1-1-2011

Explicit Constructions of RIP Matrices and Related Problems

Jean Bourgain
Institute for Advanced Study, bourgain@math.ias.edu

S J. Dilworth
University of South Carolina - Columbia, dilworth@math.sc.edu

Kevin Ford
University of Illinois at Urbana-Champaign, ford@math.uiuc.edu

Sergei Konyagin
Steklov Mathematical Institute, konyagin@mi.ras.ru

Denka Kutzarova
University of Illinois at Urbana-Champaign, denka@math.uiuc.edu

Publication Info

Published in *Duke Mathematical Journal*, Volume 159, Issue 1, 2011, pages 145-185.
Bourgain, J., Dilworth, S. J., Ford, K., Konyagin, S., & Kutzarova, D. (2011). Explicit Constructions of RIP Matrices and Related Problems. *Duke Mathematical Journal, 159* (1), 145-185.

EXPLICIT CONSTRUCTIONS OF RIP MATRICES AND RELATED PROBLEMS

JEAN BOURGAIN, STEPHEN DILWORTH, KEVIN FORD,
SERGEI KONYAGIN, and DENKA KUTZAROVA

Abstract

We give a new explicit construction of $n \times N$ matrices satisfying the Restricted Isometry Property (RIP). Namely, for some $\varepsilon > 0$, large N, and any n satisfying $N^{1-\varepsilon} \le n \le N$, we construct RIP matrices of order $k \ge n^{1/2+\varepsilon}$ and constant $\delta = n^{-\varepsilon}$. This overcomes the natural barrier $k = O(n^{1/2})$ for proofs based on small coherence, which are used in all previous explicit constructions of RIP matrices. Key ingredients in our proof are new estimates for sumsets in product sets and for exponential sums with the products of sets possessing special additive structure. We also give a construction of sets of n complex numbers whose kth moments are uniformly small for $1 \le k \le N$ (Turán's power sum problem), which improves upon known explicit constructions when $(\log N)^{1+o(1)} \le n \le (\log N)^{4+o(1)}$. This latter construction produces elementary explicit examples of $n \times N$ matrices that satisfy the RIP and whose columns constitute a new spherical code; for those problems the parameters closely match those of existing constructions in the range $(\log N)^{1+o(1)} \le n \le (\log N)^{5/2+o(1)}$.

Contents

DUKE MATHEMATICAL JOURNAL
Vol. 159, No. 1, © 2011 DOI 10.1215/00127094-1384809
Received 5 May 2010. Revision received 29 July 2010.
2010 *Mathematics Subject Classification*. Primary 11T23; Secondary 11B13, 11B30, 41A46, 94A12, 94B60.
Bourgain's work partially supported by National Science Foundation grants DMS 0808042 and DMS 0835373.
Dilworth's work supported by National Science Foundation grant DMS 0701552 and by the Workshop in Analysis and Probability.
Ford's work supported by National Science Foundation grant DMS 0901339, by the Workshop in Analysis and Probability, and by grants from the Ellentuck Fund and Friends of the Institute for Advanced Study.
Kutzarova's work supported by the Workshop in Analysis and Probability.

1. Introduction

Suppose that $1 \le k \le n \le N$ and $0 < \delta < 1$. A *signal* $\mathbf{x} = (x_j)_{j=1}^N \in \mathbb{C}^N$ is said to be k*-sparse* if $\mathbf{x}$ has at most k nonzero coordinates. An $n \times N$ matrix Φ is said to satisfy the RIP of order k with constant δ if, for all k-sparse vectors $\mathbf{x}$, we have

$$(1-\delta)\|\mathbf{x}\|_2^2 \le \|\Phi\mathbf{x}\|_2^2 \le (1+\delta)\|\mathbf{x}\|_2^2. \tag{1.1}$$

While most authors work with real signals and matrices, in this paper we work with complex matrices for convenience. Given a complex matrix Φ satisfying (1.1), the $2n \times 2N$ real matrix Φ', formed by replacing each element $a + ib$ of Φ by the 2×2 matrix $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$, also satisfies (1.1) with the same parameters k, δ.

We know from Candès, Romberg, and Tao that matrices satisfying the RIP have application to sparse signal recovery (see [13], [14], [15]). A variant of the RIP (with the ℓ_2 norm in (1.1) replaced by the ℓ_1 norm) is also useful for such problems (see [8]). A weak form of the RIP, where (1.1) holds for most k-sparse $\mathbf{x}$ (called *statistical RIP*), is studied in [22]. Other applications of RIP matrices may be found in [30] and [34].

Given n, N, δ, we wish to find $n \times N$ RIP matrices of order k with constant δ, and with k as large as possible. If the entries of Φ are independent Bernoulli random variables with values $\pm 1/\sqrt{n}$, then there is a high probability Φ will have the required properties for*

$$k \asymp \delta \frac{n}{\log(2N/n)}. \tag{1.2}$$

See [14], [32]; see also [6] for a proof based on the Johnson-Lindenstrauss lemma [25, Lemma 1]. The first result of similar type for these matrices is due to Kashin [27]. See also [16], [40] for RIP matrices with rows randomly selected from the rows of a discrete Fourier transform matrix and for other random constructions of RIP matrices. The parameter k cannot be taken larger; in fact, we have

$$k \ll \delta \frac{n}{\log(2N/n)}$$

for every RIP matrix (see [35]).

*For convenience, we utilize the Vinogradov notation $a \ll b$, which means $a = O(b)$, and the Hardy notation $a \asymp b$, which means $b \ll a \ll b$.

It is an open problem to find good *explicit* constructions of RIP matrices (see Tao's weblog [43] for a discussion of the problem). We mention here that all known explicit examples of RIP matrices are based on constructions of systems of unit vectors (the columns of the matrix) with small *coherence*.

The *coherence parameter* μ of a collection of unit vectors $\{\mathbf{u}_1, \ldots, \mathbf{u}_N\} \subset \mathbb{C}^n$ is defined by

$$\mu := \max_{r \neq s} |\langle \mathbf{u}_r, \mathbf{u}_s \rangle|. \tag{1.3}$$

Matrices whose columns are unit vectors with small coherence are connected to a number of well-known problems, a few of which we describe below. Systems of vectors with small coherence are also known as *spherical codes*. Some other applications of matrices with small coherence may be found in [18], [20], [31].

PROPOSITION 1
Suppose that $\mathbf{u}_1, \ldots, \mathbf{u}_N$ *are the columns of a matrix* Φ *and have coherence* μ. *Then* Φ *satisfies the RIP of order* k *with constant* $\delta = (k-1)\mu$.

Proof
For any k-sparse vector $\mathbf{x}$,

$$\begin{aligned} \big| \|\Phi \mathbf{x}\|_2^2 - \|\mathbf{x}\|_2^2 \big| &\le 2 \sum_{r<s} |x_r x_s \langle \mathbf{u}_r, \mathbf{u}_s \rangle| \\ &\le \mu \Big(\Big(\sum |x_j| \Big)^2 - \|\mathbf{x}\|_2^2 \Big) \le (k-1)\mu \|\mathbf{x}\|_2^2. \end{aligned} \qquad \square$$

All explicit constructions of matrices with small coherence are based on number theory. There are many constructions producing matrices with

$$\mu \ll \frac{\log N}{\sqrt{n} \log n}. \tag{1.4}$$

In particular, such examples have been constructed by Kashin [26]; Alon, Goldreich, Håstad, and Peralta [2]; DeVore [17]; and Nelson and Temlyakov [35]. By Proposition 1, these matrices satisfy the RIP with constant δ and order

$$k \asymp \delta \frac{\sqrt{n} \log n}{\log N}. \tag{1.5}$$

It follows from random constructions of Erdős and Rényi for Turán's problem (see Proposition 2 and (1.15) below) that, for any n, N, there are vectors with coherence

$$\mu \ll \sqrt{\frac{\log N}{n}}.$$

By contrast, there is a universal lower bound

$$\mu \gg \Big(\frac{\log N}{n\log(n/\log N)}\Big)^{1/2} \geq \frac{1}{\sqrt{n}} \tag{1.6}$$

valid for $2\log N \leq n \leq N/2$ and all Φ, due to Levenshtein [29] (see also [21] and [35]). Therefore, by estimating RIP parameters in terms of the coherence parameter, we cannot construct $n \times N$ RIP matrices of order larger than $\sqrt{n}$ and constant $\delta < 1$.

Using methods of additive combinatorics, we construct RIP matrices of order k with $n = o(k^2)$.

THEOREM 1
There is an effective constant $\varepsilon_0 > 0$ and an explicit number n_0 such that, for any positive integers $n \geq n_0$ and $n \leq N \leq n^{1+\varepsilon_0}$, there is an explicit $n \times N$ RIP matrix of order $\lfloor n^{1/2+\varepsilon_0}\rfloor$ with constant $n^{-\varepsilon_0}$.

Remark 1
For application to sparse signal recovery, it is sufficient to take fixed $\delta < \sqrt{2}-1$ (see [13]); one also needs an upper bound on n in terms of k, N. By Theorem 1, for some $\varepsilon_0' > 0$, large N, and $N^{1/2-\varepsilon_0'} \leq k \leq N^{1/2+\varepsilon_0'}$, we construct explicit RIP matrices with $n \leq k^{2-\varepsilon_0'}$.

The proof of Theorem 1 uses a result on additive energy of sets (see Corollary 2, Theorem 4), estimates for sizes of sumsets in product sets (see Theorem 5), and bounds for exponential sums over products of sets possessing special additive structure (see Lemma 10).

We now return to the problem of constructing matrices with small coherence. By (1.6), the bound (1.4) cannot be improved if $\log n \gg \log N$, but there is a gap between bounds (1.6) and (1.4) when $\log n = o(\log N)$. For example, (1.4) is nontrivial only for $n \gg (\log N/\log\log N)^2$. Of particular interest in coding theory is the range $n = O(\log^C N)$ for fixed C, where some improvements have been made to (1.4). A construction obtained by concatenating algebraic-geometric codes with Hadamard codes (see, e.g., [23, Corollary 3] and [7, Section 3]) produces matrices with coherence

$$\mu \ll \Big(\frac{\log N}{n\log(n/\log N)}\Big)^{1/3}, \tag{1.7}$$

which is nontrivial for $n \gg \log N$, and is better than (1.4) when $\log N \ll n \ll (\log N/\log\log N)^4$. In the range $(\log N/\log\log N)^{5/2} \ll n \ll (\log N/\log\log N)^5$, Ben-Aroya and Ta-Shma [7] improved both (1.4) and (1.7) by constructing binary codes (vectors with entries $\pm 1/\sqrt{n}$) with coherence

$$\mu \ll \left(\frac{\log N}{n^{4/5}\log\log N}\right)^{1/2}. \tag{1.8}$$

In this paper, we introduce very elementary constructions of matrices with coherence which matches (up to a $\log\log N$ factor) the bound (1.7). Our constructions, which are based on a method of Ajtai, Iwaniec, Komlós, Pintz, and Szemerédi [1], have the added utility of applying to Turán's power-sum problem and to the problem of finding thin sets with small Fourier coefficients. For these last two problems, our construction gives better estimates than existing explicit constructions in certain ranges of the parameters.

Roughly speaking, a set with small Fourier coefficients can be used to construct a set of numbers for Turán's problem, and a set of numbers in Turán's problem can be used to produce a matrix with small coherence. This is made precise below.

We next describe the problem of explicitly constructing thin sets with small Fourier coefficients. If N is a positive integer and if S is a set (or multiset) of residues modulo N, we let

$$f_S(k) = \sum_{s\in S} e^{2\pi i k s/N}$$

and

$$|f_S| := \frac{1}{|S|}\max_{1\le k\le N-1} |f_S(k)|.$$

Given N, we wish to find a small set S with $|f_S|$ also small.

Turán's problem (see [45]) concerns the estimation of the function

$$T(n,N) = \min_{|z_1|=\cdots=|z_n|=1} M_N(\mathbf{z}), \qquad M_N(\mathbf{z}) := \max_{k=1,\dots,N}\left|\sum_{j=1}^{n} z_j^k\right|,$$

where n, N are positive integers. There is a vast literature related to Turán's problem (see, e.g., [3], [4], [33, Chapter 5], [41], [42]).

