, n_2, \dots, n_{2r})$ has the property that some value n_j appears precisely once (the uniqueness property).

We no longer hope to prove a direct inequality, as such. Instead, we expand the norm

$$\begin{aligned} \left\| \sum_{n \in \mathcal{I}} f_n \right\|_{L^{2r}(M, \mu)}^{2r} &= \sum_{(n_1, \dots, n_{2r}) \in \mathcal{I}^{2r}}^* \int_M f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} d\mu \\ &\quad + \sum_{(n_1, \dots, n_{2r}) \in \mathcal{I}^{2r}}^{**} \int_M f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}} d\mu, \end{aligned}$$

in which the first sum is over those tuples with the uniqueness property and the second sum is over those tuples without the uniqueness property (so at most r distinct values appear in each such tuple). Suppose that $\{f_n\}$ has Type I or Type II quasi-superorthogonality with parameter ν . Then the first term may be bounded above by $C_r |\mathcal{I}|^{2r} |M|^\nu$ by (7.1), while the second term is controlled by a direct inequality, by the argument of Sect. 3.1. Thus

$$\left\| \sum_{n \in \mathcal{I}} f_n \right\|_{L^{2r}}^{2r} \leq C_r |\mathcal{I}|^{2r} |M|^\nu + C'_r \left\| \left(\sum_{n \in \mathcal{I}} |f_n|^2 \right)^{1/2} \right\|_{L^{2r}}^{2r} \ll_r |\mathcal{I}|^{2r} |M|^\nu + |\mathcal{I}|^r |M|. \quad (7.2)$$

This should be compared to the trivial upper bound $|\mathcal{I}|^{2r} |M|$. In particular, to minimize the right-hand side over the cardinality of \mathcal{I} , we would consider a set of indices \mathcal{I} with

$$|\mathcal{I}| = |M|^{\frac{1-v}{r}}. \quad (7.3)$$

If \mathcal{I} is of this size, then we obtain the bound

$$\left\| \sum_{n \in \mathcal{I}} f_n \right\|_{L^{2r}(M, \mu)} \ll_r |M|^{\frac{2-v}{2r}}.$$

This is better than the trivial bound $|\mathcal{I}| |M|^{1/2r}$ as long as $|\mathcal{I}|$ is at least an order of magnitude larger than $|M|^{\frac{1-v}{2r}}$, which certainly is true under our assumption on the size of \mathcal{I} .

We will now describe an important setting in which quasi-superorthogonality arises: trace functions, which are ubiquitous in number theory. In this section, we demonstrate that trace functions exhibit quasi-superorthogonality, due to a theory built up recently in great generality by Fouvry et al. [25] (see also [27]), building on ideas of N. Katz and using the truth of the Riemann Hypothesis over finite fields, due to Deligne. In Sect. 8 we then demonstrate that quasi-superorthogonality provides a clear way to motivate a proof of Burgess's celebrated bound for short multiplicative character sums.

7.1 Trace Functions

While harmonic analysis nucleated around the study of periodic functions on the unit circle, analytic number theory nucleated around properties of functions of period q , where q is a fixed integer (often prime). For example, such functions arise because of the ubiquity of the Fourier transform on the group $\mathbb{Z}/q\mathbb{Z}$, which introduces the functions $x \rightarrow e^{2\pi i ax/q}$ for $1 \leq a \leq q$. Functions of period q also arise in many other ways, for example in sieve methods, which (roughly speaking) test whether a property holds “globally” in \mathbb{Z} by testing whether it holds “locally” modulo q for many primes q . Functions of period q are also closely intertwined with the important role played by congruences $n \equiv a \pmod{q}$, for example in Dirichlet's theorem on the infinitude of primes in arithmetic progressions. This leads to other well-known examples of q -periodic functions such as the Legendre symbol $x \mapsto \left(\frac{x}{q}\right)$, or more generally any multiplicative Dirichlet character $x \mapsto \chi(x)$, a homomorphism of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^* \mapsto \mathbb{C}^*$ (if nontrivial, extended to act on $\mathbb{Z}/q\mathbb{Z}$ by setting $\chi(x) = 0$ if $(q, x) > 0$). One can also consider $x \mapsto e^{2\pi i x^{-1}/q}$ or $x \mapsto e^{2\pi i (x^{-1}+x)/q}$, in which x^{-1} denotes the multiplicative inverse of x modulo the prime q .

All the functions $x \mapsto F(x)$ mentioned above are examples of trace functions. A few more examples of trace functions include normalized Gauss and Kloosterman sums such as

$$x \mapsto \frac{1}{q^{1/2}} \sum_{x \in \mathbb{F}_q} e^{2\pi i ax^2/q}, \quad x \mapsto \frac{1}{q^{1/2}} \sum_{\substack{x, y \in \mathbb{F}_q^* \\ xy=a}} e^{2\pi i (x+y)/q},$$

or hyper-Kloosterman sums. Moreover, certain procedures applied to appropriate trace functions produce more trace functions, such as addition of trace functions, multiplication, “convolution” and taking the Fourier transform (due to Laumon, see [27, Thm. 6.6]).

The fully general definition of a trace function (associated to an appropriate ℓ -adic sheaf) would take us too far afield, and instead we ask the reader to keep the above examples in mind. For the full definition of trace functions, an extensive overview of technical results, and many far-reaching applications, we refer to the excellent “Lectures on applied ℓ -adic cohomology” of Fouvry et al. [27], which we will cite as we illustrate the connection to superorthogonality. (See in particular [27, Dfn. 3.5] for a general definition.)

7.2 Complete Sums

One of the most useful properties of trace functions is a “square-root cancellation” upper bound for the sum of a trace function $F(x)$ over all elements in \mathbb{F}_q for a prime q . We state this as: if F is a trace function associated to an appropriate ℓ -adic sheaf (precisely, weight 0 and geometrically irreducible or isotypic with no trivial component) then

$$\sum_{x \in \mathbb{F}_q} F(x) \ll C_F q^{1/2}, \quad (7.4)$$

where C_F is the conductor of F . This is a consequence of the Grothendieck–Lefschetz trace formula [27, Thm. 4.1] and Deligne’s resolution of the Weil Conjectures [21], verifying the Generalized Riemann Hypothesis over finite fields [27, Thm. 4.6]. This may be compared to the “trivial” $O(q)$ upper bound that holds because the values of a (weight 0) trace function $F(x)$ associated to \mathbb{F}_q are uniformly bounded (by the rank of the trace function). (In [27], see Definition 3.1 for the rank, Definition 3.10 for the uniform upper bound for $F(x)$, Definition 4.3 for the conductor, Corollary 4.7 for the statement of square-root cancellation as in (7.4), and §3.4 for the notions of geometrically irreducible and isotypic. Remark 3.11 indicates why the weight 0 case is sufficiently general.)

It is hard to overstate the importance of trace functions as tools in analytic number theory. The Weil–Deligne bound (7.4) is of critical importance in many proof techniques. But another type of sum is also often unavoidable in analytic methods in number theory: an incomplete sum of the form

$$\sum_{x \in \mathcal{I}} F(x)$$

where \mathcal{I} is a proper subset of \mathbb{F}_q . When \mathcal{I} is an interval, identified with $[a, b] \subsetneq [1, q]$, such incomplete sums can be further divided into two types: “long sums” in which $|\mathcal{I}| \gg q^{1/2}$ and the more difficult “short sums” in which $|\mathcal{I}| \ll q^{1/2}$. Our goal in the remainder of the paper is to show that quasi-superorthogonality of trace functions is a

natural language in which to frame the current best method for bounding short sums, the Burgess method. First we must explain why quasi-superorthogonality holds.

7.3 Quasi-superorthogonality of Trace Functions

Let q be a prime. Let an element $\gamma \in \mathrm{PGL}_2(\mathbb{F}_q)$ act on $x \in \mathbb{F}_q$ by fractional linear transformation, denoted by $x \mapsto \gamma \cdot x$. Consider for a trace function F associated to q the sum

$$\sum_{x \in \mathbb{F}_q} F(\gamma_1 \cdot x) \overline{F}(\gamma_2 \cdot x) \cdots F(\gamma_{2r-1} \cdot x) \overline{F}(\gamma_{2r} \cdot x) e^{2\pi i x h / q} \quad (7.5)$$

where $\gamma_1, \dots, \gamma_{2r} \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $h \in \mathbb{F}_q$. If all the γ_i occur in pairs, we might not expect cancellation to occur in the sum. For example, suppose that $h = 0$ and $F(x) = \chi(x)$ is a non-principal Dirichlet character modulo q ; then if $\gamma_{2i-1} = \gamma_{2i}$ for each $i = 1, \dots, r$, the sum would evaluate to q . But otherwise, we might hope that significant cancellation occurs. Recently a broad set of results of this type has been codified by Fouvry et al. [25]. We expose here that their results precisely fit the notion of quasi-superorthogonality for the sequence of functions $\{F(\gamma_n \cdot)\}_n$.

The key result is as follows: appropriate trace functions F associated to q have the property that the sequence $\{F(\gamma_n \cdot)\}_n$ with $\gamma_n \in \mathrm{PGL}_2(\mathbb{F}_q)$ satisfies Type I quasi-superorthogonality with parameter $\nu = 1/2$. Thus the approximate direct inequality (7.2) holds with $M = \mathbb{F}_q$ and $|M| = q$.

We can state this precisely in terms of a weighted Type I quasi-superorthogonality condition: for all $h \in \mathbb{F}_q$,

$$\left| \sum_{x \in \mathbb{F}_q} F(\gamma_1 \cdot x) \overline{F}(\gamma_2 \cdot x) \cdots F(\gamma_{2r-1} \cdot x) \overline{F}(\gamma_{2r} \cdot x) e^{2\pi i x h / q} \right| \ll_{r, C_F} q^{1/2}, \quad (7.6)$$

as long as at least one fractional linear transformation γ_i appears an odd number of times in the tuple $(\gamma_1, \gamma_2, \dots, \gamma_{2r})$. This holds for F being a Dirichlet character, as well as normalized Gauss sums and Kloosterman sums, and other familiar trace functions. The precise details for the general setting can be found in [25] and [27, §14], in which the left-hand side of (7.6) is called a multicorrelation sum. More general forms of the relation (7.6) also hold, in which the trace function F can itself vary from factor to factor, as explained in [25, 27]. The condition that the tuple $(\gamma_1, \gamma_2, \dots, \gamma_{2r})$ has an entry that occurs an odd number of times was called an “ad hoc” definition in [27, Dfn. 14.2]; it is very pleasing that we now see it is precisely the Type I condition.

The result (7.6) is very deep; we will return momentarily to the underlying reasons it holds. First, we highlight an important special case, known since the 1940s, which will play a critical role in the next section on the Burgess method.

7.4 The Case of Dirichlet Characters

Let us specify that $F = \chi$ is a multiplicative Dirichlet character of order Δ modulo a prime q , $h = 0$, and each $\gamma_i \cdot x = x + n_i$ for some $n_i \in \mathbb{F}_q$. Then (7.5) takes the form

$$\sum_{x \in \mathbb{F}_q} \chi((x + n_1)(x + n_2)^{\Delta-1} \cdots (x + n_{2r-1})(x + n_{2r})^{\Delta-1}) = \sum_{x \in \mathbb{F}_q} \chi(f_{\underline{n}}(x)), \quad (7.7)$$

say. This sum is trivially bounded above by q . In this special case, the square-root cancellation bound (7.6) was known already to Weil, as a consequence of Weil's proof of the Riemann hypothesis for curves [67]; for a more recent source, see e.g. [39, Thm. 11.23, Cor. 11.24]. We record the Weil bound explicitly, and then show that it verifies Type II quasi-superorthogonality for the set of functions $\{\chi(\cdot + n)\}_n$.