If $S = \{t_1, \dots, t_n\}$ is a multiset of integers modulo N and if $z_j = e^{2\pi i t_j/N}$ for $1 \le j \le n$, we see that

$$T(n, N-1) \le M_{N-1}(\mathbf{z}) \le n|f_S|. \tag{1.9}$$

We also have the following easy connection between Turán's problem and coherence.

PROPOSITION 2
Given any vector $\mathbf{z} = (z_1, \ldots, z_n)$ *with* $|z_j| = 1$ *for all* j, *the coherence* μ *of the* $n \times N$ *matrix with the columns*

$$\mathbf{u}_k^{-1/2}(z_1^{k-1}, \ldots, z_n^{k-1})^T, \quad k = 1, \ldots, N \tag{1.10}$$

satisfies $\mu = n^{-1} M_{N-1}(\mathbf{z})$.

Combining (1.9) and Proposition 2, for any multiset S of residues modulo N, the vectors (1.10) satisfy

$$\mu \le |f_S|. \tag{1.11}$$

A corollary of a character sum estimate of Katz [28] (see also [36]) shows* that for certain N and $1/N \le \mu \le 1$, there are (explicitly defined) sets T of residues modulo N so that

$$|f_T| \le \mu, \qquad |T| = O\Big(\frac{\log^2 N}{\mu^2(\log\log N + \log(1/\mu))}\Big). \tag{1.12}$$

An application of Dirichlet's approximation theorem shows that a set S with $|S| < \log N$ must have $|f_S| \gg 1$. In [1], sets which are not much larger are explicitly constructed so that $|f_S|$ is small. Specifically, by [1, (1), (2)], for each prime† N there is a set S with $|S| = O(\log N(\log^* N)^{13\log^* N})$ and

$$|f_S| = O(1/\log^* N),$$

where $\log^* N$ is the integer k so that the kth iterate of the logarithm of N lies in $[1, e)$. The proof uses an iterative procedure. By modifying this procedure and truncating after two steps, we prove the following. To state our results, for brevity we write

$$L_1 = \log N, \qquad L_2 = \log\log N, \qquad L_3 = \log\log\log N.$$

THEOREM 2
For sufficiently large prime N *and* μ *such that*

$$\frac{L_2^4}{L_1} \le \mu < 1, \quad 1/\mu \in \mathbb{N}, \tag{1.13}$$

*Here we take $N = p^d - 2$, where p is prime, $p \approx ((d-1)/\mu)^2$ and $((d-1)\mu^{-1})^{2d} \approx N$. Let $F = \mathbb{F}_{p^d}$. The group of characters on F is a cyclic group of order $N+1$ with generator χ_1. For any $x \in F \setminus \{0\}$ write $\chi_1(x) = e(t_x/N)$. Let x be an element of F not contained in any proper subfield of F and take $T = \{t_{x+j} : j = 0, \ldots, p-1\}$. Then $|T| = p$, and $|f_T| \le (d-1)\sqrt{p}$ by [28].

†A corresponding result when N is composite is given in [38].

a set S of residues modulo N can be explicitly constructed so that

$$|f_S| \le \mu \qquad \text{and} \qquad |S| = O\Big(\frac{L_1 L_2 \log(2/\mu)}{\mu^4 (L_3 + \log(1/\mu))}\Big) = O\Big(\frac{L_1 L_2}{\mu^4}\Big).$$

Remark 2

The method from [1], if applied without modification (with two iterations of the basic lemma), produces a conclusion in Theorem 2 with

$$|S| = O\Big(\frac{L_1 L_2}{\mu^8 L_3}\Big).$$

Remark 3

The bound on $|S|$ in Theorem 2 is better than (1.12) for $\mu \gg L_1^{-1/2} L_2$.

Together, the construction for Theorem 2 and (1.9) give explicit sets $\mathbf{z}$ for Turán's problem. By further modifying the construction, we can do better.

THEOREM 3

For sufficiently large positive integer N and μ such that

$$\frac{L_2^3}{L_1} \le \mu < 1, \tag{1.14}$$

a multiset $\mathbf{z} = \{z_1, \dots, z_n\}$ such that $|z_1| = \cdots = |z_n| = 1$ can be explicitly constructed so that

$$M_N(\mathbf{z}) \le \mu n, \qquad n = O\Big(\frac{L_1 L_2 \log(2/\mu)}{\mu^3 (L_3 + \log(1/\mu))}\Big) = O\Big(\frac{L_1 L_2}{\mu^3}\Big).$$

To put Theorem 3 in context, we briefly review what is known about $T(n, N)$. Erdős and Rényi [19] used probabilistic methods to prove an upper estimate

$$T(n, N) \le \big(6n \log(N+1)\big)^{1/2}. \tag{1.15}$$

Using the character sum bound of Katz [28], Andersson [5] gave explicit examples of sets $\mathbf{z}$ which give

$$T(n, N) \le M_N(\mathbf{z}) \ll \frac{\sqrt{n} \log N}{\log n}. \tag{1.16}$$

One can see that (1.16) supersedes (1.15) for $\log N \ll \log^2 n$. Also, combining (1.16) with Proposition 2 provides yet another construction of matrices with coherence satisfying (1.4). On the other hand, by (1.6) and Proposition 2, we have the lower estimate

$$T(n, N) \gg \left(\frac{n \log N}{\log(n/\log N)}\right)^{1/2} \gg n^{1/2}, \qquad (2 \log N \le n \le N/2).$$

By comparison, the constructions in Theorem 3 are better than (1.16) in the range $n \ll L_1^4/L_2^8$, that is, throughout the range (1.14) (our constructions require n to be prime, however).

The constructions in Theorem 3 also produce, by Proposition 2, explicit examples of matrices with coherence

$$\mu \ll \left(\frac{L_1 L_2}{n}\right)^{1/3},$$

which is close to the bound (1.7). By Proposition 1, these matrices satisfy the RIP with constant δ and order

$$k \gg \delta\left(\frac{n}{L_1 L_2}\right)^{1/3}.$$

We prove Theorem 1 in Sections 2–6, Theorem 2 in Section 7, and Theorem 3 in Section 8.

2. Construction of the matrix in Theorem 1

We fix a large even number m. A value of m can be specified; it depends on the constant c_0 in an estimate from additive combinatorics (see Proposition 3, Section 4). Also, the value m can be reduced if one proves a better version of the Balog-Szemerédi-Gowers lemma (Lemma 6 below).

For sufficiently large n, we take the largest prime $p \le n$, which satisfies $p \ge n/2$ by Bertrand's postulate. By $\mathbb{F}_p$ we denote the field of the residues modulo p, and we let $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. For $x \in \mathbb{F}_p$, let $e_p(x) = e^{2\pi i x/p}$. We construct an appropriate $p \times N$ matrix Φ_p with columns $\mathbf{u}_{a,b}$, $a \in \mathcal{A} \subset \mathbb{F}_p$, $b \in \mathcal{B} \subset \mathbb{F}_p$, where

$$\mathbf{u}_{a,b} = \frac{1}{\sqrt{p}}\big(e_p(ax^2 + bx)\big)_{x \in \mathbb{F}_p}$$

(the sets $\mathcal{A}$, $\mathcal{B}$ are defined below). Notice that the matrix Φ_p can be extended to an $n \times N$ matrix Φ by adding $n - p$ rows of zeros. Clearly, the matrices Φ_p and Φ have the same RIP parameters.

We take

$$\alpha = \frac{1}{8m^2}, \quad L = \lfloor p^\alpha \rfloor, \quad U = L^{4m-1}, \qquad \mathcal{A} = \{x^2 + Ux : 1 \le x \le L\}. \quad (2.1)$$

To define the set $\mathcal{B}$, we take

$$\beta = \alpha/2 = 1/(16m^2), \qquad r = \left\lfloor \frac{\beta \log p}{\log 2} \right\rfloor, \qquad M = 2^{(1/\beta)-1} = 2^{16m^2-1},$$

and we let

$$\mathcal{B} = \left\{ \sum_{j=1}^{r} x_j (2M)^{j-1} \,:\, x_1, \ldots, x_r \in \{0, \ldots, M-1\} \right\}.$$

We notice that all elements of $\mathcal{B}$ are at most $p/2$ and that

$$|\mathcal{B}| \asymp p^{1-\beta}. \tag{2.2}$$

It follows from (2.1) and (2.2) that

$$|\mathcal{A}||\mathcal{B}| \asymp p^{1+\beta} \asymp n^{1+\beta}.$$

For $n \le N \le n^{1+\beta/2}$, take Φ to be the matrix formed by the first N columns of Φ_p, padded with $n - p$ rows of zeros.

In the next four sections, we show that Φ has the required properties for Theorem 1. First, in Section 3, we show that in (1.1) we need only consider vectors $\mathbf{x}$ whose components are zero or 1 (*flat* vectors). We prove the following.

LEMMA 1
Let $k \ge 2^{10}$, and let s be a positive integer. Assume that the coherence parameter of the matrix Φ is $\mu \le 1/k$. Also, assume that for some $\delta \ge 0$ and any disjoint $J_1, J_2 \subset \{1, \ldots, N\}$ with $|J_1| \le k$, $|J_2| \le k$, we have

$$\left| \left\langle \sum_{j \in J_1} \mathbf{u}_j, \sum_{j \in J_2} \mathbf{u}_j \right\rangle \right| \le \delta k.$$

Then Φ satisfies the RIP of order $2sk$ with constant $44s\sqrt{\delta}\log k$.

Our main lemma concerns showing the RIP with flat vectors and order $k = \lfloor \sqrt{p} \rfloor$. We prove the required estimates for matrices formed from more general sets $\mathcal{A}$ and $\mathcal{B}$ having certain additive properties. Namely, let $m \in 2\mathbb{N}$, and let $0 < \alpha < 0.01$. Assume that

$$|\mathcal{A}| \le p^\alpha \tag{2.3}$$

and, for $a \in \mathcal{A}$ and $a_1, \ldots, a_{2m} \in \mathcal{A} \setminus \{a\}$, that

$$\sum_{j=1}^{m} \frac{1}{a - a_j} = \sum_{j=m+1}^{2m} \frac{1}{a - a_j} \implies (a_1, \ldots, a_m) \text{ is a permutation of } (a_{m+1}, \ldots, a_{2m}). \tag{2.4}$$

Here we write $1/x$ for the multiplicative inverse of $x \in \mathbb{F}_p$. We will consider the sets $\mathcal{B}$ satisfying

$$\forall S \subset \mathcal{B}, \quad \text{if} \quad |S| \geq p^{1/3}, \quad \text{then} \quad E(S, S) \leq p^{-\gamma} |S|^3 \tag{2.5}$$

with some $\gamma > 0$, where $E(S, S)$ is the number of solutions of $s_1 + s_2 = s_3 + s_4$ with each $s_i \in S$.

LEMMA 2
Let $m \in 2\mathbb{N}$, let $\alpha \in (0, 0.01)$, let $0 < \gamma \leq \min(\alpha, 1/3m)$, let p be sufficiently large in terms of m, α, γ, let $\mathcal{A}$ satisfy (2.3) and (2.4), and let $\mathcal{B}$ satisfy (2.5). Then for any disjoint sets $\Omega_1, \Omega_2 \subset \mathcal{A} \times \mathcal{B}$ such that $|\Omega_1| \leq \sqrt{p}$, $|\Omega_2| \leq \sqrt{p}$, the inequality

$$\Big| \sum_{(a_1,b_1)\in\Omega_1} \sum_{(a_2,b_2)\in\Omega_2} \big\langle \mathbf{u}_{a_1,b_1}, \mathbf{u}_{a_2,b_2} \big\rangle \Big| \leq p^{1/2-\varepsilon_1}$$

holds, where $\varepsilon_1 = c_0\gamma/20 - 43\alpha/m$.