Lemma 7.1 (Weil bound) *Let χ be a non-principal multiplicative Dirichlet character of order Δ modulo a prime q . Then for any polynomial $f \in \mathbb{Z}[t]$ that has m distinct roots and cannot be written as $f(t) = ch(t)^{\Delta}$ for some $h \in \overline{\mathbb{F}}_q[t]$,*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (m-1)q^{1/2}. \quad (7.8)$$

To verify Type II quasi-superorthogonality, let (n_1, \dots, n_{2r}) be a fixed tuple and define the polynomial $f_{\underline{n}}(x)$ as in (7.7). If $f_{\underline{n}}$ is a constant multiple of a Δ th power of a polynomial over $\overline{\mathbb{F}}_q$ then it also is over \mathbb{F}_q (see for example [55, Lemma 3.1]). If the tuple (n_1, \dots, n_{2r}) has the uniqueness property then some root of $f_{\underline{n}}$ either appears only once or only $\Delta - 1$ times, and hence $f_{\underline{n}}$ cannot be a Δ th power over \mathbb{F}_q , so by the lemma we have

$$\left| \sum_{x \in \mathbb{F}_q} \chi(x + n_1)\overline{\chi}(x + n_2) \cdots \chi(x + n_{2r-1})\overline{\chi}(x + n_{2r}) \right| \leq (2r-1)q^{1/2}. \quad (7.9)$$

This verifies that the sequence of functions $\{\chi(\cdot + n)\}_n$, where n varies over any finite set \mathcal{I} of integers, satisfies Type II quasi-superorthogonality with parameter $\nu = 1/2$, and the approximate direct inequality (7.2) holds. For later reference, we record this in the case that \mathcal{I} is the set of integers in an interval $(k_1, k_2]$:

$$\left\| \sum_{n \in (k_1, k_2]} \chi(\cdot + n) \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}^{2r} \ll_r (k_2 - k_1)^{2r} q^{1/2} + (k_2 - k_1)^r q. \quad (7.10)$$

7.5 The Source of Quasi-superorthogonality

The source of the quasi-superorthogonality exhibited in (7.6) is very interesting in its own right, and further exemplifies the universality of “exact” superorthogonality, in the meaning (1.1) considered earlier in this paper. To see this, let us consider in general the role of the Riemann Hypothesis over finite fields for studying a sum of the form

$$\sum_{x \in \mathbb{F}_q} F_1(x) \overline{F}_2(x) \cdots F_{2r-1}(x) \overline{F}_{2r}(x) e^{2\pi i h x / q}, \quad (7.11)$$

for appropriate trace functions F_1, \dots, F_{2r} . We will be informal here, and refer to the rigorous statements of [25, Proposition 1.1] for details. [Strictly speaking, one first restricts the sum over $x \in \mathbb{F}_q$ to a certain subset $U(\mathbb{F}_q) \subset \mathbb{F}_q$ upon which the F_i are suitably well-behaved (“unramified,” see Appendix B). In the cases of interest, the sum over $x \in U(\mathbb{F}_q)$ differs from the sum over $x \in \mathbb{F}_q$ by an error term that depends only on the trace functions F_i , and is independent of q and hence negligible for all sufficiently large q . We suppress this consideration here.]

The Grothendieck–Lefschetz trace formula expresses the sum (7.11) as a signed sum of three terms indexed by $i = 0, 1, 2$. For each i , the i th term is the trace of an endomorphism (associated to a Frobenius conjugacy class) of the i th cohomology group of a sheaf associated to the product $F_1(\cdot) \cdots \overline{F}_{2r}(\cdot) e^{2\pi i h(\cdot) / q}$ (see e.g. [27, Thm. 4.1]). Thus in order to bound the sum (7.11), one needs to bound each of these three terms from above. In fact, the contribution from the 0th cohomology group vanishes because of the product structure of $F_1(\cdot) \cdots \overline{F}_{2r}(\cdot) e^{2\pi i h(\cdot) / q}$. This leaves the first and second cohomology groups.

One way to bound a trace is to control the dimension of the representation and the maximal size of the associated eigenvalues. The dimension of the first cohomology group can be bounded above in terms of the conductors of F_1, \dots, F_{2r} . Deligne’s proof of the Riemann Hypothesis over finite fields [21] then provides the crucial information that all eigenvalues of the endomorphism (associated to a Frobenius conjugacy class) of the first cohomology group have absolute value $\leq q^{1/2}$. In the case of (7.6), this leads to the $O(q^{1/2})$ term on the right-hand side.

To summarize, the Riemann Hypothesis over finite fields shows that quasi-superorthogonality with parameter $\nu = 1/2$ holds for trace functions F_1, \dots, F_{2r} as long as the contribution of the second cohomology group vanishes. This vanishing always occurs in the case that $h \neq 0$; see [25, §4]. The case $h = 0$ is more subtle. Interestingly, this criterion on the second cohomology group for the case $h = 0$ is equivalent to “exact” superorthogonality of a different $2r$ -tuple of functions, in the original sense of an integral condition as in (1.1). Thus, the source of quasi-superorthogonality, of a certain type, for trace functions F_1, \dots, F_{2r} is exact superorthogonality, of that same type, for an associated tuple of functions.

We thank Emmanuel Kowalski for pointing this out. This phenomenon was already understood in the key results on trace functions in works such as [24, 25, 27, 45], but has typically been presented in quite different terms. (See however [45, Remark 4.2 and Prop. 4.4.] and [24, Prop. 3.2] for instances closest to the interpretation mentioned

here.) In order to make this phenomenon explicit in the literature, we include Appendix B by Emmanuel Kowalski.

7.6 Further Types for Which Quasi-superorthogonality Holds

Fouvry et al. [25] have also proved the square-root cancellation bound (7.6) under further conditions on the index tuple $(\gamma_1, \dots, \gamma_{2r})$ of $\mathrm{PGL}_2(\mathbb{F}_q)$ transformations. We briefly describe these conditions on the index tuple here, and compare them to the Type I* condition. The precise requirements on the trace function F under which the following types for $(\gamma_1, \dots, \gamma_{2r})$ suffice to verify quasi-superorthogonality can be found in [25, Thm. 1.5 and Cor. 1.6]; see also [27, §14.1].

Given an element γ , let $N(\gamma)$ denote the number of times γ appears in the r -tuple $(\gamma_1, \gamma_3, \dots, \gamma_{2r-1})$ and let $N'(\gamma)$ denote the number of times γ appears in the r -tuple $(\gamma_2, \gamma_4, \dots, \gamma_{2r})$. For appropriate trace functions F with weight 0 and rank k , (7.6) holds as long as at least one element γ appearing in $(\gamma_1, \dots, \gamma_{2r})$ has the property that $N(\gamma) \not\equiv N'(\gamma) \pmod{k}$.

This type can be interpreted as a weaker version of Type I* quasi-superorthogonality. For comparison, in the notation defined here, the condition for Type I* superorthogonality of a sequence of functions $\{f_n\}$ could be stated as follows: $\int f_{n_1} \bar{f}_{n_2} \cdots \bar{f}_{n_{2r}} = 0$ as long as there is at least one value n appearing in the $2r$ -tuple $(n_1, n_2, \dots, n_{2r})$ such that that $N(n) \neq N'(n)$.

Here is another variation on Type I* quasi-superorthogonality: a class of trace functions F with weight 0 and rank k also has an associated involution, a transformation $\varrho \in \mathrm{PGL}_2(\mathbb{F}_q)$ with $\varrho^2 = \mathrm{Id}$. Let $N(\gamma)$, $N'(\gamma)$ be defined as above, and now let $\tilde{N}(\gamma)$ denote the number of times $\varrho\gamma$ appears in the r -tuple $(n_1, n_3, \dots, n_{2r-1})$, and $\tilde{N}'(\gamma)$ denote the number of times $\varrho\gamma$ appears in the r -tuple $(n_2, n_4, \dots, n_{2r})$. For appropriate trace functions, (7.6) holds as long as at least one element γ appearing in $(\gamma_1, \dots, \gamma_{2r})$ has the property that $N(\gamma) - N'(\gamma) \not\equiv \tilde{N}(\gamma) - \tilde{N}'(\gamma) \pmod{k}$.

Examples of tuples satisfying each of these conditions can be found in [25, Example 1.4].

7.7 A First Look at Incomplete Sums: The Pólya–Vinogradov Method

We have exhibited the quasi-superorthogonality of trace functions. Now we turn to the task of bounding incomplete sums of trace functions, which play a central role in analytic number theory. We begin by recalling the classical method of Pólya and Vinogradov, which will indicate why there is a dichotomy between long and short incomplete sums. After we see that the Pólya–Vinogradov method suffices in the first case, we will focus our attention on the short case for the remainder of the paper.

We start with general considerations. Given a function $F : \mathbb{Z} \rightarrow \mathbb{C}$ of period q , what can we learn about the size of

$$\sum_{x \in \mathcal{I}} F(x)$$

as a function of q , relative to the length of the sub-interval $\mathcal{I} \subsetneq [1, q]$? We will focus on the case of q prime, later specifying properties of F as well. We first re-write the sum via Plancherel's identity on the group $\mathbb{Z}/q\mathbb{Z}$ as

$$\sum_{1 \leq x \leq q} F(x) \overline{\mathbf{1}_{\mathcal{I}}}(x) = \sum_{1 \leq y \leq q} \widehat{F}(y) \overline{\widehat{\mathbf{1}}_{\mathcal{I}}}(y), \quad (7.12)$$

where for any function F on $\mathbb{Z}/q\mathbb{Z}$ we define the Fourier transform as

$$\widehat{F}(y) = \frac{1}{q^{1/2}} \sum_{1 \leq x \leq q} F(x) e^{2\pi i xy/q}.$$

We claim that $|\widehat{\mathbf{1}}_{\mathcal{I}}(y)| \ll q^{-1/2} \min\{|\mathcal{I}|, \|y/q\|^{-1}\}$, where $\|y/q\|$ denotes the distance from y/q to the nearest integer. The first bound holds if $y \equiv 0 \pmod{q}$. If $y \not\equiv 0 \pmod{q}$, we use the notation $\mathcal{I} = [a, b]$ and write

$$\widehat{\mathbf{1}}_{\mathcal{I}}(y) = \frac{1}{q^{1/2}} \sum_{a \leq x \leq b} e^{2\pi i xy/q} = \frac{e^{\pi i(a+b)y/q}}{q^{1/2}} \frac{\sin(\pi(b-a+1)y/q)}{\sin(\pi y/q)}.$$

Since $|\sin(\pi y/q)| \geq 2\|y/q\|$, this proves the claim. As a result, $\|\widehat{\mathbf{1}}_{\mathcal{I}}\|_{\ell^1} \ll q^{-1/2}|\mathcal{I}| + q^{1/2} \log q \ll q^{1/2} \log q$, and we conclude that

$$\left| \sum_{x \in \mathcal{I}} F(x) \right| \ll q^{1/2} \log q \cdot \|\widehat{F}\|_{\ell^\infty(\mathbb{F}_q)}. \quad (7.13)$$

This method has transferred the work to studying the size of the Fourier transform of F . In this context, it is worth recalling that if F is an appropriate trace function, the complete sum of F in (7.4) is identically equal to $q^{1/2}\widehat{F}(0)$, so that the square-root cancellation bound (7.4) implies that $|\widehat{F}(0)| \ll C_F$.

The more general result we now need is as follows: if F is a trace function of “Fourier class,”

$$\|\widehat{F}\|_{\ell^\infty(\mathbb{F}_q)} \ll C_F^2,$$

where C_F is the conductor of F (see [27, Thm. 5.2]). For trace functions of this Fourier class, we thus deduce the upper bound

$$\sum_{x \in \mathcal{I}} F(x) \ll C_F^2 q^{1/2} \log q. \quad (7.14)$$

Here we have followed the exposition of [27, §7.2], to which we refer for the definition of the Fourier class [27, Dfn. 7.1]. Simplistically, the Fourier class rules out the example $F(x) = e^{2\pi i ax/q}$, in which case $\widehat{F}(x) = q^{1/2} \delta_{x \equiv -a \pmod{q}}(x)$ can take “large” values. But it allows the example $F(x) = \chi(x)$, where χ is a non-principal

multiplicative Dirichlet character modulo q , in which case $|\widehat{F}(x)| \leq q^{-1/2}|\tau(\chi)|$ as long as $\gcd(x, q) = 1$, where $\tau(\chi)$ denotes the Gauss sum of χ ; it is known that $|\tau(\chi)| = q^{1/2}$, and hence $|\widehat{F}(x)| \leq 1$ for all $x \in \mathbb{F}_q$. In the case that F is a multiplicative Dirichlet character χ , the bound (7.14) was originally proved (for any integer q) in [56, 64] and is known as the Pólya–Vinogradov bound.

One way to interpret the Pólya–Vinogradov bound (7.14) is that it is nontrivial as long as $|\mathcal{I}| \gg_{C_F} q^{1/2} \log q$. How can we improve on this? Fouvry et al developed a method in [26] to remove the factor of $\log q$ at the threshold $|\mathcal{I}| \approx q^{1/2}$. Alternatively it can be advantageous to smooth a sum before estimation; we see this directly in (7.12), since if $\mathbf{1}_{\mathcal{I}}$ is replaced by a smoother function, its Fourier transform will have better decay properties, and potentially smaller ℓ^1 norm. In the setting of trace functions, smoothing allows one to remove the $\log q$ for any interval \mathcal{I} [27, Prop. 6.5].

Nontrivial bounds when $|\mathcal{I}| = o(q^{1/2})$ seem to be out of reach of the general ideas we have mentioned so far. These are the so-called short sums, and are the focus of the next section.

8 Quasi-superorthogonality and the Burgess Method

Given a function $F : \mathbb{Z} \rightarrow \mathbb{C}$ of period q , we consider the short sum

$$\sum_{x \in \mathcal{I}} F(x) \tag{8.1}$$

over an interval $\mathcal{I} \subsetneq [1, q]$ with $|\mathcal{I}| = O(q^{1/2})$. If F is a trace function (and q is prime), an ambitious and powerful goal is to prove a nontrivial $o(|\mathcal{I}|)$ bound, perhaps even a bound as small as $O(|\mathcal{I}|^{1/2})$, as long as $|\mathcal{I}| \gg q^\varepsilon$ for some $\varepsilon > 0$. This would be a very deep result. For example, in the case where F is a Dirichlet character, this is intimately connected to the Lindelöf Hypothesis for the associated Dirichlet L -function (see for example Conjecture C_n in [28, §9] as well as their remark on equation (9.6) in that paper).

We now develop a formal chain of ideas to prove a nontrivial bound for short sums, starting from first principles. Motivated by the Pólya–Vinogradov method, we allow ourselves to guess that it will be advantageous to link the incomplete sum to a complete sum such as (7.4). A first idea might be to distribute multiple copies of the sum (8.1) via affine transformations so as to cover the complete set of residues $\mathbb{Z}/q\mathbb{Z}$, but this naive approach could lead to an error term on the order of $|\mathcal{I}|$, leading us back where we started. In his thesis in the 1950s, D. Burgess had another idea: to employ many different changes of variables to redistribute copies of the sum (8.1) sufficiently densely over $\mathbb{Z}/q\mathbb{Z}$ that the *starting points* of the transformed intervals nearly cover a complete set of residues. We now sketch this approach quite formally, to reveal three key components, including Type II quasi-superorthogonality. Once we have understood the three key requirements of the method, we will begin to work precisely.

8.1 A Formalism for Short Sums

Initially we only assume that F is of period q and $|F| \leq 1$. Suppose that σ is an invertible change of variables acting on $\mathbb{Z}/q\mathbb{Z}$, with the image of \mathcal{I} under σ denoted by $\sigma(\mathcal{I})$; for simplicity, let us also suppose temporarily that F is invariant under the change of variables (and its inverse). Then

$$\sum_{x \in \mathcal{I}} F(x) = \sum_{y \in \sigma(\mathcal{I})} F(y).$$

If L such changes of variables are denoted by $\sigma_1, \dots, \sigma_L$, then averaging yields

$$\sum_{x \in \mathcal{I}} F(x) = \frac{1}{L} \sum_{1 \leq \ell \leq L} \sum_{y \in \sigma_\ell(\mathcal{I})} F(y).$$

Suppose that each image $\sigma_\ell(\mathcal{I})$ is a collection of translated copies of some set, say X ; we will return later to what X could be. Define a non-negative function $a(m)$ on $[1, q]$ by setting $a(m)$ to be the number of ℓ such that $X + m$ appears in $\sigma_\ell(\mathcal{I})$. Then

$$\sum_{x \in \mathcal{I}} F(x) = \frac{1}{L} \sum_{1 \leq m \leq q} a(m) \sum_{x \in X} F(m + x). \quad (8.2)$$

In order to separate out the function $a(m)$, which counts redundancies among the images but contains no information about the function F , it is natural to apply Hölder's inequality for some $1/p + 1/p' = 1$, obtaining

$$\left| \sum_{x \in \mathcal{I}} F(x) \right| \leq \frac{1}{L} \left(\sum_{1 \leq m \leq q} a(m)^{p'} \right)^{1/p'} \left(\sum_{1 \leq m \leq q} \left| \sum_{x \in X} F(m + x) \right|^p \right)^{1/p}. \quad (8.3)$$

In this arithmetic setting, it is natural to assume that p is an even integer, say $p = 2r$ with $r \geq 1$, so that we can expand the p th power in the last term. Note that in this case, $1/p' = 1 - 1/2r$ and $p' = 2r/(2r - 1) \leq 2$. The nesting property of discrete ℓ^p spaces shows that $\|\{a(m)\}\|_{\ell^2} \leq \|\{a(m)\}\|_{\ell^{p'}}$, but we are more likely going to succeed at estimating the second moment of the sequence $\{a(m)\}$ than a fractional moment. Since $a(\cdot)$ takes its values in non-negative integers, $\sum_m a(m)^{p'} \leq \sum_m a(m)^2$, so we can write $\|\{a(m)\}\|_{\ell^{p'}} \leq \|\{a(m)\}\|_{\ell^2}^{2/p'}$. It now suffices to understand two quantities: the second moment

$$\sum_{1 \leq m \leq q} a(m)^2, \quad (8.4)$$

and the ℓ^{2r} norm

$$\begin{aligned} \left\| \sum_{x \in X} F(m + x) \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}^{2r} &= \sum_{(x_1, \dots, x_{2r}) \in X^{2r}} \sum_{1 \leq m \leq q} F(m + x_1) \overline{F}(m + x_2) \\ &\quad \cdots F(m + x_{2r-1}) \overline{F}(m + x_{2r}) \\ &= \sum_{(x_1, \dots, x_{2r}) \in X^{2r}} q^{1/2} \widehat{F}_{\underline{x}}(0), \end{aligned} \quad (8.5)$$

where

$$F_{\underline{x}}(m) = F(m + x_1) \overline{F}(m + x_2) \cdots F(m + x_{2r-1}) \overline{F}(m + x_{2r}). \quad (8.6)$$

For which tuples \underline{x} would we expect good control of $q^{1/2} \widehat{F}_{\underline{x}}(0)$? This is characterized by the condition of quasi-superorthogonality. Define $f_n(m) = F(m + n)$, so that the left-hand side of (8.5) is

$$\left\| \sum_{n \in X} f_n \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}^{2r}. \quad (8.7)$$

Correspondingly, the contribution to the right-hand side from a tuple $(x_1, \dots, x_{2r}) \in X^{2r}$ is

$$\sum_{1 \leq m \leq q} f_{x_1}(m) \overline{f}_{x_2}(m) \cdots f_{x_{2r-1}}(m) \overline{f}_{x_{2r}}(m).$$

If the sequence of functions $\{f_n\}_{n \in X}$ has Type I (or Type II) quasi-superorthogonality with parameter ν , then the approximate direct inequality (7.2) shows that

$$\sum_{1 \leq m \leq q} \left| \sum_{x \in X} F(m + x) \right|^{2r} \ll |X|^{2r} q^\nu + |X|^r q. \quad (8.8)$$

Even at this level of abstraction, we have learned something: this general approach is optimized if each change of variables σ_ℓ transforms \mathcal{I} into a collection of even smaller sets X of cardinality $\approx q^{(1-\nu)/r}$. In particular, if F is a trace function that satisfies the quasi-superorthogonality property (7.6) with $\nu = 1/2$, we would see that this upper bound is minimized as a function of $|X|$ if $|X| = q^{1/(2r)}$.

These speculations suggest an approach to bounding the short sum of F over the interval \mathcal{I} :

- (I) construct appropriate changes of variables that replace \mathcal{I} by sets of “short short” intervals of length $\approx q^{1/(2r)}$ that are well-distributed over $[1, q]$;
- (II) control the redundancy of the intervals after such changes of variables via the second moment (8.4);

(III) prove that the family $\{f_n\}_n = \{F(\cdot + n)\}_n$ exhibits Type I or Type II quasi-superorthogonality in $\ell^{2r}(\mathbb{Z}/q\mathbb{Z})$.

Although Burgess's exposition in [11] is framed very differently, these can be seen as the three pillars of his method.

We state the special case of Burgess's theorem that we will prove by making these three principles precise.

Theorem 8.1 (Burgess) *Let χ be a multiplicative Dirichlet character modulo a prime q . Then for every integer $r \geq 1$,*

$$\left| \sum_{m \in (N, N+H]} \chi(m) \right| \ll_r H^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}} (\log q)^2. \quad (8.9)$$

Burgess further developed his method to apply when F is a primitive multiplicative Dirichlet character with composite modulus q , but with some restrictions: if q is not cubefree, then $r \leq 3$; see [12–14]. Burgess's work set record bounds for short character sums (essentially still standing), a question of Vinogradov on the least quadratic non-residue modulo q [65] (essentially still standing), and subconvexity bounds for Dirichlet L -functions (only recently broken by the Weyl-strength bound of Petrow and Young [51]).

The upshot of Burgess's work is that a nontrivial bound for a sum of length H holds when F is a non-principal (resp. primitive) multiplicative Dirichlet character with q prime (resp. q cubefree), as long as $H \gg q^{1/4+\varepsilon}$ for some small $\varepsilon > 0$. We see this by computing the optimal choice of r in (8.9) for a given H . If $H = q^{1/4+\kappa}$ for some small κ , then the Burgess bound (ignoring the logarithmic factor) proves the upper bound $\ll Hq^{-\delta}$ with $\delta = (4\kappa r - 1)/(4r^2)$. Computing the maximum of δ as a function of r , it is advantageous to choose r to be the nearest integer to $1/(2\kappa)$, so that as $\kappa \rightarrow 0$ the savings is on the order of $\delta \approx \kappa^2$.

Remark 8.2 Burgess proves a bound with $(\log q)$ instead of the factor $(\log q)^2$ we demonstrate here. One logarithm comes from the density of prime numbers; the extra logarithm in our presentation comes from the application of the Menchov–Rademacher inequality in Corollary 8.5.

We now provide a rigorous exposition of how to achieve the three points (i), (ii), and (iii) and prove Theorem 8.1. Initially, in order to rely only on these three principles, we omit an averaging step from Burgess's original argument. This makes the method more intuitive but the result is weaker than (8.9) by a factor of $q^{1/4r^2}$; see Theorem 8.6. This nevertheless provides a bound that is nontrivial for $H > q^{1/4+\kappa}$ for any $\kappa > 0$ once we choose r optimally. Finally, we show how to include the additional averaging step and recover Theorem 8.1. See Sect. 8.8 for citations of recent proofs that inspire two aspects of our exposition here, and further remarks.

It is an open, and very important, question whether some version of Burgess's ideas can be applied to more general (non-multiplicative) trace functions F . It would also be very significant to prove nontrivial bounds for Dirichlet character sums that are shorter than $q^{1/4+\varepsilon}$. We highlight a barrier for each of these goals below.

8.2 Property (i): Changes of Variables

Initially, let $F : \mathbb{Z} \rightarrow \mathbb{C}$ be a function of period q , for an integer q , and with $|F| \leq 1$. Let $\mathcal{I} \subset [1, q]$ be an interval of length at most $q^{1/2}$, which we will denote by $(N, N + H]$. By periodicity of F , we may assume that $0 \leq N < q$. We will make further assumptions about F as the need arises.

Fix $r \geq 1$. We seek a collection of changes of variables $x \mapsto \sigma_\ell(x)$ such that for each ℓ , the image $\sigma_\ell(\mathcal{I})$ is a set of short-short intervals, each of which is of length $\approx q^{1/2r}$. One idea is to break $(N, N + H]$ according to congruence classes. Fix an integer ℓ and $0 \leq b \leq \ell - 1$. Then $n = b + m_b \ell$ varies over the integers in $(N, N + H]$ that are congruent to $b \pmod{\ell}$ as m_b varies over integers in the interval $(\frac{N-b}{\ell}, \frac{N-b}{\ell} + \frac{H}{\ell}]$. This motivates us to think of σ_ℓ as a collection of maps from n to m_b , for each $0 \leq b < \ell$. Optimizing the approximate direct inequality (8.8) motivates us to choose ℓ so that $H/\ell \approx q^{1/2r}$.

We set $L = (1/2)Hq^{-1/2r}$ and suppose $\mathcal{L} \subseteq [L, 2L]$ is a set of integers ℓ that are relatively prime to q , which we will specify precisely later in (8.15). To ensure that $L \geq 1$, we suppose from now on that $H \geq 2q^{1/2r}$. We may do so, since for $H < 2q^{1/2r}$ the bound in Theorem 8.1 already holds. Once we fix r , we also assume that q is sufficiently large that $H/L = 2q^{1/2r} \geq 1$. Finally, we can assume that $H \leq q^{1/2+1/4r}$, since otherwise the Pólya–Vinogradov bound supersedes Theorem 8.1.

Now for each $\ell \in \mathcal{L}$ we write

$$\sum_{x \in (N, N + H]} F(x) = \sum_{0 \leq b < \ell} \sum_{\substack{x \in (N, N + H] \\ x \equiv b \pmod{\ell}}} F(x) = \sum_{0 \leq b < \ell} \sum_{m \in \left(\frac{N-b}{\ell}, \frac{N-b}{\ell} + \frac{H}{\ell}\right]} F(b + \ell m).$$

We still must make F invariant under this change of variables, as we required in (8.2). We can use the periodicity of F to our advantage; observe that as long as $(\ell, q) = 1$ then there is a bijection between the sets $\{b : b \pmod{\ell}\}$ and $\{aq : a \pmod{\ell}\}$. Thus the last expression is identical to

$$\sum_{0 \leq a < \ell} \sum_{m \in \left(\frac{N-aq}{\ell}, \frac{N-aq}{\ell} + \frac{H}{\ell}\right]} F(aq + \ell m) = \sum_{0 \leq a < \ell} \sum_{m \in \left(\frac{N-aq}{\ell}, \frac{N-aq}{\ell} + \frac{H}{\ell}\right]} F(\ell m), \quad (8.10)$$

under the periodicity of F .

In order to achieve uniformity with respect to ℓ , we must make an assumption about F : we assume that F is *totally multiplicative*, meaning that $F(\ell m) = F(\ell)F(m)$ for all integers ℓ, m . This is a significant restriction: any function $F : \mathbb{Z} \rightarrow \mathbb{C}$ that has the property that it is periodic of period q , totally multiplicative, and $F(n)$ is nonzero if and only if $(n, q) = 1$ is a multiplicative Dirichlet character modulo q ; see e.g. [1, Thm. 6.15]. Thus from now on we assume that F is a multiplicative Dirichlet character.