The proof of Lemma 2 is quite involved, and will be handled in three subsequent sections. We next demonstrate how Theorem 1 may be deduced from it.

We first prove (2.4) for the specific set $\mathcal{A}$ defined in (2.1), provided that $p > (2m)^{8m^2}$ (and thus $L \geq 2m$). We have to show that, for any distinct $x, x_1, \ldots, x_n \in \{1, \ldots, L\}$ and any nonzero integers $\lambda_1, \ldots, \lambda_n$ such that $n \geq 2m$ and $|\lambda_1| + \cdots + |\lambda_n| \leq 2m$, the sum

$$V = \sum_{j=1}^{n} \frac{\lambda_j}{(x - x_j)(x + x_j + U)}$$

is a nonzero element of $\mathbb{F}_p$. However, we will treat V as a rational number. Denote

$$D_1 = \prod_{j=1}^{n} (x - x_j), \qquad D_2 = \prod_{j=1}^{n} (x + x_j + U).$$

So, we have

$$D_1 D_2 V = \sum_{j=1}^{n} \frac{\lambda_j D_1}{x - x_j} \frac{D_2}{x + x_j + U}. \tag{2.6}$$

All the summands in the right-hand side of (2.6) except the first one are divisible by $x + x_1 + U$. For the first summand, we have

$$\frac{\lambda_1 D_1}{x - x_1} \frac{D_2}{x + x_1 + U} \equiv V_1 \pmod{x_0 + x_1 + U},$$

where

$$V_1 = \lambda_1 \prod_{j=2}^{n} (x - x_j) \prod_{j=2}^{n} (x_j - x_1).$$

We have

$$|V_1| \leq 2mL^{2n-2} \leq 2mL^{4m-2} \leq L^{4m-1} = U < U + x_0 + x_1.$$

This shows that $V_1 \neq 0 \pmod{x_0 + x_1 + U}$. Therefore, $V \neq 0$. By assumption, $p \nmid D_1$ and

$$|D_2 V| \leq 2m(U + 2L)^n / U \leq 4mU^{2m-1} \leq U^{2m} < p.$$

Hence $p \nmid D_1 D_2 V$, as desired.

Condition (2.5) is satisfied due to Corollary 4 of Section 5 with $\gamma = \beta/50$. If $m > 86000c_0^{-1}$, then Lemma 2 gives a nontrivial estimate with $\varepsilon_1 > 0$. Thus, Φ_p satisfies the conditions of Corollary 1 with $k = \lfloor \sqrt{p} \rfloor \geq \sqrt{n/2}$ and $\delta = p^{-\varepsilon_1} \leq (n/2)^{-\varepsilon_1}$ (using $p \geq 0.9n$ for large n, which follows from the prime number theorem). Let $\varepsilon_0 = \varepsilon_1/5$. Let $n \leq N \leq n^{1+\varepsilon_0}$ and let Φ be the $n \times N$ matrix formed by taking the first N columns of Φ_p and then adding $n - p$ rows of zeros. Clearly, Φ satisfies the conditions of Corollary 1 with the same parameters as Φ_p. By Lemma 1 with $s = \lfloor p^{\varepsilon_1/4} \rfloor$, Theorem 1 follows.

In Section 4, we introduce some notation and recall standard estimates in additive combinatorics which will be applied to subsets of $\mathcal{B}$. Section 5 is devoted to the sumset theory of $\mathcal{B}$, from which we deduce (2.5). The completion of the proof of Lemma 2 is in Section 6. We give some preliminaries here.

It is easy to see that, for a fixed a, the vectors $\{u_{a,b} : b \in \mathbb{F}_p\}$ form an orthogonal system. Using a well-known formula for Gauss sums $\sum_{x \in \mathbb{F}_p} e_p(dx^2)$ (see, e.g., [24, Proposition 6.31]), we have, for $a_1 \neq a_2$, the equality

$$\langle \mathbf{u}_{a_1,b_1}, \mathbf{u}_{a_2,b_2} \rangle = p^{-1} e_p\Big(-\frac{(b_1-b_2)^2}{4(a_1-a_2)} \Big) \sum_{x \in \mathbb{F}_p} e_p\big((a_1-a_2)x^2 \big)$$

$$= \frac{\sigma_p}{\sqrt{p}} \Big(\frac{a_1-a_2}{p} \Big) e_p\Big(-\frac{(b_1-b_2)^2}{4(a_1-a_2)} \Big),$$

where $(\frac{d}{p})$ is the Legendre symbol* and where $\sigma_p = 1$ or i according to whether $p \equiv 1$ or $3 \pmod 4$. We remark that there is no analogous formula for exponential sums $\sum_{x \in \mathbb{F}_p} e_p(F(x))$ when F is a polynomial of degree greater than or equal to 3. Consequently, the assertion of Lemma 2 can be rewritten as

$$\Big| \sum_{(a_1,b_1)\in\Omega_1} \sum_{(a_2,b_2)\in\Omega_2} \Big(\frac{a_1-a_2}{p} \Big) e_p\Big(\frac{(b_1-b_2)^2}{4(a_1-a_2)} \Big) \Big| \le p^{1-\varepsilon_1}, \tag{2.7}$$

where the summands with $a_1 = a_2$ are excluded from the summation. We next break Ω_1, Ω_2 into *balanced* sets. For $a \in \mathcal{A}$ and $i = 1, 2$, let

$$\Omega_i(a) = \big\{ b \in \mathcal{B} : (a, b) \in \Omega_i \big\}.$$

To prove (2.7), it is enough to show that

$$|S(A_1, A_2)| \le p^{1-1.1\varepsilon_1}, \quad S(A_1, A_2) = \sum_{\substack{a_1 \in A_1, \\ a_2 \in A_2}} \sum_{\substack{b_1 \in \Omega_1(a_1), \\ b_2 \in \Omega_2(a_2)}} \Big(\frac{a_1-a_2}{p} \Big) e_p\Big(\frac{(b_1-b_2)^2}{4(a_1-a_2)} \Big), \tag{2.8}$$

whenever M_1, M_2 are powers of two and, for $i = 1, 2$ and for any $a_i \in A_i$, that

$$M_i/2 \le |\Omega_i(a_i)| < M_i, \qquad |A_i| M_i \le 2\sqrt{p}. \tag{2.9}$$

Indeed, there are $O(\log^2 p)$ choices for M_1, M_2. To prove the cancellation in (2.8), we basically split it into two cases: (i) some $B' = \Omega_i(a_j)$ has additive structure (i.e., $E(B', B')$ is large), where the cancellation comes from the sum over b_1, b_2 (with a_1, a_2 fixed), and (ii) when B' does not have additive structure, in which case one gets dispersion of the phases from the dilation weights $1/(a_1 - a_2)$ (taking a large moment and using (2.4)). Incidentally, oscillations of the factor $(\frac{a_1-a_2}{p})$ play no role in the argument.

3. The flat RIP

Let $\mathbf{u}_1, \dots, \mathbf{u}_N$ be the columns of an $n \times N$ matrix Φ. Suppose that, for every j, $\|\mathbf{u}_j\|_2 = 1$. We say that Φ satisfies the flat RIP of order k with constant δ if, for any

*For $d \in \mathbb{F}_p^*$, we have $(\frac{d}{p}) = 1$ if the congruence $x^2 \equiv d \pmod p$ has a solution, and $(\frac{d}{p}) = -1$ otherwise.

disjoint $J_1, J_2 \subset \{1, \ldots, N\}$ with $|J_1| \le k$, $|J_2| \le k$, we have

$$\left|\left\langle \sum_{j\in J_1} \mathbf{u}_j, \sum_{j\in J_2} \mathbf{u}_j \right\rangle\right| \le \delta(|J_1||J_2|)^{1/2}. \tag{3.1}$$

For technical reasons, it is more convenient to work with the flat RIP than with the RIP. However, the flat RIP implies an RIP with an increase in δ. The flat RIP is closely related to the property that (1.1) holds for any $\mathbf{x}$ with entries which are zero or one and at most k ones (see the calculation at the end of this section).

LEMMA 3
Let $k \ge 2^{10}$, and let s be a positive integer. Suppose that Φ satisfies the flat RIP of order k with constant δ. Then Φ satisfies the RIP of order $2sk$ with constant $44s\delta\log k$.

Proof
First, by a convexity-type argument and our assumption, we have

$$\left|\left\langle \sum_{j\in J_1} x_j\mathbf{u}_j, \sum_{j\in J_2} y_j\mathbf{u}_j \right\rangle\right| \le \delta(|J_1||J_2|)^{1/2} \tag{3.2}$$

provided that $|J_1| \le k$, $|J_2| \le k$, and $0 \le x_j, y_j \le 1$ for all j. Next, suppose that $|J_1| \le k$, $|J_2| \le k$, and $0 \le x_j, y_j$ for all j. Without loss of generality, assume that $\|\mathbf{x}\|_2 = \|\mathbf{y}\|_2 = 1$, where $\|\cdot\|_2$ denotes the l_2 norm. For a positive integer ν, let

$$J_{1,\nu} = \{j \in J_1 : 2^{-\nu} < x_j \le 2^{1-\nu}\}, \qquad J_{2,\nu} = \{j \in J_2 : 2^{-\nu} < y_j \le 2^{1-\nu}\}.$$

Observe that

$$\sum_\nu 4^{-\nu}|J_{1,\nu}| \le 1, \qquad \sum_\nu 4^{-\nu}|J_{2,\nu}| \le 1. \tag{3.3}$$

Applying (3.2) to sets $J_{1,\nu}$, $J_{2,\nu}$, we get

$$\begin{aligned}\left|\left\langle \sum_{j\in J_1} x_j\mathbf{u}_j, \sum_{j\in J_2} y_j\mathbf{u}_j \right\rangle\right| &\le \sum_{\nu_1,\nu_2}\left|\left\langle \sum_{j\in J_{1,\nu_1}} x_j\mathbf{u}_j, \sum_{j\in J_{2,\nu_2}} y_j\mathbf{u}_j \right\rangle\right| \\ &\le \sum_{\nu_1,\nu_2} 2^{2-\nu_1-\nu_2}\delta(|J_{1,\nu_1}||J_{2,\nu_2}|)^{1/2} \\ &= 4\delta\sum_\nu 2^{-\nu}|J_{1,\nu}|^{1/2}\sum_\nu 2^{-\nu}|J_{2,\nu}|^{1/2}.\end{aligned}$$

Let $t = \lfloor 3 + \log k/(2\log 2)\rfloor$. By the Cauchy-Schwarz inequality, we infer that

$$\begin{aligned}\sum_{\nu} 2^{-\nu}|J_{1,\nu}|^{1/2} &\le \sum_{\nu=1}^{t} 2^{-\nu}|J_{1,\nu}|^{1/2} + \sum_{\nu=t+1}^{\infty} 2^{-\nu}|J_{1,\nu}|^{1/2}\\ &\le t^{1/2}\Big(\sum_{\nu=1}^{t} 4^{-\nu}|J_{1,\nu}|\Big)^{1/2} + \sum_{\nu=t+1}^{\infty} 2^{-\nu}k^{1/2} \le t^{1/2} + \frac{1}{4}.\end{aligned}$$

Similarly,

$$\sum_{\nu} 2^{-\nu}|J_{2,\nu}|^{1/2} \le t^{1/2} + \frac{1}{4}.$$

Therefore, we have

$$\Big|\Big\langle \sum_{j\in J_1} x_j\mathbf{u}_j, \sum_{j\in J_2} y_j\mathbf{u}_j\Big\rangle\Big| \le 4\delta\Big(t^{1/2}+\frac{1}{4}\Big)^2 \le 5.5\delta\log k. \tag{3.4}$$

For the next step, suppose that x_j, y_j take arbitrary complex values $|J_1| \le sk$ and $|J_2| \le sk$, respectively. We partition J_1 and J_2 into s subsets of cardinality at most k each: $J_1 = \bigcup_{\mu=1}^{s} J_{1,\mu}$, $J_2 = \bigcup_{\mu=1}^{s} J_{2,\mu}$. Next, for any j, we have

$$x_j = \sum_{\nu=1}^{4} x_{j,\nu} i^{\nu}, \quad y_j = \sum_{\nu=1}^{4} y_{j,\nu} i^{\nu}, \quad |x_j|^2 = \sum_{\nu=1}^{4} x_{j,\nu}^2, \quad |y_j|^2 = \sum_{\nu=1}^{4} y_{j,\nu}^2,$$

where $x_{j,\nu}$, $y_{j,\nu}$ are nonnegative. By (3.4) and the Cauchy-Schwarz inequality,

$$\begin{aligned}\Big|\Big\langle \sum_{j\in J_1} x_j\mathbf{u}_j, \sum_{j\in J_2} y_j\mathbf{u}_j\Big\rangle\Big| &\le \sum_{\mu_1=1}^{s}\sum_{\nu_1=1}^{4}\sum_{\mu_2=1}^{s}\sum_{\nu_2=1}^{4}\Big|\Big\langle \sum_{j\in J_{1,\mu_1}} x_{j,\nu_1}\mathbf{u}_j, \sum_{j\in J_{2,\mu_2}} y_{j,\nu_2}\mathbf{u}_j\Big\rangle\Big|\\ &\le \sum_{\mu_1,\nu_1,\mu_2,\nu_2} 5.5\delta(\log k)\Big(\sum_{j\in J_{1,\mu_1}} x_{j,\nu_1}^2\Big)^{1/2}\Big(\sum_{j\in J_{2,\mu_2}} y_{j,\nu_2}^2\Big)^{1/2}\\ &\le 22s\delta\|\mathbf{x}\|_2\|\mathbf{y}\|_2\log k. \end{aligned}\tag{3.5}$$

To complete the proof of the lemma, assume that $N \ge 2sk$, and consider a vector $\mathbf{x} = \sum_{j\in J} x_j e_j$ with $\|\mathbf{x}\|_2 = 1$ and $|J| = 2sk$, where $(e_1, \dots, e_N)$ is the standard basis of $\mathbb{C}^N$. Take arbitrary partitions of J into two sets J_1, J_2 of cardinality sk each.

By (3.5), we have

$$\begin{aligned}
\left| \|\Phi\mathbf{x}\|_2^2 - \|\mathbf{x}\|_2^2 \right| &= \Big| \sum_{j_1, j_2 \in J, j_1 \neq j_2} \langle x_{j_1}\mathbf{u}_{j_1}, x_{j_2}\mathbf{u}_{j_2} \rangle \Big| \\
&= \binom{2sk-2}{sk-1}^{-1} \Big| \sum_{J_1, J_2} \Big\langle \sum_{j\in J_1} x_j \mathbf{u}_j, \sum_{j \in J_2} x_j \mathbf{u}_j \Big\rangle \Big| \\
&\le \binom{2sk-2}{sk-1}^{-1} \sum_{J_1, J_2} 22 s\delta (\log k) \Big(\sum_{j\in J_1} |x_j|^2 \Big)^{1/2} \Big(\sum_{j\in J_2} |x_j|^2 \Big)^{1/2} \\
&\le \binom{2sk-2}{sk-1}^{-1} \sum_{J_1, J_2} 11 s\delta \|\mathbf{x}\|_2^2 \log k \\
&= \binom{2sk}{sk} \binom{2sk-2}{sk-1}^{-1} 11 s\delta \|\mathbf{x}\|_2^2 \log k \le 44 s\delta \|\mathbf{x}\|_2^2 \log k. \qquad \square
\end{aligned}$$

Proof of Lemma 1

For any disjoint $J_1, J_2 \subset \{1, \dots, N\}$ with $|J_1| \le k$, $|J_2| \le k$, we have

$$\Big| \Big\langle \sum_{j\in J_1} \mathbf{u}_j, \sum_{j\in J_2} \mathbf{u}_j \Big\rangle \Big| \le \min(\delta k, \mu |J_1||J_2|) \le \min(\delta k, |J_1||J_2|/k) \le \sqrt{\delta |J_1||J_2|},$$

and it remains to apply Lemma 3. $\square$

Remark 4

Using the assumptions of the Lemma 1 directly rather than reducing it to Lemma 3, one can get a better constant for the RIP; however, we do not need a stronger version of the corollary for our purposes.

4. Some definitions and results from additive combinatorics

For an (additive) abelian group G, we define the sum and the difference of subsets $A, B \subset G$:

$$A + B = \{a + b : a \in A, b \in B\}, \quad A - B = \{a - b : a \in A, b \in B\}.$$

We denote $-A = \{-x : x \in A\}$. If $A \subseteq G = \mathbb{F}_p$ and $b \in \mathbb{F}_p$, write $bA = \{ba : a \in A\}$.

Consider $G = \mathbb{F}_p$, and let $\mathcal{B} \subset G$ be the set defined in Section 2. There is a natural bijection Φ between $\mathcal{B}$ and the cube $\mathcal{C}_{M,r} = \{0, \dots, M-1\}^r$ defined by $\Phi(\sum_{j=1}^r x_j (2M)^{j-1}) = (x_1, \dots, x_r)$. Moreover, it is trivial that $b_1 + b_2 = b_3 + b_4$ if and only if $\Phi(b_1) + \Phi(b_2) = \Phi(b_3) + \Phi(b_4)$. In the language of additive combinatorics, Φ is a Freiman isomorphism between $\mathcal{B}$ and $\mathcal{C}_{M,r}$. Thus, $|B_1 + B_2| = |\Phi(B_1) + \Phi(B_2)|$

for any $B_1 \subseteq \mathcal{B}$, $B_2 \subseteq \mathcal{B}$. The problem of the size of sumsets in $\mathcal{C}_{M,r}$ is investigated in the next section.

We use the following lemma which is a particular case of Plünecke-Ruzsa estimates.

LEMMA 4 ([44, Exercise 6.5.15])
For any nonempty set $A \subset G$, we have $|A + A| \leq |A - A|^2/|A|$.

If $A, B \subset G$, we define the (additive) energy $E(A, B)$ of the sets A and B as the number of solutions of the equation

$$a_1 + b_1 = a_2 + b_2, \quad a_1, a_2 \in A,\ b_1, b_2 \in B.$$

Next, let $F \subset A \times B$. The F-restricted sum of A and B is defined as

$$A +_F B = \big\{a + b :\ a \in A, b \in B, (a, b) \in F\big\}.$$

Trivially, $E(A, A) \leq |A|^3$. If $E(A, A)$ is close to $|A|^3$, then A must have a special additive structure.

LEMMA 5 ([44, Lemma 2.30])
If $E(A, A) \geq |A|^3/K$, then there exists $F \subset A \times A$ such that $|F| \geq |A|^2/(2K)$ and $|A +_F A| \leq 2K|A|$.

The following lemma (see [11]) is a version of the Balog-Szemerédi-Gowers lemma which plays a very important role in additive combinatorics.

LEMMA 6
If $F \subset A \times A$, $|F| \geq |A|^2/L$, and $|A +_F A| \leq L|A|$, then there exists a set $A' \subset A$ such that $|A'| \geq |A|/(10L)$ and $|A' - A'| \leq 10^4 L^9 |A|$.

Combining Lemmas 5 and 6 gives the following.

COROLLARY 1
If $E(A, A) \geq |A|^3/K$, then there exists a set $A' \subset A$ such that $|A'| \geq |A|/(20K)$ and $|A' - A'| \leq 10^7 K^9 |A|$.

For a function $f : \mathbb{F}_p \to \mathbb{C}$ and a number $r \geq 1$, we define the L_r norm of f as

$$\|f\|_r = \Big(\sum_{x \in \mathbb{F}_p} |f(x)|^r\Big)^{1/r}.$$

The additive convolution of two functions $f, g : \mathbb{F}_p \to \mathbb{C}$ is defined as

$$f * g(x) = \sum_{y \in \mathbb{F}_p} f(y) g(x - y).$$

By 1_A we denote the indicator function of the set A. With this notation, we have

$$E(A, B) = E(A, -B) = \|1_A * 1_B\|_2^2. \tag{4.1}$$

We say that a function $f : \mathbb{F}_p \to \mathbb{R}_+$ is a *probability measure* if $\|f\|_1 = 1$. Notice that if f, g are probability measures, then $f * g$ is also a probability measure.

PROPOSITION 3 ([10, Theorem C])
Assume that $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p^*$ with $|A| \geq |B|$. For some $c_0 > 0$, we have

$$\sum_{b \in B} E(A, bA) \ll \min(p/|A|, |B|)^{-c_0} |A|^3 |B|. \tag{4.2}$$

Remark 5
An explicit version of Proposition 3, with $c_0 = 1/10430$, is given in [12].

Note that if $|A| < |B|$, we may decompose B as a disjoint union of at most $2|B|/|A|$ sets B_j with $|A|/2 < |B_j| \leq |A|$ and apply (4.2) for each B_j. Hence

$$\sum_{b \in B} E(A, bA) \ll \left[\min\left(|A|, |B|, \frac{p}{|A|} \right) \right]^{-c_0} |A|^3 |B|.$$

Applying the Cauchy-Schwarz inequality, we get

$$\sum_{b \in B} \|1_A * 1_{bA}\|_2 \ll |A|^{3/2} (|A|^{-c_0/2} |B| + |B|^{1 - c_0/2} + p^{-c_0/2} |A|^{c_0/2} |B|). \tag{4.3}$$

Remark 6
It would be interesting to find the best possible value for c_0 in Proposition 3. The example $A = B = \{1, \ldots, [\sqrt{p}]\}$ shows that $c_0 < 1$.

COROLLARY 2
For any $A \subset \mathbb{F}_p$ and a probability measure λ, we have

$$\sum_{b \in \mathbb{F}_p^*} \lambda(b) \|1_A * 1_{bA}\|_2 \ll (\|\lambda\|_2 + |A|^{-1/2} + |A|^{1/2} p^{-1/2})^{c_0} |A|^{3/2}.$$

Proof
Put $\lambda(p) = 0$, and let b be a permutation of $\{1, \dots, p\}$ such that $\lambda(b_1) \geq \cdots \geq \lambda(b_p) = 0$. By Lemma 3, for $1 \leq j \leq p-1$, we have $S_j \ll G_j$, where

$$S_j = \sum_{h=1}^{j} \|1_A * 1_{bA}\|_2, \quad G_j := |A|^{3/2}(|A|^{-c_0/2} j + |A|^{c_0/2} p^{-c_0/2} j + j^{1-c_0/2}).$$

Applying summation by parts, we have

$$\begin{aligned}\sum_{b\in\mathbb{F}_p^*} \lambda(b)\|1_A * 1_{bA}\|_2 &= \sum_{j=1}^{p} \lambda(b_j)(S_j - S_{j-1}) = \sum_{j=1}^{p-1} S_j \left(\lambda(b_j) - \lambda(b_{j+1})\right) \\ &\ll \sum_{j=1}^{p-1} G_j \left(\lambda(b_j) - \lambda(b_{j+1})\right) = \sum_{j=1}^{p-1} \lambda(b_j)(G_j - G_{j-1}) \\ &= |A|^{3/2}\Big[|A|^{-c_0/2} + p^{-c_0/2}|A|^{c_0/2} + O\Big(\sum_{j=1}^{p} \lambda(b_j) j^{-c_0/2}\Big)\Big].\end{aligned}$$

Denote $u_0 = \|\lambda\|_2^{-2}$. Notice that $1 \leq u_0 \leq p$ since $\|\lambda\|_1 = 1$. Separately considering $j \leq u_0$ and $j > u_0$ and using the Cauchy-Schwarz inequality, we get

$$\sum_{j=1}^{p} \lambda(b_j) j^{-c_0/2} \leq \|\lambda\|_2 \Big(\sum_{j\leq u_0} j^{-c_0}\Big)^{1/2} + u_0^{-c_0/2} = O\left(\|\lambda\|_2^{c_0}\right). \qquad \square$$

Although Corollary 2 suffices for the purposes of this paper, a further generalization of Proposition 3 might be useful. For $z \in \mathbb{F}_p^*$, we define a function $\rho_z[f]$ by $\rho_z[f](x) = f(x/z)$.