Even after writing $F(\ell m) = F(\ell)F(m)$ in (8.10), the resulting expression is not completely invariant; by using the property that $|F| \leq 1$, we can achieve invariance if

we take absolute values, writing

$$\left| \sum_{x \in (N, N+H]} F(x) \right| \leq \sum_{0 \leq a < \ell} \left| \sum_{m \in \left(\frac{N-aq}{\ell}, \frac{N-aq}{\ell} + \frac{H}{\ell} \right]} F(m) \right|.$$

This is a transformation of the original sum, according to one such choice of ℓ . We average the above inequality over all $\ell \in \mathcal{L}$, leading to

$$\left| \sum_{x \in (N, N+H]} F(x) \right| \leq |\mathcal{L}|^{-1} \sum_{\ell \in \mathcal{L}} \sum_{0 \leq a < \ell} \left| \sum_{m \in \left(\frac{N-aq}{\ell}, \frac{N-aq}{\ell} + \frac{H}{\ell} \right]} F(m) \right|. \quad (8.11)$$

We define $a(m)$ to count the redundancies of the starting points,

$$a(m) = \#\{\ell \in \mathcal{L}, 0 \leq a < \ell : \lfloor (N - aq)/\ell \rfloor = m\}. \quad (8.12)$$

In particular, we can rewrite (8.11) as

$$\left| \sum_{x \in (N, N+H]} F(x) \right| \ll |\mathcal{L}|^{-1} \sum_m a(m) \max_{k \leq 2H/L} \left| \sum_{x \in (m, m+k]} F(x) \right|.$$

In our simple paradigm, the next step is to apply Hölder's inequality. First, it is worth noting that the sum over m is in fact finite, since by construction $a(m)$ is supported inside the set $[-q, q]$. Thus for $p = 2r$ with $1/p + 1/p' = 1$, again recalling $p' \leq 2$ and that the sequence $\{a(m)\}$ takes its values in non-negative integers, we can write

$$\begin{aligned} \left| \sum_{x \in (N, N+H]} F(x) \right| &\ll |\mathcal{L}|^{-1} \left(\sum_m a(m)^2 \right)^{1-1/2r} \\ &\cdot \left\| \max_{k \leq 2H/L} \left| \sum_{x \in (0, k]} F(\cdot + x) \right| \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}. \end{aligned} \quad (8.13)$$

This is an echo of (4.12) in Paley's proof of the direct inequality for the partial sums of the Walsh–Paley series.

8.3 Property (ii): Redundancy of Short–Short Intervals

By the definition of $a(m)$, the average is bounded by

$$\sum_m a(m) \ll \sum_{\ell \in \mathcal{L}, 0 \leq a < \ell} 1 \ll L^2.$$

We will show that the short-short intervals are well-distributed in the sense that the second moment has the same upper bound:

$$\sum_m a(m)^2 \ll L^2, \quad (8.14)$$

as long as we restrict the values in \mathcal{L} to be prime. Thus we now formally define

$$\mathcal{L} := \{\text{primes } \ell \nmid q, \ell \in [L, 2L] = [Hq^{-1/2r}/2, Hq^{-1/2r}]\}. \quad (8.15)$$

By the Prime Number Theorem, $|\mathcal{L}| \gg L/\log L$ as soon as q is larger than an absolute constant depending only on r , as we may assume by possibly enlarging the implicit constant in the bound of Theorem 8.1.

The main input to proving (8.14) is a lemma that counts the number of starting points that lie within a short distance of each other.

Lemma 8.3 *Fix $B \geq 1$ and $L \geq 1$ with $BL^2 < q$. For any integers ℓ, ℓ' let*

$$\mathcal{M}(\ell, \ell') = \#\{0 \leq a < \ell, 0 \leq a' < \ell' : |(N - aq)/\ell - (N - a'q)/\ell'| \leq B\}.$$

As ℓ, ℓ' range over a set \mathcal{L} of prime values in $[L, 2L]$,

$$\sum_{\ell, \ell'} \mathcal{M}(\ell, \ell') \ll L^2.$$

We apply this with $B = 1$ and \mathcal{L} as defined above. Then $\sum_m a(m)^2 \ll \sum_{\ell, \ell' \in \mathcal{L}} \mathcal{M}(\ell, \ell')$ and the second moment bound (8.14) follows from the case $B = 1$. Note that the assumption that $L^2 < q$ is met since we assume $H \leq q^{1/2+1/4r}$.

Proof of Lemma 8.3 We prove the lemma by adapting a method of Heath-Brown [35, §4]. If $\ell = \ell'$,

$$\mathcal{M}(\ell, \ell) = \#\left\{0 \leq a, a' < \ell : |a - a'| \leq \frac{B\ell}{q} \leq \frac{2BL}{q} \leq 2\right\} \ll L,$$

which suffices.

The case $\ell \neq \ell'$ is more intricate. We assume $N \geq 1$; the case $N = 0$ may be handled by a simpler adaptation. The first step is to replace N by a multiple of q (with an acceptable error relative to the scale B), so that a factor of q can be pulled out of all terms in the inequality defining $\mathcal{M}(\ell, \ell')$. We motivate this as follows. If we suppose that for some t we have $N/\ell - tq/\ell = O(B)$ this would require that $N - tq = O(BL)$, but by hypothesis $BL \leq BL^2 < q$ and we cannot necessarily replace N by an integral multiple of q with an error smaller than $q/2$. So we must allow for t itself to be a rational number, which we denote by t_1/t_2 . Thus we suppose for some integers t_1, t_2 that

$$\left|N - \frac{t_1 q}{t_2}\right| \leq 2BL. \quad (8.16)$$

This will hold for some $q/(BL) < t_2 \leq 2q/(BL)$ and $Nt_2/q < t_1 \leq 2Nt_2/q$ that we will specify momentarily.

Assume such t_1, t_2 exist for the moment. Fix $\ell \neq \ell'$. For any a, a' counted by $\mathcal{M}(\ell, \ell')$ we then see that

$$|(t_1q/t_2 - aq)/\ell - (t_1q/t_2 - a'q)/\ell'| \leq B + 2BL/\ell + 2BL/\ell' \leq 5B.$$

Thus

$$|t_1(\ell' - \ell) - (a\ell' - a'\ell)t_2| \leq 5\ell\ell't_2B/q \leq 20Lt_2(BL)/q \leq 40L.$$

For each d , let $D(\ell, \ell'; d)$ denote $\#\{0 \leq a < \ell, 0 \leq a' < \ell' : a\ell' - a'\ell = d\}$. Then let $D = \max_{d, \ell \neq \ell'} D(\ell, \ell'; d)$. We have shown that

$$\sum_{\ell \neq \ell' \in \mathcal{L}} \mathcal{M}(\ell, \ell') \ll D \sum_{|m| \leq 40L} \#\{\ell \neq \ell' \in \mathcal{L} : t_1(\ell' - \ell) \equiv m \pmod{t_2}\}. \quad (8.17)$$

We claim that if \mathcal{L} contains only prime values then $D \leq 1$. We further claim that we can choose t_1, t_2 satisfying the constraints above, with t_2 prime and $(t_1, t_2) = 1$. Assume these two claims, which we prove momentarily. Then given m , the congruence $t_1(\ell' - \ell) \equiv m \pmod{t_2}$ identifies $(\ell' - \ell)$ uniquely modulo t_2 . In \mathbb{Z} , the difference $(\ell' - \ell)$ is at most L , and under the hypothesis $BL^2 < q$ we see that $L < t_2$ so that $(\ell' - \ell)$ is uniquely identified in \mathbb{Z} as well. Thus once ℓ is chosen freely, ℓ' is uniquely chosen, and the sum over m on the right-hand side of (8.17) is $\ll L^2$, which suffices as long as $D \leq 1$.

We prove the two remaining claims. We choose t_2 to be a prime in the interval $(q/(BL), 2q/(BL))$, which exists by Bertrand's postulate (or alternatively by the Prime Number Theorem if we may assume that $q/(BL)$ is larger than an absolute constant, which we may in our application). Given t_2 , we choose t_1 to be either $\lceil Nt_2/q \rceil$ or $\lceil Nt_2/q \rceil + 1$, so that it is relatively prime to t_2 . Note that (8.16) then holds with these choices.

Finally, we bound D . It suffices to observe that under the assumption that $\ell \neq \ell'$ are primes, for each d , there is at most one pair a, a' with $0 \leq a < \ell$ and $0 \leq a' < \ell'$ solving $a\ell' - a'\ell = d$. Otherwise, suppose $a\ell' - a'\ell = d = b\ell' - b'\ell$ for $0 \leq a, b < \ell$ and $0 \leq a', b' < \ell'$. Then because we have assumed that $\ell \neq \ell'$ are primes, this shows that $\ell|(a - b)$ and $\ell'|(a' - b')$, which can only occur for a, a', b, b' in the allowed ranges if both differences are zero in \mathbb{Z} . \square

This completes the verification of (8.14) for property (ii).

8.4 Property (iii): Type II Quasi-superorthogonality and the Maximal Operator

We now need to bound the maximal partial sum norm in (8.13), using property (iii). Recall from (7.10) that as an application of Type II quasi-superorthogonality for Dirich-

let characters, for any integers $k_1 < k_2$,

$$\left\| \sum_{x \in (k_1, k_2]} F(\cdot + x) \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})} \ll_r (k_2 - k_1)q^{1/4r} + (k_2 - k_1)^{1/2}q^{1/2r}. \quad (8.18)$$

We now need to deduce an upper bound for the norm of the maximal partial sum operator, $\left\| \max_{k \leq 2H/L} \left| \sum_{x \in (0, k]} F(\cdot + x) \right| \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}$. We will do so via the “method of bisection,” which originated in the same paper of Rademacher we encountered earlier [57, pp. 118 and 129]. (This method also appeared independently in Menchov [47]. See e.g. [2] for references to modern proofs; it can also be used to prove the related Kolmogorov–Doob inequality for martingales [22, Chap. III Thm. 2.1, Chap. VII Thm. 3.2].) We encapsulate the method in two general statements.

Lemma 8.4 (Menchov–Rademacher) *Given a sequence $\{b(n)\}$ of complex numbers, for any integer $t \geq 0$ and any $p \geq 1$,*

$$\max_{0 \leq n \leq 2^t} |b(n) - b(0)|^p \leq (t+1)^{p-1} \sum_{i=0}^t \sum_{0 \leq v < 2^i} |b((v+1)2^{t-i}) - b(v2^{t-i})|^p.$$

The key point of this lemma is that the length of the sum over i on the right-hand side is logarithmic in scale, compared to the range $0 \leq n \leq 2^t$ of the maximum on the left-hand side. We deduce from this a useful fact: relative to the norm of a partial sum operator, the norm of an associated maximal partial sum operator (over a finite range) increases by at most a logarithm.

Corollary 8.5 *Let (\mathcal{M}, μ) be a measure space. Let $\{a_k(u)\}_k$ be a sequence of complex-valued functions in $L^p(\mathcal{M}, d\mu)$. Define for each integer $k \geq 0$,*

$$S_k(u) = \sum_{0 < m \leq k} a_m(u), \quad S_{k_1, k_2}(u) = \sum_{k_1 < m \leq k_2} a_m(u).$$

Fix $1 \leq p < \infty$. Suppose that uniformly in $k_2 > k_1$,

$$\|S_{k_1, k_2}(\cdot)\|_{L^p(\mathcal{M})} \leq c_p |k_2 - k_1|^{\alpha_p}.$$

Then as long as $p\alpha_p \geq 1$, for every $K \geq 2$,

$$\left\| \max_{0 \leq k \leq K} |S_k(\cdot)| \right\|_{L^p(\mathcal{M})} \ll_p c_p K^{\alpha_p} (\log K).$$

We defer the proof of the lemma and its corollary to the end of the section. We apply the corollary to the partial sums of $F(\cdot + x)$, using the uniform upper bound

(8.18), and $\mathcal{M} = \mathbb{Z}/q\mathbb{Z}$ with counting measure. This proves that for any $K \geq 2$,

$$\left\| \max_{k \leq K} \left| \sum_{x \in (0, k]} F(\cdot + x) \right| \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})} \ll_r (Kq^{1/4r} + K^{1/2}q^{1/2r})(\log K). \quad (8.19)$$

For our application in (8.13) we take $K = 2H/L = 4q^{1/2r}$, so that the right-hand side is $\ll_r q^{3/4r}(\log q)$.

8.5 Deduction of a Weak Burgess Bound

We input the consequences (8.14) and (8.19) of properties (ii) and (iii) into our key relation (8.13). Upon recalling the definition of \mathcal{L} and L , this yields the following result, which is larger than the classical Burgess bound by a factor of $q^{1/4r^2}$.