THEOREM 4
Let λ, μ be probability measures on $\mathbb{F}_p$. Then

$$\sum_{b\in\mathbb{F}_p^*} \lambda(b)\|\mu * \rho_b[\mu]\|_2 \ll (\|\lambda\|_2 + \|\mu\|_2 + \|\mu\|_2^{-1} p^{-1/2})^{c_0/7} \|\mu\|_2.$$

Proof
Using a parameter $\Delta \geq 1$, which will be specified later, we define the sets

$$A_- = \left\{x : \mu(x) \geq \|\mu\|_2^2 \Delta\right\}, \quad A_+ = \left\{x : \mu(x) < \|\mu\|_2^2 \Delta^{-2}\right\}, \quad A = \mathbb{F}_p \backslash A_- \backslash A_+.$$

Decompose $\mu = \mu_- + \mu_0 + \mu_+$, where

$$\mu_- = \mu 1_{A_-}, \qquad \mu_0 = \mu 1_A, \qquad \mu_+ = \mu 1_{A_+}.$$

The contribution to the sum in the theorem from μ_- and μ_+ is negligible. First,

$$\|\mu_-\|_1 \leq \frac{1}{\Delta \|\mu\|_2^2} \sum_{x \in A_-} \mu(x)^2 \leq \Delta^{-1} \tag{4.4}$$

and

$$\|\mu_+\|_2 \leq \|\mu\|_2 \Delta^{-1} \|\mu_+\|_1^{1/2} \leq \|\mu\|_2 \Delta^{-1}. \tag{4.5}$$

Using Young's inequality (see [44, Theorem 4.8]), we find that

$$\begin{aligned} \sum_{b \in \mathbb{F}_p^*} \lambda(b) \|\mu_- * \rho_b[\mu]\|_2 &\leq \sum_{b \in \mathbb{F}_p^*} \lambda(b) \|\mu_-\|_1 \|\rho_b[\mu]\|_2 \\ &\leq \sum_{b \in \mathbb{F}_p^*} \lambda(b) \Delta^{-1} \|\mu\|_2 \leq \Delta^{-1} \|\mu\|_2, \end{aligned} \tag{4.6}$$

$$\begin{aligned} \sum_{b \in \mathbb{F}_p^*} \lambda(b) \|\mu_+ * \rho_b[\mu]\|_2 &\leq \sum_{b \in \mathbb{F}_p^*} \lambda(b) \|\mu_+\|_2 \|\rho_b[\mu]\|_1 \\ &\leq \sum_{b \in \mathbb{F}_p^*} \lambda(b) \Delta^{-1} \|\mu\|_2 \leq \Delta^{-1} \|\mu\|_2. \end{aligned} \tag{4.7}$$

Similarly, we have

$$\sum_{b \in \mathbb{F}_p^*} \lambda(b) \|\mu_0 * \rho_b[(\mu_- + \mu_+)]\|_2 \leq 2\Delta^{-1} \|\mu\|_2. \tag{4.8}$$

So, it suffices to estimate the contribution of μ_0. We have

$$1 = \|\mu\|_1 \geq \sum_{x \in A} \mu(x) \geq |A| \|\mu\|_2^2 \Delta^{-2}.$$

Hence, $|A| \le \|\mu\|_2^{-2}\Delta^2$. Now we can use Corollary 2 to get

$$\begin{aligned}\sum_{b\in\mathbb{F}_p^*}\lambda(b)\|\mu_0 * \rho_b[\mu_0]\|_2 &\le \|\mu\|_2^4\Delta^2\sum_{b\in\mathbb{F}_p^*}\lambda(b)\|1_A * 1_{bA}\|_2\\ &\ll \|\mu\|_2^4\Delta^2(\|\lambda\|_2^{c_0} + |A|^{-c_0/2} + |A|^{c_0/2}p^{-c_0/2})|A|^{3/2}\\ &\le \|\mu\|_2^4\Delta^2(\|\lambda\|_2^{c_0}\|\mu\|_2^{-3}\Delta^3 + \|\mu\|_2^{-3+c_0}\Delta^{3-c_0} + \|\mu\|_2^{-3-c_0}\Delta^{3+c_0})\\ &\le \Delta^6\|\mu\|_2(\|\lambda\|_2^{c_0} + \|\mu\|_2^{c_0} + \|\mu\|_2^{-c_0}p^{-c_0/2}).\end{aligned}$$

Combining the last inequality with (4.6) – (4.8), we get

$$\sum_{b\in\mathbb{F}_p^*}\lambda(b)\|\mu * \rho_b[\mu]\|_2 \le 4\Delta^{-1}\|\mu\|_2 + O(\Delta^6\|\mu\|_2 S),$$

where

$$S = \|\lambda\|_2^{c_0} + \|\mu\|_2^{c_0} + \|\mu\|_2^{-c_0}p^{-c_0/2}.$$

Taking $\Delta = \max(1, S^{1/7})$ completes the proof of the theorem. □

5. A sumset estimate in product sets

The main result of this section is the following.

THEOREM 5
Let $r, M \in \mathbb{N}$, let $M \ge 2$, and let $\mathcal{C} = \mathcal{C}_{M,r} = \{0, \dots, M-1\}^r$. Let $\tau = \tau_M$ be the solution of the equation

$$\Big(\frac{1}{M}\Big)^{2\tau} + \Big(\frac{M-1}{M}\Big)^{\tau} = 1.$$

Then for any subsets $A, B \subset \mathcal{C}$, we have

$$|A+B| \ge (|A||B|)^{\tau}. \tag{5.1}$$

Proof
Observe that, for $A = B = \mathcal{C}$, we have $|A+B| = |A|^{\tau'}|B|^{\tau'}$, where

$$\tau' = \tau'_M = \frac{\log(2M-1)}{2\log M}.$$

By Theorem 5, $\tau \le \tau'$. On the other hand, $\tau > 1/2$. If $M \to \infty$, then

$$u^{2\tau} = 1-(1-u)^{\tau} \sim \frac{u}{2}, \qquad 2\tau - 1 \sim \frac{\log 2}{\log M} \sim 2\tau' - 1. \tag{5.2}$$

So, the asymptotic behavior of $2\tau_M - 1$ as $M \to \infty$ is sharp. Likely, inequality (5.1) holds with $\tau = \tau'$. This was proved in the case $M = 2$ by Woodall [47].

Results of a similar spirit, concerning addition of subsets of $\mathbb{F}_p{}^r$ and related groups, are considered in [9].

For positive integers K, L, we define a UR-path as a sequence of pairs of integers $\mathcal{P} = ((i_1, j_1) = (0,0), \dots, (i_{K+L-1}, j_{K+L-1}) = (K-1, L-1))$ such that, for any n, either $i_{n+1} = i_n + 1$, $j_{n+1} = j_n$ or $i_{n+1} = i_n$, $j_{n+1} = j_n + 1$.

LEMMA 7
Let $KL \le M^2$, let $u_0 \ge \cdots \ge u_{K-1} \ge 0$, let $v_0 \ge \cdots \ge v_{L-1} \ge 0$, and let $\tau = \tau_M$. Then there exists a UR-path $\mathcal{P}$ such that

$$\sum_{n=1}^{K+L-1} (u_{i_n} v_{j_n})^\tau \ge \Big(\sum_{i=0}^{K-1} u_i\Big)^\tau \Big(\sum_{j=0}^{L-1} v_j\Big)^\tau. \tag{5.3}$$

Proof
We proceed by induction on $K + L$. For $K = 1$ or $L = 1$ the assertion is obvious. We prove it for K, L with $\min(K, L) \ge 2$, $KL \le M^2$ supposing that it holds for (K, L) replaced by $(K-1, L)$ and $(K, L-1)$. Without loss of generality, we assume that

$$\sum_{i=0}^{K-1} u_i = \sum_{j=0}^{L-1} v_j = 1.$$

By the induction supposition, there exists a UR-path $\mathcal{P}$ such that $i_1 = 1$, $j_1 = 0$, and

$$\sum_{n=2}^{K+L-1} (u_{i_n} v_{j_n})^\tau \ge \Big(\sum_{i=1}^{K-1} u_i\Big)^\tau \Big(\sum_{j=0}^{L-1} v_j\Big)^\tau = (1-u_0)^\tau.$$

Therefore, we have

$$S := \max_{\mathcal{P}} \sum_{n=1}^{K+L-1} (u_{i_n} v_{j_n})^\tau \ge (u_0 v_0)^\tau + (1-u_0)^\tau.$$

Similarly, $S \ge (u_0 v_0)^\tau + (1-v_0)^\tau$. Thus $S \ge w^{2\tau} + (1-w)^\tau$, where

$$w = (u_0 v_0)^{1/2} \ge (KL)^{-1/2} \ge 1/M.$$

The function $f(x) = x^{2\tau} + (1-x)^\tau - 1$ has a negative third derivative on $[0, 1]$ and $f(0) = f(1/M) = f(1) = 0$. By Rolle's theorem, f has no other zeros on $[0, 1]$, and since $f(u) > 0$ for u close to 1, $f(x) \geq 0$ for $1/M \leq x \leq 1$. Therefore, $f(w) \geq 0$ as desired. □

We will need Lemma 7 only for $K = L = M$ (although for the proof it was convenient to have varying K, L).

LEMMA 8
Let $U_0, \ldots, U_{M-1}$, $V_0, \ldots, V_{M-1}$ be nonnegative numbers, and let $\tau = \tau_M$. Then

$$\sum_{\mu=0}^{2M-2} \max_{\substack{\kappa+\lambda=\mu, \\ \kappa\geq 0, \lambda\geq 0}} (U_\kappa V_\lambda)^\tau \geq \Big(\sum_{\kappa=0}^{M-1} U_\kappa\Big)^\tau \Big(\sum_{\lambda=0}^{M-1} V_\lambda\Big)^\tau. \tag{5.4}$$

Lemma 8 has some similarity with inequality (2.1) from [37].

Proof
We order $U_0, \ldots, U_{M-1}$ and $V_0, \ldots, V_{M-1}$ in the descending order $u_0 \geq \cdots \geq u_{M-1}$ and $v_0 \geq \cdots \geq v_{M-1}$, respectively, where for some permutations π and σ of the set $\{0, \ldots, M-1\}$, we have $u_i = U_{\pi_i}$, $v_j = V_{\sigma_j}$. We consider an arbitrary UR-path $\mathcal{P}$ with $K = L = M$. Since $|\{\pi_{i_1}, \ldots, \pi_{i_n}\}| = i_n + 1$ and $|\{\sigma_{j_1}, \ldots, \sigma_{j_n}\}| = j_n + 1$, we have

$$|\{\pi_{i_1}, \ldots, \pi_{i_n}\} + \{\sigma_{j_1}, \ldots, \sigma_{j_n}\}| \geq i_n + j_n + 1.$$

Consequently, there is a permutation ψ of $\{0, \ldots, 2M-2\}$ so that

$$\psi(n-1) \in \{\pi_{i_1}, \ldots, \pi_{i_n}\} + \{\sigma_{j_1}, \ldots, \sigma_{j_n}\} \quad (1 \leq n \leq 2M-1).$$

Thus, for some $\kappa_0 \in \{\pi_{i_1}, \ldots, \pi_{i_n}\}$ and $\lambda_0 \in \{\sigma_{j_1}, \ldots, \sigma_{j_n}\}$, we have

$$\max_{\substack{\kappa+\lambda=\psi(n-1), \\ \kappa\geq 0, \lambda\geq 0}} (U_\kappa V_\lambda)^\tau \geq (U_{\kappa_0} V_{\lambda_0})^\tau.$$