Theorem 8.6 (Weak bound) *Let χ be a non-principal multiplicative Dirichlet character modulo a prime q . Then for every integer $r \geq 1$,*

$$\left| \sum_{x \in (N, N+H]} \chi(x) \right| \ll_r H^{1-1/r} q^{(r+2)/4r^2} (\log q)^2. \quad (8.20)$$

Supposing that $H = q^\beta$, we see that for a fixed r , the exponent is $< \beta$ (so that the bound is $o(H)$) when $\beta > 1/4 + 1/2r$. Thus in particular, the bound only has a chance of being nontrivial if $\beta > 1/4$, showing that we recovered the same core threshold as the classical Burgess bound. Now let us fix $\beta = 1/4 + \kappa$ for some small $\kappa > 0$ and compute the optimal choice of r . Up to a factor of $(\log q)^2$, the upper bound in (8.20) is $\ll Hq^{-\delta}$ with $\delta = (2\kappa r - 1)/(2r^2)$. Computing the maximum of δ as a function of r , it is advantageous to choose r to be the nearest integer to $1/\kappa$, and as $\kappa \rightarrow 0$ the savings is on the order of $\delta \approx \kappa^2/2$. See Sect. 8.8.1 for further comparison to the Burgess bound.

We proved this weak bound in order to demonstrate the three core principles. To recover the classical Burgess bound, we now introduce further averaging to (8.11) and prove a second moment bound analogous to (8.14) but for a different function $a^\sharp(m)$.

8.6 Property (ii) Revisited: Additional Averaging to Prove the Strong Burgess Bound

In our schematic argument, when passing from (8.2) to (8.3) via Hölder's inequality, we lose less if $a(m)$ is nonzero for as many $m \in [1, q]$ as possible (but also not too large at any m). Within our precise argument, this motivates us to further average (8.11) over an even larger family of short-short intervals that are relatively well-distributed across $[1, q]$. A version of the further averaging we now describe appeared in Burgess's original work.

Any interval $(A, A + B]$ can be written as a difference $(A - A_0, A + B] \setminus (A - A_0, A]$, for every $A_0 \geq 0$. Moreover, as long as $A_0 \leq B$, then the longer interval $(A - A_0, A + B]$ is still of length at most $2B$, and hence comparable to the length of the original interval. There are B ways to write $(A, A + B]$ as such a difference. We apply this to $\left(\frac{N-aq}{\ell}, \frac{N-aq}{\ell} + \frac{H}{\ell}\right]$ in order to average (8.11) over $H/\ell \approx q^{1/2r}$ more short-short intervals.

Precisely, we observe that the right-hand side of (8.11) is equal to

$$\begin{aligned} & |\mathcal{L}|^{-1} \sum_{\ell \in \mathcal{L}} \sum_{0 \leq a < \ell} (H/\ell)^{-1} \sum_{m \in \left(\frac{N-aq}{\ell} - \frac{H}{\ell}, \frac{N-aq}{\ell}\right]} \left| \sum_{x \in \left(m, \frac{N-aq}{\ell} + \frac{H}{\ell}\right]} F(x) - \sum_{x \in \left(m, \frac{N-aq}{\ell}\right]} F(x) \right| \\ & \ll |\mathcal{L}|^{-1} q^{-1/2r} \sum_{\ell \in \mathcal{L}} \sum_{0 \leq a < \ell} \sum_{m \in \left(\frac{N-aq}{\ell} - \frac{H}{L}, \frac{N-aq}{\ell}\right]} 2 \max_{k \leq 2H/L} \left| \sum_{x \in (m, m+k]} F(x) \right|. \end{aligned}$$

Now we define $a^\sharp(m)$ to count the redundancies of the starting points,

$$a^\sharp(m) = \#\left\{\ell \in \mathcal{L}, 0 \leq a < \ell : m \in \left(\frac{N-aq}{\ell} - \frac{H}{L}, \frac{N-aq}{\ell}\right]\right\}. \quad (8.21)$$

We conclude that

$$\left| \sum_{x \in (N, N+H]} F(x) \right| \ll |\mathcal{L}|^{-1} q^{-1/2r} \sum_m a^\sharp(m) \max_{k \leq 2H/L} \left| \sum_{x \in (m, m+k]} F(x) \right|.$$

We prepare to apply Hölder's inequality so we can exploit Type II quasi-superorthogonality in $\ell^{2r}(\mathbb{Z}/q\mathbb{Z})$. First note that the sum is finite since $a^\sharp(m)$ is supported inside $[-2q, 2q]$. Thus for $p = 2r$ with $1/p + 1/p' = 1$, upon recalling $p' \leq 2$, since $a^\sharp(\cdot)$ takes its values in non-negative integers we can write

$$\begin{aligned} \left| \sum_{x \in (N, N+H]} F(x) \right| & \ll |\mathcal{L}|^{-1} q^{-1/2r} \left(\sum_m a^\sharp(m)^2 \right)^{1-1/2r} \\ & \cdot \left\| \max_{k \leq 2H/L} \left| \sum_{x \in (0, k]} F(\cdot + x) \right| \right\|_{\ell^{2r}(\mathbb{Z}/q\mathbb{Z})}. \end{aligned} \quad (8.22)$$

Compared to (8.13), we have an extra savings $q^{-1/2r}$, but possibly larger values $a^\sharp(m)$ compared to $a(m)$.

We will again bound the second moment comparable to its average:

$$\sum_m a^\sharp(m)^2 \ll HL.$$

This is larger than (8.14) by a factor of $q^{1/2r}$, but since this is raised to the power $(1 - 1/2r)$ in (8.22), we still gain a total of $q^{-1/4r^2}$ in extra savings in (8.22). Note that

$$\sum_m a^\sharp(m)^2 \ll (H/L) \sum_{\ell, \ell' \in \mathcal{L}} M^\sharp(\ell, \ell'),$$

where we now define

$$M^\sharp(\ell, \ell') = \#\{0 \leq a < \ell, 0 \leq a' < \ell' : |(N - aq)/\ell - (N - a'q)/\ell'| \leq H/L\}.$$

We can then apply Lemma 8.3 with $B = H/L$; note that $BL^2 = HL < q$ is satisfied since $H \leq q^{1/2+1/4r}$, and this verifies the second moment bound. With this and (8.19) in hand, (8.22) immediately proves

$$\left| \sum_{x \in (N, N+H]} F(x) \right| \ll_r |\mathcal{L}|^{-1} q^{-1/2r} (LH)^{1-1/2r} q^{3/4r} \log q \ll_r H^{1-1/r} q^{(r+1)/4r^2} (\log q)^2,$$

proving Theorem 8.1.

8.7 The Menchov–Rademacher Inequality: Proof of the Lemmas

Proof of Lemma 8.4 If $n = 2^t$ then $|b(n) - b(0)|^p$ appears on the right-hand side as the summand with $i = v = 0$, and thus we may fix our attention on the maximum over $1 \leq n < 2^t$. Fix $1 \leq n < 2^t$ and write its binary expansion as

$$n = \sum_{i=0}^t \varepsilon_i 2^{t-i}, \quad \varepsilon_i = \varepsilon_i(n) \in \{0, 1\}, \quad \varepsilon_0 = \varepsilon_0(n) = 0.$$

We write a telescoping sum for the difference of interest:

$$\begin{aligned} b(n) - b(0) &= \sum_{i=1}^t \left\{ b\left(\sum_{j \leq i} \varepsilon_j 2^{t-j}\right) - b\left(\sum_{j < i} \varepsilon_j 2^{t-j}\right) \right\} \\ &= \sum_{i=1}^t \left\{ b\left(2^{t-i} \sum_{j \leq i} \varepsilon_j 2^{i-j}\right) - b\left(2^{t-i} \sum_{j < i} \varepsilon_j 2^{i-j}\right) \right\}. \end{aligned}$$

For each $1 \leq i \leq t$ it is then convenient to define

$$v_i = v_i(n) = \sum_{0 \leq j < i} \varepsilon_j 2^{i-j}.$$

We also define $v_0 = 0$. Observe that $0 \leq v_i < 2^i$ for each $1 \leq i \leq t$, and (recalling $\varepsilon_0 = 0$) we can write

$$b(n) - b(0) = \sum_{i=0}^t \left\{ b(v_i 2^{t-i} + \varepsilon_i 2^{t-i}) - b(v_i 2^{t-i}) \right\}.$$

Fix $1 \leq p < \infty$. Taking absolute values and applying Hölder's inequality,

$$|b(n) - b(0)|^p \leq (t+1)^{p-1} \sum_{i=0}^t \left| b(v_i 2^{t-i} + \varepsilon_i 2^{t-i}) - b(v_i 2^{t-i}) \right|^p.$$

We only possibly increase the right-hand side if we sum over all possible values of $v_i < 2^i$; additionally, all nonzero terms on the right-hand side have $\varepsilon_i = 1$, and we only possibly increase the right-hand side if we assume this always is the case. Thus

$$|b(n) - b(0)|^p \leq (t+1)^{p-1} \sum_{i=0}^t \sum_{0 \leq v < 2^i} \left| b((v+1)2^{t-i}) - b(v2^{t-i}) \right|^p.$$

Now we note that the right-hand side is independent of $1 \leq n < 2^t$, and the lemma is proved. \square

Proof of Corollary 8.5 Fix $1 \leq p < \infty$. Given $K \geq 2$, let $t \geq 1$ be such that $2^{t-1} \leq K < 2^t$. Then the left-hand side of the claimed inequality is dominated by $\| \max_{0 \leq k \leq 2^t} |S_k(\cdot)| \|_{L^p(\mathcal{M})}$ while the putative right-hand side is comparable to $(2^t)^{\alpha_p} (\log(2^t))$. Thus it suffices to prove the inequality for the case $K = 2^t$.

We apply the lemma for each fixed u , with the choice $b(k) = S_k(u)$, followed by the uniform upper bound for the L^p norm in the hypothesis. (Note that by construction $S_0(u) \equiv 0$ since it is an empty sum, so $|b(k) - b(0)| = |b(k)|$.) Thus we reason that:

$$\begin{aligned} \left\| \max_{0 \leq k \leq 2^t} |S_k(\cdot)| \right\|_{L^p(\mathcal{M})}^p &= \int_{\mathcal{M}} \max_{0 \leq k \leq 2^t} |S_k(u)|^p d\mu(u) \\ &\leq \int_{\mathcal{M}} (t+1)^{p-1} \sum_{i=0}^t \sum_{0 \leq v < 2^i} |S_{v2^{t-i}, (v+1)2^{t-i}}(u)|^p d\mu(u) \\ &= (t+1)^{p-1} \sum_{i=0}^t \sum_{0 \leq v < 2^i} \|S_{v2^{t-i}, (v+1)2^{t-i}}(\cdot)\|_{L^p(\mathcal{M})}^p \\ &\leq c_p^p (t+1)^{p-1} \sum_{i=0}^t \sum_{0 \leq v < 2^i} (2^{t-i})^{p\alpha_p} \\ &\leq c_p^p (t+1)^p 2^{tp\alpha_p}. \end{aligned}$$

Here we used $\alpha_p p \geq 1$ so that the factor $2^{-ip\alpha_p}$ at least dominates the $O(2^i)$ contribution of summing trivially over v . Thus we have shown $\| \max_{0 \leq k \leq 2^t} |S_k(\cdot)| \|_{L^p(\mathcal{M})} \leq$

$c_p(t+1)2^{t\alpha_p}$. Since $(t+1) \ll 2 \log(2^t)$ as long as $t \geq 1$, this suffices for the case $K = 2^t$ under consideration. \square

8.8 Further Remarks on the Burgess Bound

8.8.1 Comparison of the Weak Bound to Burgess Bound

For a given r , the weak bound (8.20) is nontrivial if $H > q^{1/4+1/2r}$ while the Burgess bound (8.9) is nontrivial if $H > q^{1/4+1/4r}$. Thus in the limit of arbitrarily large r , each has a threshold around $H > q^{1/4+\varepsilon}$ for $\varepsilon > 0$ arbitrarily small. But for any fixed r , and in particular for small r , the difference between (8.20) and (8.9) is significant. Up to logarithmic factors, the weak bound is worse than Pólya–Vinogradov if $r = 1$, meets it if $r = 2$, and improves on it for $r \geq 3$; the Burgess bound meets Pólya–Vinogradov for $r = 1$ and improves on it for $r \geq 2$. This behavior for small r also matters for composite q ; the Burgess bound (8.9) is only known (via a more intricate proof) for $r \leq 3$ unless q is cubefree, and one would expect similar restrictions for the weak bound.

We specify the impact on subconvexity bounds for the Dirichlet L -function $L(1/2 + it, \chi)$ with χ of modulus q . Assume an upper bound of the form

$$S(x) = \sum_{1 \leq n \leq x} \chi(n) \ll q^\varepsilon \min\{q^{1/2}, x^\alpha q^\beta\}$$

for some $\alpha \leq 1$, $\beta \leq 1/2$. An application of the approximate functional equation [39, Chap. 12] shows that if $\alpha \leq 1/2$ then

$$|L(1/2 + it, \chi)| \ll q^\varepsilon \max\{q^{(\alpha+\beta-1/2)/(2\alpha)}, q^\beta\},$$

and if $\alpha > 1/2$ then

$$|L(1/2 + it, \chi)| \ll q^\varepsilon \max\{q^{(\alpha+\beta-1/2)/(2\alpha)}, q^{\beta+(1/2+\beta)(\alpha-1/2)/\alpha}\}.$$

The Burgess bound (8.9) provides $\alpha = 1 - 1/r$, $\beta = (r+1)/4r^2$ and the optimal choice occurs at $r = 2$, thus proving Burgess's famous subconvexity bound $q^{1/4-1/16+\varepsilon}$. But the weaker bound (8.20) provides $\alpha = 1 - 1/r$, $\beta = (r+2)/4r^2$ and the optimal choice occurs at $r = 3$, leading to the much weaker bound $q^{1/4-1/48+\varepsilon}$.

8.8.2 Influences and Expositions

One can speculate how Burgess arrived at his clever method. Burgess's first paper cites Davenport and Erdős [19] as a point of inspiration [11, Lemma 2, p. 108]. Davenport and Erdős addressed Vinogradov's question on the least quadratic nonresidue modulo a prime q . In [19, Lemma 1] they consider (8.5) in the case $r = 1$, proving the

identity

$$\sum_{m \pmod{q}} \left| \sum_{x \in (0, k]} \chi(m+x) \right|^2 = qk - k^2.$$

This does not require the Weil or Deligne bounds; Davenport and Erdős cite a 1906 thesis of Jacobsthal, and conjecture in a footnote it could have been known to Gauss. In [19, Lemma 3] they consider the $2r$ th moment for any $r \geq 1$ and prove what we call here an approximate direct inequality, referencing Weil's very recent work at that time (Burgess cites [68, §IV]). But they state that “it does not seem to throw any light on the problem of the magnitude of the least quadratic non-residue;” Burgess changed this.

In this exposition, we introduce the new perspective that Burgess's argument is an application of superorthogonality, which incidentally we have seen was “in the air” in the 1920s and 1930s. Additionally, we incorporated elements of two treatments that streamline Burgess's original method. Unpublished notes of H. Montgomery from the 1970s, later developed into [29], introduced the use of the Menchov–Rademacher argument; this allows a more direct approach than Burgess described, and unifies the treatment when $N = 0$ and $N \neq 0$, at the cost of a factor of $(\log q)^2$ instead of $(\log q)$ in the final Burgess bound. (In Burgess's work, certain disjointness properties of the short-short intervals were easier to prove when $N = 0$.) We also applied ideas of Heath-Brown [35], which completely removed the need to show the short-short intervals are disjoint, by instead bounding the second moment (8.14). There are other modern approaches of alternative flavors, such as [39, Thm. 12.6] in terms of multiplicative shifts, and a smoothed version in [27, §17].

Recent work has succeeded in applying Burgess-type arguments in other settings that involve multiplicative Dirichlet characters: see among other works [4, 15, 16, 20, 35, 36]. See also [27, §17.2, §17.3] for an exposition applying some of these ideas to so-called Type II and Type III sums, after introducing further averaging. Burgess arguments have also now been developed for “mixed” character sums, in which $F(x) = \chi(x)e^{2\pi i g(x)}$ where χ is a multiplicative Dirichlet character and g is any real-valued polynomial; interestingly, these use the resolution of the Vinogradov Mean Value Theorem; see [37, 52, 54, 55], and also the earlier [17]. But the step (8.10), in which we assumed that F is totally multiplicative, prevents this argument from working more generally for trace functions. It would be of great interest to expand these ideas to apply to non-multiplicative trace functions.

8.9 Further Types: Short Sums of Random Multiplicative Functions

In this section we studied short sums of multiplicative trace functions. Short sums of other multiplicative functions are also of great interest; for example, the Riemann Hypothesis is equivalent to the claim that $\sum_{n \leq x} \mu(n) = O(x^{1/2+\varepsilon})$ for all $x \geq 1$, and all $\varepsilon > 0$, where $\mu(\cdot)$ is the Möbius function.

Wintner [69] initiated a more general study of short sums of “random multiplicative functions.” One model is given by Rademacher random multiplicative functions. These are built from the Rademacher distributions we have already seen, as follows. As p varies over primes, f_p is a sequence of independent random variables taking values ± 1 with probability $1/2$. For square-free n , the random variable f_n is defined by $f_n = \prod_{p|n} f_p$. Another model is a Steinhaus random multiplicative function: as p varies over primes, f_p is a sequence of independent random variables uniformly distributed on the unit circle, with $f_n = \prod_{p^a||n} f_p^a$.

Let $\{f_n\}_n$ denote a sequence of such independent random multiplicative functions. Recent work has computed (among other striking results) asymptotics for $\|\sum_{n \leq N} f_n\|_{L^k}$, see [33,34]. In the Steinhaus case, for $k = 2r$ an even integer, the first step of the proof is an observation of superorthogonality, namely that a term $\int f_{n_1} \bar{f}_{n_2} \cdots f_{n_{2r-1}} \bar{f}_{n_{2r}}$ vanishes unless $n_1 n_3 \cdots n_{2r-1} = n_2 n_4 \cdots n_{2r}$. We can think of this as a “multiplicative diagonal” constraint. In the Rademacher case, for any integer k the first step of the proof reveals yet another type of superorthogonality, namely that a term $\int f_{n_1} \cdots f_{n_k}$ vanishes unless $n_1 \cdots n_k$ is a perfect square and each n_1, \dots, n_k is square-free. Each of these can be compared to Type I* superorthogonality.

Acknowledgements Pierce is partially supported by NSF CAREER Grant DMS-1652173, a Sloan Research Fellowship, and the AMS Joan and Joseph Birman Fellowship.

Appendix A: Further Remarks on Walsh–Paley Series

We deferred a few details on the direct and converse inequalities in the setting of Walsh–Paley series in Sect. 4. Here, we first remark on the limiting argument to obtain (4.4) for $p = 2r$ from the truncated version (4.21). Second, we remark on deducing the cases for $1 < p < \infty$ from the cases with p an even integer; this illustrates a further application of Khintchine’s inequality. Third, we show how to deduce the operator bound (4.5) from the dyadic direct and converse inequalities (4.4).

A.1. Limiting Arguments for Direct and Converse Inequalities

Fix $p = 2r$. In the main text we showed that uniformly in N ,

$$\left\| \sum_{n=0}^N f_n \right\|_{L^p} \leq c_p \left\| \left(\sum_{n=0}^N f_n^2 \right)^{1/2} \right\|_{L^p} \leq c_p \left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p}.$$

The same method of proof used to obtain this shows that for any $N_1 < N_2$,

$$\|S_{2^{N_2}} f - S_{2^{N_1}} f\|_{L^p} \leq c_p \left\| \left(\sum_{n=N_1+1}^{N_2} f_n^2 \right)^{1/2} \right\|_{L^p}.$$

If f is such that the right-hand side of the direct inequality converges, then this tail must vanish as $N_1, N_2 \rightarrow \infty$, so that as $N \rightarrow \infty$, $S_{2N} f$ converges in L^p norm to some function, say F , which satisfies $\|F\|_{L^p} \leq c_p \left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p}$. By the Dominated Convergence Theorem, for each m

$$c_m(F) = \int_0^1 F(\theta) w_m(\theta) d\theta = \int_0^1 f(\theta) w_m(\theta) d\theta = c_m(f),$$

and since $\{w_m\}$ is a complete orthonormal system on $[0, 1]$, we conclude $F = f$, verifying the direct inequality. For the converse inequality, we apply the maximal bound (4.20) to see that $\left\| \left(\sum_{n=0}^N f_n^2 \right)^{1/2} \right\|_{L^p} \leq c'_p \left\| \sum_{n=0}^N f_n \right\|_{L^p} \ll_p \|f\|_{L^p}$ uniformly in N , which suffices.

A.2 Linearization

We have verified the direct and converse inequalities (4.4) in L^p for each even integer $p \geq 2$. To conclude the results for all $1 < p < \infty$, we recall Paley's arguments (now standard), in which the Rademacher functions again make an appearance, via Khintchine's inequality.

One would like to interpolate either the direct inequality (or the converse inequality, respectively), but one must first linearize. For any fixed $1 < p < \infty$, the truth for all $f \in L^p$ of the direct and converse inequalities

$$\left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p} \ll_p \|f\|_{L^p} \ll_p \left\| \left(\sum_{n=0}^{\infty} f_n^2 \right)^{1/2} \right\|_{L^p} \quad (\text{A.1})$$

is equivalent to the truth of the statement that

$$\|f^*\|_{L^p} \ll_p \|f\|_{L^p} \ll_p \|f^*\|_{L^p} \quad (\text{A.2})$$

holds for all $f \in L^p$, uniformly for all choices of $\varepsilon_n \in \{\pm 1\}$, where

$$f^*(t) = \sum_{n=0}^{\infty} \varepsilon_n f_n(t).$$

The advantage of (A.2) is that the expressions in this inequality are linear, and thus well-suited to interpolation.

Let us verify the equivalence. If (A.2) holds, to deduce (A.1), we use the Rademacher functions. Given f and its associated sequence $\{f_n\}$ we define an auxiliary function $F(t, \theta) = \sum_{n=0}^{\infty} r_n(\theta) f_n(t)$ for each $\theta \in [0, 1]$. By assumption of (A.2), for each fixed θ ,

$$\int_0^1 |F(t, \theta)|^p dt \ll_p \int_0^1 |f(t)|^p dt \ll_p \int_0^1 |F(t, \theta)|^p dt.$$

We integrate this over $\theta \in [0, 1]$ to conclude by Fubini's theorem that

$$\int_0^1 \int_0^1 \left| \sum_{n=0}^{\infty} r_n(\theta) f_n(t) \right|^p d\theta dt \ll_p \int_0^1 |f(t)|^p dt \ll_p \int_0^1 \int_0^1 \left| \sum_{n=0}^{\infty} r_n(\theta) f_n(t) \right|^p d\theta dt.$$

Now for each fixed t we apply Khintchine's inequality (2.5), and this proves that (A.1) holds, as desired.

The converse is more elementary. Given $f \in L^p$, and any choice of $\{\varepsilon_n\}$, f^* is the function with associated expansion $\sum_{n=0}^{\infty} g_n$ with $g_n = \varepsilon_n f_n$, so that applying the direct inequality followed by the converse inequality assumed in (A.1) shows that

$$\|f^*\|_{L^p} \ll_p \left\| \left(\sum_n g_n^2 \right)^{1/2} \right\|_{L^p} = \left\| \left(\sum_n f_n^2 \right)^{1/2} \right\|_{L^p} \ll_p \|f\|_{L^p}.$$

One obtains $\|f\|_{L^p} \ll_p \|f^*\|_{L^p}$ in an analogous fashion.

A.3 Remarks for $2 \leq p < \infty$

We know that (A.1) and hence (A.2) holds for each $p = 2r$ with $r \geq 1$ an integer. We fix a sequence $\{\varepsilon_n\}_n$ with $\varepsilon_n \in \{\pm 1\}$ and consider a truncation $(S_{2^N} f)^*(t) = \sum_{0 \leq n \leq N} \varepsilon_n f_n(t)$. Then applying the left-hand side of (A.2), for every even integer $p \geq 2$,

$$\|(S_{2^N} f)^*\|_{L^p} \ll_p \|S_{2^N} f\|_{L^p} \ll_p \|f\|_{L^p},$$

in which the last inequality holds uniformly in N , by the maximal theorem in (4.20). By Riesz–Thorin interpolation between $p = 2$ and any even integer, we conclude that this inequality holds for all $2 \leq p < \infty$. For a fixed $p \geq 2$, we can then deduce that $(S_{2^N} f)^*$ converges in L^p norm to a limit function, say F^* . By the Dominated Convergence Theorem, the coefficients $c_m(F^*)$ agree with those of f^* , and since the Walsh functions form a complete system, we learn that $F^* = f^*$. We conclude that $\|f^*\|_{L^p} \ll_p \|f\|_{L^p}$, obtaining the left-hand inequality of (A.2) for each $2 \leq p < \infty$. For the other inequality, we simply observe that given f and a fixed sequence $\{\varepsilon_n\}$, then $(f^*)^* = f$, so the right-hand inequality of (A.2) follows.