But $U_{\kappa_0} = u_i$ for some $i \in \{i_1, \ldots, i_n\}$. Recalling that $i_1 \leq i_2 \leq \ldots$ and that $u_1 \geq u_2 \geq \ldots$, we obtain $U_{\kappa_0} \geq u_{i_n}$. Similarly, $V_{\lambda_0} \geq v_{j_n}$. Therefore, we have

$$\max_{\substack{\kappa+\lambda=\psi(n-1), \\ \kappa\geq 0, \lambda\geq 0}} (U_\kappa V_\lambda)^\tau \geq (u_{i_n} v_{j_n})^\tau$$

and

$$\sum_{\mu=0}^{2M-2} \max_{\substack{\kappa+\lambda=\mu, \\ \kappa\geq 0, \lambda\geq 0}} (U_\kappa V_\lambda)^\tau = \sum_{n=1}^{2M-1} \max_{\substack{\kappa+\lambda=\psi(n-1), \\ \kappa\geq 0, \lambda\geq 0}} (U_\kappa V_\lambda)^\tau \geq \sum_{n=1}^{2M-1} (u_{i_n} v_{j_n})^\tau,$$

and the result follows from Lemma 7. □

Now we are ready to prove Theorem 5. We proceed by induction on r. For $r = 0$, the set $\mathcal{C}_{M,r}$ is a singleton, and there is nothing to prove. Now suppose that the assertion holds for r replaced by $r-1 \geq 0$. We consider arbitrary subsets $A, B \subset \mathcal{C} = \mathcal{C}_{M,r}$. For $i = 0, \dots, M-1$, we denote

$$A_i = \Big\{(x_1, \dots, x_{r-1}) : (x_1, \dots, x_{r-1}, i) \in A\Big\},$$

$$B_i = \Big\{(x_1, \dots, x_{r-1}) : (x_1, \dots, x_{r-1}, i) \in B\Big\}.$$

Let $D = A + B$. For $n = 0, \dots, 2M-2$, we denote

$$D_n = \Big\{(x_1, \dots, x_{r-1}) : (x_1, \dots, x_{r-1}, n) \in D\Big\}.$$

Observe that

$$|A| = \sum_i |A_i|, \qquad B = \sum_j |B_j|, \qquad D = \sum_n |D_n|.$$

For any $n = 0, \dots, 2M-2$, we have

$$|D_n| \geq \max_{\substack{i+j, \\ i\geq 0, j\geq 0}} |A_i + B_j|.$$

By the induction supposition, $|A_i + B_j| \geq (|A_i||B_j|)^\tau$. Hence

$$|D_n| \geq \max_{\substack{i+j, \\ i\geq 0, j\geq 0}} (|A_i||B_j|)^\tau.$$

Applying Lemma 8, we have

$$|D| = \sum_n |D_n| \geq \sum_n \max_{\substack{i+j, \\ i\geq 0, j\geq 0}} (|A_i||B_j|)^\tau \geq \Big(\sum_i |A_i|\Big)^\tau \Big(\sum_j |B_j|\Big)^\tau = (|A||B|)^\tau.$$

The proof of Theorem 5 is complete. □

COROLLARY 3

Let m be a positive integer. For the set $\mathcal{B} \subset \mathbb{F}_p$ defined in Section 2, and for any subset $B \subset \mathcal{B}$, $|B| > p^{1/4}$, we have $|B - B| \geq p^{\beta/5}|B|$.

Proof

The set $-B$ is a translate of some set $B' \subset \mathcal{B}$, and $\mathcal{B}$ is Freiman isomorphic to $\mathcal{C}_{M,r}$. Hence, for any $B \subset \mathcal{B}$, we have $|B - B| = |B + B'| \geq |B|^{2\tau_M}$. If $|B| > p^{1/4}$, then $|B - B| \geq |p|^{(2\tau_M - 1)/4}|B|$. By (5.2) and a short calculation using $M \geq 2^{15}$, $p^{(2\tau_M-1)/4} \geq p^{\beta/5}$. □

COROLLARY 4

Fix $m \in \mathbb{N}$, and let $p \geq p(m)$ be a sufficiently large prime. Let $\mathcal{B} \subset \mathbb{F}_p$ be the set defined in Section 2. Then for any subset $S \subset \mathcal{B}$, $|S| > p^{1/3}$, we have $E(S, S) \leq p^{-\beta/50}|S|^3$.

Proof

Let $E(S, S) = |S|^3/K$. By Corollary 1, there is a set $B \subset S$ such that $|B| \geq |S|/(20K)$ and $|B - B| \leq 10^7 K^9 |S|$. If $K \leq p^{\beta/50} < p^{1/24}$ and p is so large that $10^7 \leq p^{\beta/50}$, then we get a contradiction with Corollary 3. □

6. The proof of Lemma 2

We may assume that $\varepsilon_1 > 0$; otherwise there is nothing to prove. Adopt the notation $(A_i, M_i, \Omega_i(a))$ from Section 2. If $|A_1|M_1 < p^{1/2-\gamma/10}$, then, by (2.9), $|S(A_1, A_2)| \leq 2p^{1-\gamma/10}$ and (2.8) holds (recall that $c_0 < 1$; hence $\varepsilon_1 < \gamma/20$). Thus, we can assume that $|A_1|M_1 \geq p^{1/2-\gamma/10}$, which implies, by (2.3), that

$$M_1 \geq p^{1/2-\alpha-\gamma/10}. \tag{6.1}$$

LEMMA 9

For any $\theta \in \mathbb{F}_p^*$, $B_1 \subset \mathbb{F}_p$, $B_2 \subset \mathbb{F}_p$, we have

$$\Bigg| \sum_{\substack{b_1 \in B_1,\\ b_2 \in B_2}} e_p\left(\theta(b_1 - b_2)^2\right) \Bigg| \leq |B_1|^{1/2} E(B_1, B_1)^{1/8} |B_2|^{1/2} E(B_2, B_2)^{1/8} p^{1/8}.$$

Proof

Let W denote the double sum over b_1, b_2. By the Cauchy-Schwarz inequality, we get

$$\begin{aligned} |W|^2 &\leq |B_1| \sum_{b_1 \in B_1} \Bigg| \sum_{b_2 \in B_2} e_p\left(\theta(b_1 - b_2)^2\right) \Bigg|^2 \\ &= |B_1| \sum_{b_2, b_2' \in B_2} \sum_{b_1 \in B_1} e_p\left(\theta(b_2^2 - (b_2')^2 - 2b_1(b_2 - b_2'))\right). \end{aligned}$$

Another application of the Cauchy-Schwarz inequality gives

$$\begin{aligned} |W|^4 &\leq |B_1|^2 |B_2|^2 \sum_{b_2, b_2' \in B_2} \Bigg| \sum_{b_1} e_p\left(2\theta b_1(b_2 - b_2')\right) \Bigg|^2 \\ &= |B_1|^2 |B_2|^2 \sum_{x, y \in \mathbb{F}_p} \lambda_x \mu_y e_p(-2\theta x y), \end{aligned}$$

where

$$\lambda_x = 1_{B_1} * 1_{(-B_1)}(x), \qquad \mu_y = 1_{B_2} * 1_{(-B_2)}(y).$$

A third application of the Cauchy-Schwarz inequality, followed by Parseval's identity, yields a well-known inequality (see [46, Chapter 6, Problem 14(a)])

$$\Big| \sum_{x,y\in\mathbb{F}_p} \lambda_x \mu_y e_p(-2\theta xy)\Big|^2 \le \|\lambda\|_2^2 \sum_{x\in\mathbb{F}_p} \Big| \sum_{y\in\mathbb{F}_p} \mu_y e_p(-2\theta xy)\Big|^2$$
$$= p\|\lambda\|_2^2\|\mu\|_2^2 = pE(B_1, B_1)E(B_2, B_2). \qquad \square$$

By (6.1), $|\Omega_i(a_i)| \ge p^{1/3}$, Lemma 9, and (2.5), we have

$$\Big| \sum_{\substack{b_1\in\Omega_1(a_1)\\ b_2\in\Omega_2(a_2)}} e_p\Big(\frac{(b_1-b_2)^2}{4(a_1-a_2)}\Big)\Big| \le |\Omega_1(a_1)|^{7/8}|\Omega_2(a_2)|^{7/8} p^{1/8-\gamma/4}.$$

Next, by (2.9), we have

$$|S(A_1, A_2)| \le 4|A_1|^{1/8}|A_2|^{1/8} p^{1-\gamma/4}.$$

Thus, if $|A_1| < p^{\gamma/2}$, and $|A_2| < p^{\gamma/2}$, then $|S(A_1, A_2)| \le 4p^{1-\gamma/8}$, and (2.8) follows. Otherwise, without loss of generality, we may assume that

$$|A_2| \ge p^{\gamma/2}. \tag{6.2}$$

The following lemma gives the necessary estimates to complete the proof of Lemma 2. For $a_1 \in A_1$, set

$$T(A, B) = T_{a_1}(A, B) = \sum_{\substack{b_1\in B\\ a_2\in A, b_2\in\Omega_2(a_2)}} \Big(\frac{a_1-a_2}{p}\Big) e_p\Big(\frac{(b_1-b_2)^2}{4(a_1-a_2)}\Big).$$

LEMMA 10
If $a_1 \in A_1$, $0 < \gamma \le \min(\alpha, 1/(3m))$, conditions (2.9) and (6.2) are satisfied, and a set $B \subset \mathbb{F}_p$ is such that

$$p^{1/2-6\alpha} \le |B| \le p^{1/2} \tag{6.3}$$

and

$$|B - B| \le p^{28\alpha}|B|, \tag{6.4}$$

then

$$|T(A_2, B)| \le |B| p^{(1/2)-\varepsilon_2}, \qquad \varepsilon_2 = \frac{c_0\gamma}{20} - \frac{42\alpha}{m}. \tag{6.5}$$

Remark 7

The proof of Lemma 10 applies to more general sums; for example, in $T(A, B)$, one may replace the Legendre symbol $(\frac{a_1-a_2}{p})$ with arbitrary complex numbers $\psi(a_1, a_2)$ with modulus less than or equal to 1, and one may replace $1/(a_1 - a_2)$ with different quantities $g(a_1, a_2)$ having the dissociative property (the analog of (2.4) holds).

Postponing the proof of Lemma 10, we first show how to deduce Lemma 2.

We take a maximal subset $B_0 \subset \Omega_1(a_1)$ so that (6.5) holds for $B = B_0$. Denote $B_1 = \Omega_1(a_1) \setminus B_0$. By Lemma 9, (2.9), and (2.3), we have

$$\begin{aligned}
|T_{a_1}(A_2, B_1)| &\le \sum_{a_2 \in A_2} |B_1|^{1/2} E(B_1, B_1)^{1/8} |\Omega_2(a_2)|^{1/2} E\big(\Omega_2(a_2), \Omega_2(a_2)\big)^{1/8} p^{1/8} \\
&\le |A_2|\,|B_1|^{1/2} E(B_1, B_1)^{1/8} M_2^{7/8} p^{1/8} \\
&\le 2|B_1|^{1/2} E(B_1, B_1)^{1/8} p^{(9/16)+(\alpha/8)}.
\end{aligned}$$

Consider the case when

$$E(B_1, B_1) \le p^{-3\alpha} M_1^3. \tag{6.6}$$

Then, due to (2.9), we have

$$|T_{a_1}(A_2, B_1)| \le 2M_1^{7/8} p^{(9/16)-\alpha/4}. \tag{6.7}$$

Now assume that (6.6) does not hold. By (2.9), we get

$$|B_1| > p^{-\alpha} M_1, \qquad E(B_1, B_1) \ge p^{-3\alpha} |B_1|^3.$$

Now by applying Corollary 1 and (2.9), we obtain the existence of a set $B_1' \subset B_1$ such that

$$|B_1'| \ge \frac{M_1}{20 p^{4\alpha}} \ge \frac{p^{1/2-5\alpha-\gamma/10}}{20} \ge p^{1/2-6\alpha}$$

and $|B_1' - B_1'| \le 10^7 p^{27\alpha} |B_1| \le p^{28\alpha} |B_1|$. Using Lemma 10, we get inequality (6.5) for $B = B_1'$. Therefore, (6.5) is also satisfied for $B = B_0 \cup B_1'$, contradicting the choice of B_0.