A.4 Remarks for $1 < p \leq 2$

One again uses the linearized inequalities (A.2) in order to apply duality. Fix $1 < p \leq 2$, and fix a sequence of $\varepsilon_n \in \{\pm 1\}$, and accordingly define $f_N^* = \sum_{0 \leq n \leq N} \varepsilon_n f_n$. By duality, to show that $\|f_N^*\|_{L^p} \ll_p \|f\|_{L^p}$ it suffices to show that for all $g \in L^{p'}$ with $1/p + 1/p' = 1$, $\|f_N^* g\|_{L^1} \ll_p \|g\|_{L^{p'}} \|f\|_{L^p}$. Precisely,

$$\left\| \left(\sum_{n=0}^N \varepsilon_n f_n \right) g \right\|_{L^1} = \left\| \left(\sum_{n=0}^N \varepsilon_n g_n \right) f \right\|_{L^1} \leq \left\| \sum_{n=0}^N \varepsilon_n g_n \right\|_{L^{p'}} \left\| f \right\|_{L^p},$$

with the last inequality due to Hölder's inequality. We apply the known case for $p' \geq 2$, so that $\left\| \sum_{n=0}^N \varepsilon_n g_n \right\|_{L^{p'}} \ll_p \|g\|_{L^{p'}}$, uniformly in the choice of signs $\{\varepsilon_n\}$. We conclude that $\|f_N^*\|_{L^p} \ll_p \|f\|_{L^p}$ uniformly in N , and uniformly in the choice of $\{\varepsilon_n\}$. Thus we may argue as before that f_N^* converges in L^p norm to a function, which we may check is indeed $f^* = \sum \varepsilon_n f_n$, and this verifies that $\|f^*\|_{L^p} \ll_p \|f\|_{L^p}$ holds. For the other inequality, we again note that for each fixed choice of signs, $(f^*)^* = f$, and thus we obtain $\|f\|_{L^p} \ll_p \|f^*\|_{L^p}$, concluding the proof.

A.5 Combining the Direct and Converse Inequalities

Fix $1 < p < \infty$ and $n \geq 1$. To combine the direct and converse inequalities for the dyadic differences $f_n = S_{2^n}f - S_{2^{n-1}}f$ in order to bound $S_n f$ on L^p , we must be able to express the partial sum $S_n f$ in terms of dyadic differences. Paley employs an identity of the following flavor. Write the binary expansion $n = 2^{n_1} + \dots + 2^{n_s}$ with $n_1 > \dots > n_s$. We claim

$$\begin{aligned} w_n(t)w_n(\theta) \sum_{m=0}^{n-1} w_m(t)w_m(\theta) &= \sum_{m \in [2^{n_1}, 2^{n_1+1})} w_m(t)w_m(\theta) \\ &\quad + \dots + \sum_{m \in [2^{n_s}, 2^{n_s+1})} w_m(t)w_m(\theta). \end{aligned} \quad (\text{A.3})$$

Once we have verified this, the deduction is simple. Recall

$$S_n f(t) = \sum_{m=0}^{n-1} c_m(f) w_m(t) = \int_0^1 f(\theta) \sum_{m=0}^{n-1} w_m(\theta) w_m(t) d\theta.$$

To introduce the extraneous factor w_n which is critical to the identity (A.3), given any $f \in L^p[0, 1]$ we define the function $g(\theta) = f(\theta)w_n(\theta)$ with identical L^p norm; we will also use the notation $g_m = S_{2^m}g - S_{2^{m-1}}g$. Then using $w_n(\theta)^2 \equiv 1$ followed by (A.3),

$$w_n(t)(S_n f)(t) = \int_0^1 g(\theta)w_n(\theta)w_n(t) \sum_{m=0}^{n-1} w_m(\theta)w_m(t) d\theta = g_{n_1+1}(t) + \dots + g_{n_s+1}(t).$$

Now applying first the direct inequality and then the converse inequality for the functions $\{g_n\}$ we obtain the desired result:

$$\begin{aligned}\|S_n f\|_{L^p} &= \left\| \sum_{j=1}^s g_{n_j+1} \right\|_{L^p} \ll_p \left\| \left(\sum_{j=1}^s g_{n_j+1}^2 \right)^{1/2} \right\|_{L^p} \\ &\leq \left\| \left(\sum_{n=0}^{\infty} g_n^2 \right)^{1/2} \right\|_{L^p} \ll_p \|g\|_{L^p} = \|f\|_{L^p}.\end{aligned}$$

To verify (A.3), it suffices to observe an equivalent identity about sets of numbers written in binary (also expressible in terms of properties of the Walsh group or “dyadic group,” see [23, §2] or [3]). Precisely, fix n and $m \leq n$ and suppose $n = 2^{n_1} + \dots + 2^{n_s}$ (with $n_1 > \dots > n_s$) and $m = 2^{m_1} + \dots + 2^{m_r}$ (with $m_1 > \dots > m_r$), and let the $(n_1 + 1)$ -digit representation of n and m in binary be \underline{n} , \underline{m} , respectively. Then $w_n w_m = w_u$ where $\underline{u} = \underline{n} \oplus \underline{m}$; here \oplus denotes exclusive-or summation. (Since the square of any Rademacher function is identically one, if any exponent occurs in both the binary expansion of n and of m , then it does not appear as an exponent in the binary expansion of u for the function w_u such that $w_u = w_n w_m$.)

Consequently, (A.3) is equivalent to the following identity on sets of distinct binary numbers:

$$\{\underline{n} \oplus \underline{m} : 0 \leq m < n\} = \bigsqcup_{j=1}^s \{\underline{m} : 2^{n_j} \leq m < 2^{n_j+1}\}.$$

We can first verify that for $j = 1$, $\{\underline{n} \oplus \underline{m} : 0 \leq m < 2^{n_1}\} = \{\underline{m} : 2^{n_1} \leq m < 2^{n_1+1}\}$. This is because the map acting on $0 \leq m < 2^{n_1}$ by $m \mapsto \underline{n} \oplus \underline{m}$ is injective and maps into $\{\underline{m} : 2^{n_1} \leq m < 2^{n_1+1}\}$; since the cardinalities match, it is a bijection. Similarly, one can see that for each $2 \leq j \leq s$,

$$\{\underline{n} \oplus \underline{m} : 2^{n_1} + \dots + 2^{n_{j-1}} \leq m < 2^{n_1} + \dots + 2^{n_{j-1}} + 2^{n_j}\} = \{\underline{m} : 2^{n_j} \leq m < 2^{n_j+1}\},$$

and the claim holds.

In Remark 4.3, we claimed that while the functions $\{w_n\}$ are orthogonal, they do not themselves possess superorthogonality properties for $2r$ -tuples with $r \geq 2$. This referred to the fact that for any $r \geq 2$, we can pick $2r$ functions w_n with $2r$ distinct values of n (so the tuple (n_1, \dots, n_{2r}) satisfies the hypothesis of Type I or Type II or Type III) such that $\int w_{n_1} \cdots w_{n_{2r}} = 1$. Using the notation introduced above, this follows from the fact that we can choose $2r$ pairwise distinct integers n_1, \dots, n_{2r} such that when written in binary, $\underline{n}_1 \oplus \dots \oplus \underline{n}_{2r} = 0$.

Appendix B: The Source of Quasi-superorthogonality for Trace Functions

Appendix by Emmanuel Kowalski¹

This short note will attempt to explain the source of the quasi-superorthogonality of trace functions that appears in Sect. 7, and in particular it will highlight that it arises from “exact” superorthogonality (of the corresponding type) for other functions, combined with Deligne’s very deep work on the Riemann Hypothesis over finite fields. We then explain briefly the source of the exact superorthogonality in the type of examples considered in the survey [25] of Fouvry, Kowalski and Michel.

Remark The presentation is not fully rigorous, since we did not want to obscure the key conceptual point with technical aspects, such as the need to work with continuous ℓ -adic representations, etc.

Let q be a prime number. The key data is a certain compact topological group Π_q associated to q , with a normal subgroup Π_q^g (both are algebraic variants of the classical fundamental group of topology, but mainly viewed as classifying coverings of the space, instead of groups of homotopy classes of loops). Moreover, for every $x \in \mathbb{Z}/q\mathbb{Z}$, there exists a conjugacy class $\theta_q(x)$ in Π_q (called the *Frobenius* conjugacy class at x), and Π_q^g is big enough that it and a single Frobenius conjugacy class generate Π_q topologically.

A trace function F modulo q always has the following form: there exists a finite-dimensional vector space V on which Π_q acts linearly (i.e., a finite-dimensional representation of the group) in such a way that

$$F(x) = \text{tr}(\theta_q(x) \mid V), \quad (\text{B.1})$$

the trace of the endomorphism of V associated to the Frobenius conjugacy class at x . This is well-defined, since the trace is invariant under conjugation.

We view the action as a homomorphism $\varrho: \Pi_q \rightarrow \text{GL}(V)$. Then the formula (B.1) shows that *a trace function is the restriction of the character of a representation to a certain subset of conjugacy classes of that group*.²

The Grothendieck–Lefschetz trace formula combined with Deligne’s Riemann Hypothesis can then be shown to imply (for suitable trace functions) the statement that

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} F(x) = \left(\int_{\Pi_q^g} \text{tr}(\varrho(y)) dy \right) cq + O(\sqrt{q}), \quad (\text{B.2})$$

for some complex number c with $|c| \leq 1$, where the integral is with respect to the probability Haar measure on the compact group Π_q^g and the implied constant in the $O(\cdot)$ symbol depends only on “local” invariants of ϱ which are usually easy to bound.

¹ ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland. Email: kowalski@math.ethz.ch.

² To be more precise, this applies exactly in this way only when all $x \in \mathbb{Z}/q\mathbb{Z}$ are “unramified” for ϱ ; since exceptions to this are rare for the cases that interest us, and since there is in any case a similar (but slightly more complicated) description even when x is ramified, we do not dwell on this issue.

Remark In many cases of interest, one deals with an action of Π_q which has the property that $\varrho(\Pi_q^g) = \varrho(\Pi_q)$. Then (B.2) holds with $c = 1$, and thus it indicates that the discrete sum of the trace of ϱ over the finitely many Frobenius classes $\theta_q(x)$ is close to the integral over the whole group [note that $\varrho(\theta_q(x)) \in \Pi_q^g$ because of the assumption on ϱ]. However, the formula (B.2) holds in general in the stated form.

We can now explain how this, together with algebraic properties of certain compact Lie groups, leads to quasi-superorthogonality.

Suppose we have finitely many trace functions F_1, \dots, F_{2r} , each associated to a representation ϱ_i (on the space V_i), satisfying suitable conditions. We want to understand the sum

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} F_1(x) \overline{F_2(x)} \cdots F_{2r-1}(x) \overline{F_{2r}(x)}.$$

Part of the unspecified properties required of ϱ_i imply that the contragradient or dual representation $D(\varrho_i)$ of ϱ_i satisfies

$$\text{tr}(D(\varrho_i)(y)) = \overline{\text{tr}(\varrho_i(y))}.$$

So, according to (B.2), applied to the representation

$$\varrho = \varrho_1 \otimes D(\varrho_2) \otimes \cdots \otimes \varrho_{2r-1} \otimes D(\varrho_{2r}),$$

we get

$$\begin{aligned} & \sum_{x \in \mathbb{Z}/q\mathbb{Z}} F_1(x) \overline{F_2(x)} \cdots F_{2r-1}(x) \overline{F_{2r}(x)} \\ &= \left(\int_{\Pi_q^g} \text{tr}(\varrho_1(y)) \overline{\text{tr}(\varrho_2(y))} \cdots \text{tr}(\varrho_{2r-1}(y)) \overline{\text{tr}(\varrho_{2r}(y))} dy \right) c' q + O(\sqrt{q}), \end{aligned}$$

for some complex number c' with $|c'| \leq 1$.

Thus, we will obtain quasi-superorthogonality, of any type, for the trace functions, provided the characters $\text{tr}(\varrho_i)$ of the ϱ_i (restricted to the subgroup Π_q^g) satisfy *exact* superorthogonality of the same type.

We present now one source of such superorthogonality that lies behind many examples (but not all—for Dirichlet characters, such as in the inequality (7.9), the mechanism is a bit different).

In fact, at this point, we can replace Π_q^g by any fixed compact group G , with the ϱ_i being unitary (continuous) finite-dimensional representations of G .

According to the character theory of compact groups the integral

$$\int_G \text{tr}(\varrho_1(y)) \overline{\text{tr}(\varrho_2(y))} \cdots \text{tr}(\varrho_{2r-1}(y)) \overline{\text{tr}(\varrho_{2r}(y))} dy \tag{B.3}$$

is equal to the dimension of the space of invariant vectors in the tensor product representation ϱ . Now suppose that each V_i has dimension at least 2 and that the image of

each ϱ_i , which is a subgroup of the unitary group of the space V_i , happens to be the special unitary group $\mathrm{SU}(V_i)$. Consider the map

$$y \mapsto (\varrho_1(y), \dots, \varrho_{2r}(y))$$

from G to

$$\mathrm{SU}(V_1) \times \cdots \times \mathrm{SU}(V_{2r}).$$

Let H be its image. It is again a compact group, and it has the property that the projection of H to each factor $\mathrm{SU}(V_i)$ is surjective. Now a special case of what Katz [44, §1.8, Prop. 1.8.2] has called the Goursat–Kolchin–Ribet property is that such a subgroup H is *equal* to the product

$$\mathrm{SU}(V_1) \times \cdots \times \mathrm{SU}(V_{2r}),$$

unless at least two of the representations are equivalent, in which case at least two of the characters $\mathrm{tr}(\varrho_i)$ are the same functions. (To see that this may be the case, consider the special case where all V_i have different dimensions; then the groups $\mathrm{SU}(V_i)$ are pairwise non-isomorphic “almost” simple groups, and the projection assumption implies that the group H has to contain all of them as “Jordan–Hölder factors”, which is only possible if H is the full product.)

Thus, if no two of the characters are equal, then we have a splitting of the integral

$$\begin{aligned} & \int_G \mathrm{tr}(\varrho_1(y)) \overline{\mathrm{tr}(\varrho_2(y))} \cdots \mathrm{tr}(\varrho_{2r-1}(y)) \overline{\mathrm{tr}(\varrho_{2r}(y))} dy \\ &= \int_H \mathrm{tr}(y_1, y_2^*, \dots, y_{2r-1}, y_{2r}^*) dy_1 \cdots dy_{2r} \\ &= \left(\int_{\mathrm{SU}(V_1)} \mathrm{tr}(y_1) dy_1 \right) \cdots \left(\int_{\mathrm{SU}(V_{2r})} \overline{\mathrm{tr}(y_{2r})} dy_{2r} \right), \end{aligned}$$

which vanishes. In other words, in these conditions, we obtain superorthogonality of Type II, and in fact really in the same way suggested at the beginning of the paper, i.e., from independent random variables, these being the different characters $y \mapsto \mathrm{tr}(\varrho_i(y))$.

One can be more precise about conditions on the representations ϱ_i that lead to vanishing of the integral (B.3), but we hope that this sketch has given some idea of how this may arise.

References

1. Apostol, T.M.: Introduction to Analytic Number Theory, vol. I. Springer, New York (1976)
2. Bednorz, W.: A note on the Menchov–Rademacher inequality. Bull. Pol. Acad. **54**(1), 26–30 (2006)
3. Billard, P.: Sur la convergence presque partout des séries de Fourier–Walsh des fonctions de l'espace $L^2(0, 1)$. Studia Math. **28**, 363–388 (1967)

4. Bourgain, J., Chang, M.-C.: On a multilinear character sum of Burgess. *C. R. Acad. Sci. Paris* **I**(348), 115–120 (2010)
5. Bourgain, J., Demeter, C.: A study guide for the l^2 decoupling theorem. *Chin. Ann. Math. B* **38**(1), 173–200 (2017)
6. Bourgain, J., Demeter, C., Guth, L.: Proof of the main conjecture in Vinogradov’s mean value theorem for degrees higher than three. *Ann. Math.* (2) **184**(2), 633–682 (2016)
7. Bourgain, J.: An approach to pointwise ergodic theorems. In: *Geometric Aspects of Functional Analysis* (1986/87), Lecture Notes in Mathematics, vol. 1317, pp. 204–223. Springer, Berlin (1988)
8. Bourgain, J.: On the maximal ergodic theorem for certain subsets of the integers. *Isr. J. Math.* **61**, 39–72 (1988)
9. Bourgain, J.: On the pointwise ergodic theorem on L^p for arithmetic sets. *Isr. J. Math.* **61**, 73–84 (1988)
10. Bourgain, J.: Pointwise ergodic theorems for arithmetic sets. *Inst. Hautes Études Sci. Publ. Math.* (69):5–45 (with an Appendix by the author, Harry Furstenberg, Yitzhak Katznelson and Donald S, Ornstein) (1989)
11. Burgess, D.A.: The distribution of quadratic residues and non-residues. *Mathematika* **4**, 106–112 (1957)
12. Burgess, D.A.: On character sums and L -series. *J. Reine Angew. Math.* **3**(12), 193–206 (1962)
13. Burgess, D.A.: On character sums and L -series II. *Proc. Lond. Math. Soc.* **3**(13), 524–536 (1963)
14. Burgess, D.A.: The character sum estimate with $r = 3$. *J. Lond. Math. Soc.* **2**(33), 219–226 (1986)
15. Chang, M.-C.: On a question of Davenport and Lewis and new character sum bounds in finite fields. *Duke Math. J.* **145**(3), 409–442 (2008)
16. Chang, M.-C.: Burgess inequality in \mathbb{F}_{p^2} . *Geom. Funct. Anal.* **19**, 1001–1016 (2009)
17. Chang, M.-C.: An estimate of incomplete mixed character sums. In: *An Irregular Mind*, Bolyai Society Mathematics Studies, vol. 21, pp. 243–250. János Bolyai Mathematics Society, Budapest (2010)
18. Córdoba, A.: A note on Bochner–Riesz operators. *Duke Math. J.* **46**(3), 505–511 (1979)
19. Davenport, H., Erdős, P.: The distribution of quadratic and higher residues. *Publ. Math. Debr.* **2**, 252–265 (1952)
20. Davenport, H., Lewis, D.J.: Character sums and primitive roots in finite fields. *Rend. Circ. Mat. Palermo Ser. II Tomo XII Anno(1963)* **XII**, 129–136 (1963)
21. Deligne, P.: La conjecture de Weil II. *Inst. Hautes Études Sc. Publ. Math. No.* **52**, 137–252 (1980)
22. Doob, J.L.: *Stochastic Processes*. Wiley, New York (1953)
23. Fine, N.J.: On the Walsh functions. *Trans. Am. Math. Soc.* **65**, 372–414 (1949)
24. Fouvry, É., Ganguly, S., Kowalski, E., Michel, P.: Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions. *Comment. Math. Helv.* **89**(4), 979–1014 (2014)
25. Fouvry, É., Kowalski, E., Michel, P.: A study in sums of products. *Philos. Trans. R. Soc. A* **373**(2040), 1–26 (2015)
26. Fouvry, É., Kowalski, E., Michel, P., Raju, C.S., Rivat, J., Soundararajan, K.: On short sums of trace functions. *Ann. Inst. Fourier (Grenoble)* **167**(1), 423–449 (2017)
27. Fouvry, É., Kowalski, E., Michel, P., Sawin, W.: Lectures on applied ℓ -adic cohomology. *Contemp. Math.* **740**, 113–195 (2019)
28. Friedlander, J.B., Iwaniec, H., Mazur, B., Rubin, K.: The spin of prime ideals. *Invent. Math.* **193**(3), 697–749 (2013)
29. Gallagher, P.X., Montgomery, H.L.: A note on Burgess’s estimate. *Math. Notes* **88**, 321–329 (2010)
30. Gressman, P.T., Guo, S., Pierce, L.B., Roos, J., Yung, P.-L.: Reversing a philosophy: from counting to square functions and decoupling. *J. Geom. Analysis* (2020). [arXiv:1906.05877](https://arxiv.org/abs/1906.05877)
31. Gressman, P.T.: Geometric averaging operators and nonconcentration inequalities (2019). [arXiv:1906.04599](https://arxiv.org/abs/1906.04599)
32. Haagerup, U.: The best constants in the Khintchine inequality. *Studia Math.* **70**(3), 231–283 (1981)
33. Harper, A., Nikeghbali, A., Radziwiłł, M.: A note on Helson’s conjecture on moments of random multiplicative functions. In: *Analytic Number Theory*. Springer, Cham (2015)
34. Heap, W., Lindqvist, S.: Moments of random multiplicative functions and truncated characteristic polynomials. *Q. J. Math.* **67**(4), 683–714 (2015)
35. Heath-Brown, D.R.: Burgess’s bounds for character sums. *Proc. Math. Stat.* **43**, 199–213 (2012)
36. Heath-Brown, D.R.: Small solutions of quadratic congruences, and character sums with binary quadratic forms. *Mathematika* **62**, 551–571 (2016)
37. Heath-Brown, D.R., Pierce, L.B.: Burgess bounds for short mixed character sums. *J. Lond. Math. Soc.* (2) **91**(3), 693–708 (2015)

38. Ionescu, A.D., Wainger, S.: L^p boundedness of discrete singular Radon transforms. *J. Am. Math. Soc.* **19**(2), 357–383 (2005)
39. Iwaniec, H., Kowalski, E.: *Analytic Number Theory*, vol. 53. Amer. Math. Soc. Colloquium Publications, Providence RI (2004)
40. Kac, M.: *Statistical Independence in Probability, Analysis, and Number Theory*. The Mathematical Association of America, Washington, DC (1964)
41. Kaczmarz, S.: Über ein Orthogonalsystem. In: *Comptes rendus du premier congrès des math. des pays slaves* (Varsovie), pp. 189–192 (1929)
42. Kaczmarz, S., Steinhaus, H.: Le système orthogonal de M. Rademacher. *Studia Math.* **2**(1), 231–247 (1930)
43. Kaczmarz, S., Steinhaus, H.: *Theorie der Orthogonalreihen*. Instytut Matematyczny Polskiej Akademii Nauk, Warszawa-Lwów (1936)
44. Katz, N.M.: *Exponential Sums and Differential Equations*. Annals of Mathematics Studies, vol. 124. Princeton University Press, Princeton (1990)
45. Kowalski, E., Ricotta, G.: Fourier coefficients of $GL(N)$ automorphic forms in arithmetic progressions. *Geom. Funct. Anal.* **24**(4), 1229–1297 (2014)
46. Magyar, A., Stein, E.M., Wainger, S.: Discrete analogues in harmonic analysis: spherical averages. *Ann. Math.* **155**, 189–208 (2002)
47. Menchov, D.: Sur les séries de fonctions orthogonales. *Fundam. Math.* **1**, 82–105 (1923)
48. Mirek, M., Stein, E.M., Zorin-Kranich, P.: Jump inequalities for translation-invariant operators of Radon type on \mathbb{Z}^d (2018). [arXiv:1809.03803](https://arxiv.org/abs/1809.03803)
49. Paley, R.E.A.C.: A remarkable series of orthogonal functions (I). *Proc. Lond. Math. Soc.* (2) **34**(4), 241–264 (1932)
50. Paley, R.E.A.C., Zygmund, A.: On some series of functions. *Math. Proc. Camb. Philos. Soc.* **26**(3), 337–357 (1930)
51. Petrow, I., Young, M.P.: The fourth moment of Dirichlet L -functions along a coset and the Weyl bound (2019). [arXiv:1908.10346](https://arxiv.org/abs/1908.10346)
52. Pierce, L.B.: Burgess bounds for multi-dimensional short mixed character sums. *J. Number Theory* **163**, 172–210 (2016)
53. Pierce, L.B.: The Vinogradov mean value theorem [after Wooley, and Bourgain, Demeter and Guth]. Number 407, Exp. No. 1134. In: *Séminaire Bourbaki*, vol. 2016/2017. Exposés 1120–1135, pp. 479–564 (2019)
54. Pierce, L.B.: Burgess bounds for short character sums evaluated at forms II: the mixed case. *Riv. Mat. Univ. di Parma* (2020). [arXiv:2002.03435](https://arxiv.org/abs/2002.03435)
55. Pierce, L.B., Xu, J.: Burgess bounds for short character sums evaluated at forms. *Algebra Number Theory* **14**, 1911–1951 (2020)
56. Pólya, G.: Über die Verteilung der quadratischen Reste und Nichtreste, pp. 21–29. *Göttinger Nachrichten* (1918)
57. Rademacher, H.: Einige Sätze über Reihen von allgemeinen Orthogonal-Funktionen. *Math. Ann.* **87**, 112–138 (1922)
58. Rubio de Francia, J.L.: A Littlewood–Paley inequality for arbitrary intervals. *Rev. Mat. Iberoam.* **1**(2), 1–14 (1985)
59. Sjölin, P.: An inequality of Paley and convergence ae of Walsh–Fourier series. *Ark. Mat.* **7**, 551–570 (1969)
60. Stein, E.M.: On limits of sequences of operators. *Ann. Math.* **2**(74), 140–170 (1961)
61. Stein, E.M.: *Singular Integrals and Differentiability Properties of Functions*. Princeton University Press, Princeton (1970)
62. Stein, E.M.: *Harmonic Analysis: Real-Variable Methods, Orthogonality, and Oscillatory Integrals*. Princeton University Press, Princeton (1993)
63. Thiele, C.M.: Time–frequency analysis in the discrete phase plane. ProQuest LLC, Ann Arbor, MI, 1995. Thesis (PhD), Yale University
64. Vinogradov, I.M.: Sur la distribution des résidus et des nonrésidus des puissances. *J. Soc. Phys. Math. Soc. Univ. Permi* **1**, 94–96 (1918)
65. Vinogradov, I.M.: On a general theorem concerning the distribution of the residues and non-residues of powers. *Trans. Am. Math. Soc.* **29**, 209–217 (1927)
66. Walsh, J.L.: A closed set of normal orthogonal functions. *Am. J. Math.* **45**, 5–24 (1923)
67. Weil, A.: On the Riemann hypothesis in function fields. *Proc. Nat. Acad. Sci. USA* **27**, 345–347 (1941)

68. Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent. *Actualités Math. et Sci.*, 1041(Deuxième partie,):§IV, (1945)
69. Wintner, A.: Random factorizations and Riemann's hypothesis. *Duke Math. J.* **11**, 267–275 (1944)
70. Wolff, T.H.: In: Łaba, I., Shubin, C. (eds) *Lectures on Harmonic Analysis*, University Lecture Series, vol. 29. AMS, Providence (2003) (with a foreword by C. Fefferman and preface by I. Łaba)
71. Zygmund, A.: *Trigonometric Series, Volumes I and II*, 3rd edn. Cambridge University Press, Cambridge (2002)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.