Thus, we have shown that (6.6) must hold. Using (6.5) for $B = B_0$ and (6.7), we get

$$\left|T_{a_1}\big(A_2, \Omega_1(a_1)\big)\right| \le M_1 p^{(1/2)-\varepsilon_2} + 2M_1^{7/8} p^{(9/16)-\alpha/4}.$$

Summing on $a_1 \in A_1$ and using (2.3) and (2.9), we obtain

$$\begin{aligned}|S(A_1, A_2)| &\le |A_1|(M_1 p^{(1/2)-\varepsilon_2} + 2M_1^{7/8} p^{(9/16)-\alpha/4})\\ &\le 2p^{1-\varepsilon_2} + 4|A_1|^{1/8} p^{1-\alpha/4} \le 2p^{1-\varepsilon_2} + 4p^{1-\alpha/8},\end{aligned}$$

completing the proof of Lemma 2. □

Proof of Lemma 10

By the Cauchy-Schwarz inequality, we have

$$|T(A_2, B)|^2 \le \sqrt{p} \sum_{b_1, b \in B} |F(b, b_1)|,$$

where

$$F(b, b_1) = \sum_{\substack{a_2 \in A_2\\ b_2 \in \Omega_2(a_2)}} e_p\Big(\frac{b_1^2 - b^2}{4(a_1 - a_2)} - \frac{b_2(b_1 - b)}{2(a_1 - a_2)}\Big).$$

Consequently, by Hölder's inequality, we have

$$|T(A_2, B)|^2 \le \sqrt{p}|B|^{2-2/m}\Big(\sum_{b_1, b \in B} |F(b, b_1)|^m\Big)^{1/m}. \tag{6.8}$$

Next, we have

$$\begin{aligned}\sum_{b_1, b \in B} |F(b, b_1)|^m &\le \sum_{\substack{x \in B+B,\\ y \in B-B}} \Big|\sum_{\substack{a_2 \in A_2,\\ b_2 \in \Omega_2(a_2)}} e_p\Big(\frac{xy}{4(a_1 - a_2)} - \frac{b_2 y}{2(a_1 - a_2)}\Big)\Big|^m\\ &\le \sum_{y \in B-B} \sum_{\substack{a_2^{(i)} \in A_2\\ b_2^{(i)} \in \Omega_2(a_2^{(i)})\\ 1 \le i \le m}} \Big|\sum_{x \in B+B} e_p\Big(\frac{xy}{4} \sum_{i=1}^{m/2} \Big[\frac{1}{a_1 - a_2^{(i)}} - \frac{1}{a_1 - a_2^{(i+m/2)}}\Big]\Big)\Big|.\end{aligned}$$

Hence, for some complex numbers $\varepsilon_{y,\xi}$ of modulus less than or equal to 1, we have

$$\sum_{b_1,b\in B}|F(b,b_1)|^m \le M_2^m \sum_{y\in B-B}\sum_{\xi\in\mathbb{F}_p}\lambda(\xi)\varepsilon_{y,\xi}\sum_{x\in B+B} e_p(xy\xi/4), \tag{6.9}$$

where

$$\lambda(\xi)=\Big|\Big\{a^{(1)},\dots,a^{(m)}\in A_2:\ \sum_{i=1}^{m/2}\Big(\frac{1}{a_1-a^{(i)}}-\frac{1}{a_1-a^{(i+m/2)}}\Big)=\xi\Big\}\Big|.$$

By (2.4), we have

$$\lambda(0)\le (m/2)!|A_2|^{m/2}. \tag{6.10}$$

Let

$$\zeta'(z)=\sum_{\substack{y\in B-B\\ \xi\in\mathbb{F}_p^*\\ y\xi=z}}\varepsilon_{y,\xi}\lambda(\xi),\qquad \zeta(z)=\sum_{\substack{y\in B-B\\ \xi\in\mathbb{F}_p^*\\ y\xi=z}}\lambda(\xi).$$

Then $|\zeta'(z)|\le\zeta(z)$. By Hölder's inequality,

$$\begin{aligned}
\Big|\sum_{y\in B-B}\sum_{\xi\in\mathbb{F}_p^*}\lambda(\xi)\varepsilon_{y,\xi}\sum_{x\in B+B} e_p(xy\xi/4)\Big|
&=\Big|\sum_{\substack{x\in B+B\\ z\in\mathbb{F}_p}}\zeta'(z)e_p(xz/4)\Big|\\
&\le |B+B|^{3/4}\Big(\sum_{x\in\mathbb{F}_p}\Big|\sum_{z\in\mathbb{F}_p}\zeta'(z)e_p(xz/4)\Big|^4\Big)^{1/4}\\
&=|B+B|^{3/4}\Big(\sum_{x\in\mathbb{F}_p}\Big|\sum_{z'\in\mathbb{F}_p}(\zeta'*\zeta')(z')e_p(xz'/4)\Big|^2\Big)^{1/4}\\
&=|B+B|^{3/4}\|\zeta'*\zeta'\|_2^{1/2}p^{1/4}\\
&\le |B+B|^{3/4}\|\zeta*\zeta\|_2^{1/2}p^{1/4}.
\end{aligned} \tag{6.11}$$

As $\zeta(z) = \sum_\xi 1_{B-B}(z/\xi)$, we have by the triangle inequality,

$$\|\zeta * \zeta\|_2 \leq \sum_{\xi,\xi' \in \mathbb{F}_p^*} \lambda(\xi)\lambda(\xi')\|1_{\xi(B-B)} * 1_{\xi'(B-B)}\|_2$$

$$= \sum_{\xi,\xi' \in \mathbb{F}_p^*} \lambda(\xi)\lambda(\xi')\|1_{B-B} * 1_{(\xi'/\xi)(B-B)}\|_2. \tag{6.12}$$

Define the probability measure λ_1 by

$$\lambda_1(\xi) = \frac{\lambda(\xi)}{\|\lambda\|_1} = \frac{\lambda(\xi)}{|A_2|^m}.$$

The sum $\sum_{\xi \in \mathbb{F}_p} \lambda(\xi)^2$ is equal to the number of solutions of the equation

$$\frac{1}{a_1 - a^{(1)}} + \cdots + \frac{1}{a_1 - a^{(m)}} - \frac{1}{a_1 - a^{(m+1)}} - \frac{1}{a_1 - a^{(2m)}} = 0$$

with $a^{(1)}, \ldots, a^{(2m)} \in A_2$. By (2.4), this has only trivial solutions, and thus

$$\sum_{\xi \in \mathbb{F}_p} \lambda(\xi)^2 \leq m!|A_2|^m. \tag{6.13}$$

Now we are in position to apply Corollary 2 which gives, for any $\xi' \in \mathbb{F}_p^*$,

$$\sum_{\xi \in \mathbb{F}_p^*} \lambda_1(\xi)\|1_{B-B} * 1_{(\xi'/\xi)(B-B)}\|_2$$

$$\ll (\|\lambda_1\|_2 + |B-B|^{-1/2} + |B-B|^{1/2}p^{-1/2})^{c_0}|B-B|^{3/2}. \tag{6.14}$$

By (6.2) and (6.13), we have

$$\|\lambda_1\|_2 \leq \sqrt{m!}\,p^{-m\gamma/4}.$$

By (6.3) and $\alpha < 0.01$, we have

$$|B-B| \geq |B| \geq p^{1/2-6\alpha} \geq p^{0.44}.$$

On the other hand, it follows from (6.3) and (6.4) that

$$|B-B| \leq p^{1/2+28\alpha} \leq p^{0.78}.$$

Since $m\gamma \leq 1/3$, we get

$$\|\lambda_1\|_2 + |B-B|^{-1/2} + |B-B|^{1/2}p^{-1/2} \leq \sqrt{m!}\,p^{-m\gamma/4} + p^{-0.1} \leq p^{-m\gamma/5}.$$

So, by (6.12) and (6.14), we have

$$\begin{aligned}\|\zeta * \zeta\|_2 &\le |A_2|^{2m} \sum_{\xi' \in \mathbb{F}_p^*} \lambda_1(\xi') \sum_{\xi \in \mathbb{F}_p^*} \lambda_1(\xi) \|1_{B-B} * 1_{(\xi'/\xi)(B-B)}\|_2 \\ &\ll |A_2|^{2m} p^{-(c_0/5)m\gamma} |B-B|^{3/2}.\end{aligned}$$

Subsequent application of (6.9), (6.10), and (6.11) gives

$$\begin{aligned}\sum_{b_1, b \in B} |F(b, b_1)|^m &\le (\tfrac{m}{2})! (M_2|A_2|)^m |A_2|^{-m/2} |B-B||B+B| \\ &\quad + O(M_2^m |A_2|^m |B-B|^{3/4} |B+B|^{3/4} p^{-(c_0/10)m\gamma} p^{1/4}).\end{aligned}$$

Due to Lemma 4, condition (6.4) implies that

$$|B+B| \le p^{56\alpha} |B|.$$

By (6.3), $p^{1/4} \le |B|^{1/2} p^{3\alpha}$. Recalling $\gamma \le \alpha$, (2.9), (6.2), and (6.4), we conclude that

$$\begin{aligned}\sum_{b_1, b \in B} |F(b, b_1)|^m &\ll (\tfrac{m}{2})! (2\sqrt{p})^m p^{-m\gamma/4} p^{84\alpha} |B|^2 \\ &\quad + (2\sqrt{p})^m p^{63\alpha} |B|^{3/2} p^{-(c_0/10)m\gamma} p^{1/4} \\ &\le |B|^2 p^{m/2 - (c_0/10)m\gamma + 84\alpha}.\end{aligned}$$

Plugging the last estimate into (6.8), we get

$$|T(A_2, B)|^2 \le \sqrt{p} |B|^{2-2/m} (|B|^2 p^{m/2-(c_0/10)m\gamma+84\alpha})^{1/m} \le |B|^2 p^{1+84\alpha/m-(c_0/10)\gamma}. \qquad \square$$

7. Thin sets with small Fourier coefficients

Denote by $(a^{-1})_m$ the inverse of a modulo m. It is easy to see, for relatively prime integers a, b, that

$$\frac{(a^{-1})_b}{b} + \frac{(b^{-1})_a}{a} - \frac{1}{ab} \in \mathbb{Z}. \tag{7.1}$$

LEMMA 11

Let $P \ge 4$, $S \ge 2$, and let R be a positive integer. Suppose that, for every prime $p \le P$, S_p is a set of integers in $(-p/2, p/2)$. Suppose that q is a prime satisfying $q \ge RP^2$. Then the numbers $r + s^{(p)}(p^{-1})_q$, where $1 \le r \le R$, $P/2 < p \le P$, and $s^{(p)} \in S_p$ are distinct modulo q.

Proof
Suppose that

$$r_1 + s_1^{(p_1)}(p_1^{-1})_q \equiv r_2 + s_2^{(p_2)}(p_2^{-1})_q \pmod q.$$

Multiplying both sides by $p_1 p_2$ gives

$$r_1 p_1 p_2 + p_2 s_1^{(p_1)} \equiv r_2 p_1 p_2 + p_1 s_2^{(p_2)} \pmod q.$$

By hypothesis, we have

$$|(r_1 - r_2) p_1 p_2 + p_2 s_1^{(p_1)} - p_1 s_2^{(p_2)}| < (R-1)P^2 + P^2 \le q,$$

thus

$$(r_1 - r_2) p_1 p_2 = -p_2 s_1^{(p_1)} + p_1 s_2^{(p_2)}.$$

The right side is divisible by $p_1 p_2$, and the absolute value of the right side is $< p_1 p_2$; hence both sides are zero, $r_1 = r_2$, $p_1 = p_2$, and $s_1^{(p_1)} = s_2^{(p_2)}$. □

For brevity, we write $e(z)$ for $e^{2\pi i z}$ is what follows.

LEMMA 12
Let $P \ge 4$, $S \ge 2$, and let R be a positive integer. Suppose that, for every prime $p \in (P/2, P]$, S_p is a multiset of integers in $(-p/2, p/2)$, $|S_p| = S$, and $|f_{S_p}| \le \varepsilon$. Suppose that q is a prime satisfying $q > P$. Then the multiset

$$T = \left\{ r + s^{(p)}(p^{-1})_q : 1 \le r \le R,\, P/2 < p \le P,\, s^{(p)} \in S_p \right\}$$

of residues modulo q satisfies

$$|f_T| \le \varepsilon + \frac{2/\sqrt{3}}{R} + \frac{\log(q/3)}{V \log(P/2)}, \tag{7.2}$$

where V is the number of primes in $(P/2, P]$.

Proof
Since $|f_T(k)| = |f_T(q-k)|$, we may assume without loss of generality that $1 \le k < q/2$. We have

$$f_T(k) = A(k) \sum_{P/2 < p \le P} B(p, k),$$

where

$$A(k)=\sum_{r\le R} e\Big(\frac{kr}{q}\Big), \qquad B(p,k)=\sum_{s\in S_p} e\Big(\frac{ks(p^{-1})_q}{q}\Big).$$

Trivially,

$$|A(k)|\le \min\Big(R, \frac{2}{|e(k/q)-1|}\Big). \tag{7.3}$$

If $k\ge q/3$, we use the trivial bound $|B(p,k)|\le S$, and we conclude that

$$\frac{|f_T(k)|}{|T|}\le \frac{2}{R|e(k/q)-1|}\le \frac{2}{R|e(1/3)-1|}=\frac{2/\sqrt{3}}{R}.$$

Now assume that $k\le q/3$. If $p|k$, then $|B(p,k)|\le S$. When $p\nmid k$, by (7.1), we get

$$\begin{aligned}|B(p,k)| &= \Big|\sum_{s\in S_p} e\Big(-\frac{sk(q^{-1})_p}{p}+\frac{ks}{pq}\Big)\Big| \\ &\le |S_p|\max_{s\in S_p}\Big|e\Big(\frac{ks}{pq}\Big)-1\Big| + \Big|\sum_{s\in S_p} e\Big(\frac{sk(q^{-1})_p}{p}\Big)\Big| \\ &\le \big(\varepsilon+|e(k/2q)-1|\big)S.\end{aligned}$$

Since there are $\le \log k/\log(P/2)$ primes $p|k$ with $p>P/2$, we have

$$\sum_{P/2<p\le P}|B(p,k)|\le \big(\varepsilon+|e(k/2q)-1|\big)SV+\frac{\log(q/3)}{\log(P/2)}S.$$

Combining our estimates for $|A(k)|$ and $|B(p,k)|$, we arrive at

$$\begin{aligned}\frac{|f_T(k)|}{|T|} &\le \varepsilon+\frac{\log(q/3)}{V\log(P/2)}+\frac{2}{R}\Big|\frac{e(k/2q)-1}{e(k/q)-1}\Big| \\ &\le \varepsilon+\frac{\log(q/3)}{V\log(P/2)}+\frac{2/\sqrt{3}}{R}.\end{aligned}$$

□

For a specific choice of S_p, the inequality (7.2) can be strengthened.

LEMMA 13
Let $P\ge 4$, and let R be a positive integer. For every prime $p\in(P/2,P]$, denote by S_p the set of all integers in $(-p/2,p/2)$. Suppose that q is a prime satisfying $q>P$.

Then the multiset

$$T = \left\{r + s^{(p)}(p^{-1})_q : 1 \le r \le R,\, P/2 < p \le P,\, s^{(p)} \in S_p\right\}$$

of residues modulo q satisfies

$$|f_T| \le \frac{W}{2V} + \frac{W}{RV}\left(1 + \frac{\log\left(1 + \frac{V}{W}\right)}{2}\right), \tag{7.4}$$

where V is the number of primes in $(P/2, P]$ and where $W = 4(\log(q/2))/(\log(P/2))$.

Proof

Again, we may assume without loss of generality that $1 \le k < q/2$. We use notation from the proof of Lemma 12. If $p|k$, we use the trivial estimate $|B(p,k)| \le |S_p| \le P$. Now there are $\le \log(q/2)/\log(P/2)$ primes $p|k$ with $p > P/2$. When $p \nmid k$, by (7.1), we get

$$|B(p,k)| \le \Big|\sum_{s=(1-p)/2}^{(p-1)/2} e\Big(-\frac{sk(q^{-1})_p}{p} + \frac{ks}{pq}\Big)\Big| = \frac{\left|e\left(\frac{k}{q}\right) - 1\right|}{\left|e\left(-\frac{k(q^{-1})_p}{p} + \frac{k}{pq}\right) - 1\right|}$$

$$\le \frac{\left|e\left(\frac{k}{q}\right) - 1\right|}{\left|e\left(-\frac{2|k(q^{-1})_p| - 1}{2p}\right) - 1\right|} \le \frac{\left|e\left(\frac{k}{q}\right) - 1\right|}{\left|e\left(-\frac{2|k(q^{-1})_p| - 1}{2P}\right) - 1\right|},$$

where it is assumed that $k(q^{-1})_p \in (-p/2, p/2)$. For $a = 1, \dots, [(P-1)/2]$, we denote

$$P_a = \left\{p \in (P/2, P] : |k(q^{-1})_p| = a\right\}.$$

Taking into account that $|e(u) - 1|^{-1} \le 1/(4u)$ for $u \in (0, 1/2]$, we get

$$\sum_{p\nmid k} |B(p,k)| \le \frac{P}{2}\left|e\left(\frac{k}{q}\right) - 1\right| \sum_a |P_a| \frac{1}{2a-1}. \tag{7.5}$$

If $k(q^{-1})_p = \pm a$, then $k \pm aq$ is divisible by p. But $|k \pm aq| \le Pq/2$. Therefore, the number of prime divisors $p > P/2$ of any number $k \pm aq$ is at most $(\log q)/\log(P/2) + 1$, and, for any a, we get

$$|P_a| \le 2\left[\frac{\log q}{\log(P/2)}\right] + 2 \le W.$$

Let $A = [V/W] + 1$. We have

$$\sum_a |P_a| \frac{1}{2a-1} \le \sum_{a \le A} |P_a| \frac{1}{2a-1} + \Big(V - \sum_{a\le A} |P_a| \Big) \frac{1}{2A+1}$$
$$\le \sum_{a\le A} W \frac{1}{2a-1} + \Big(V - \sum_{a \le A} W \Big) \frac{1}{2A+1} \le \sum_{a\le A} W \frac{1}{2a-1}$$
$$\le W\Big(1 + \frac{\log A}{2}\Big) \le W\Big(1 + \frac{\log\big(1+\frac{V}{W}\big)}{2}\Big).$$

Combining our estimates for $|A(k)|$ and $|B(p,k)|$ ((7.3) and (7.5)), we arrive at

$$\frac{|f_T(k)|}{|T|} \le \frac{2\log(q/2)}{V\log(P/2)} + \frac{PW/2}{R(P-2)V/2}\Big(1 + \frac{\log\big(1+\frac{V}{W}\big)}{2}\Big)$$
$$= \frac{W}{2V} + \frac{W}{RV}\Big(1 + \frac{\log\big(1+\frac{V}{W}\big)}{2}\Big). \qquad \square$$

Remark 8
Applying Lemma 12 for all primes q in a dyadic interval, we can then feed these multisets $T = T_q$ back into the lemma and iterate.

Using explicit estimates for counts of prime numbers (see [39]), we have the following.

PROPOSITION 4
For $P \ge 250$, there are more than $2P/(5\log(P/2))$ primes in $(P/2, P]$. For any $P > 2$, there are at most $0.76P/\log P$ primes in $(P/2, P]$.

Using Proposition 4, we obtain a more convenient version of Lemma 13.

LEMMA 14
Let $P \ge 250$. For every prime $p \in (P/2, P]$, denote by S_p the set of all nonzero integers in $(-p/2, p/2)$. Suppose that q is a prime satisfying $q > P$, and suppose that $R \ge 1 + \log(1 + 0.26P/\log(2q))/2$ is a positive integer. Then the multiset

$$T = \big\{ r + s^{(p)}(p^{-1})_q : 1 \le r \le R,\ P/2 < p \le P,\ s^{(p)} \in S_p \big\}$$

of residues modulo q satisfies

$$|f_T| \le 15 \frac{\log q}{P}. \tag{7.6}$$

Proof
We use the notation of Lemma 13. By Proposition 4, we have

$$\frac{W}{2V} \leq 5\frac{\log q}{P}. \tag{7.7}$$

On the other hand, using Proposition 4 again, we get

$$\frac{V}{W} \leq \frac{0.76P/\log P}{4\log(q/2)/\log(P/2)} \leq 0.19\frac{P}{\log(q/2)} \leq 0.26\frac{P}{\log(2q)}.$$

Hence, we have

$$R \geq 1 + \frac{\log\left(1+\frac{V}{W}\right)}{2}.$$

Now the inequality (7.6) follows from (7.7) and (7.4). □

Using just one iteration, one can get the following effective result on thin sets with small Fourier coefficients of nearly the same strength as (1.12).

COROLLARY 5
For sufficiently large prime N and μ such that $N^{-1/2}\log^2 N \leq \mu < 1$, there is a set T of residues modulo N so that

$$|f_T| \leq \mu, \qquad |T| = O\Big(\frac{L_1^2}{\mu^2}\Big(\frac{1+\log(1/\mu)}{L_2+\log(1/\mu)}\Big)\Big).$$

Proof
We choose $P = (15/\mu)\log N$ and

$$R = \left\lceil 2 + \frac{\log(1+5/\mu)}{2}\right\rceil \geq 1 + \frac{\log\left(1+\frac{0.26P}{\log N}\right)}{2}.$$

Clearly, $R \ll 1+\log(1/\mu)$. Let T be the multiset constructed in Lemma 14. We have $|f_T| \leq \mu$. By Lemma 11, T is a set. Moreover, we have

$$|T| \ll P^2\frac{1+\log(1/\mu)}{\log P} \ll \frac{P^2(1+\log(1/\mu))}{L_2+\log(1/\mu)}.$$ □

Proof of Theorem 2
We choose real parameters P_0, P_1 and positive integers R_0, R_1 so that

$$P_0 \geq 250, \qquad P_1 \geq 2R_0 P_0^2, \qquad N \geq R_1 P_1^2, \qquad R_0 \geq 1 + \frac{\log\left(1 + \frac{0.26 P_0}{\log P_1}\right)}{2}, \tag{7.8}$$

and also that

$$\frac{2/\sqrt{3}}{R_1} + 15\frac{\log P_1}{P_0} + \frac{5\log N}{2P_1} \leq \mu. \tag{7.9}$$

For $P_0/2 < p \leq P_0$, let S_p be the set of integers in $(-p/2, p/2)$. By Lemmas 11 and 14 and (7.8), for each prime $q \in (P_1/2, P_1]$, there is a set $T = S_q$ of residues modulo q such that

$$|f_{S_q}| \leq 15\frac{\log(P_1)}{P_0} =: \varepsilon_1.$$

By an application of Lemmas 11 and 12 with $P = P_1$, $\varepsilon = \varepsilon_1$, $q = N$, and $S = R_0 \sum_{P_0/2<p\leq P_0} p$, together with (7.9), there is a set T of residues modulo N so that

$$|f_T| \leq \varepsilon_1 + \frac{2/\sqrt{3}}{R_1} + \frac{5\log N}{2P_1} \leq \mu.$$

Using Proposition 4, we find that

$$|T| \leq (0.76)^2 R_0 R_1 \frac{P_1 P_0^2}{(\log P_0)(\log P_1)}.$$

Recalling that $1/\mu \in \mathbb{N}$, we now take

$$R_0 = \left[2 + \log(1 + 13/\mu)/2\right], \qquad R_1 = 4/\mu,$$
$$P_1 = (8/\mu)\log N, \qquad P_0 = (45/\mu)\log P_1$$

so that (7.9) follows immediately. Condition (1.13) implies (7.8) for large enough N. □

Remark 9
Theorem 2 supersedes Corollary 5 for $\mu \gg L_1^{-1/2} L_2^{1/2}$.

8. An explicit construction for Turán's problem

Proof of Theorem 3
We follow the proof of Theorem 2 and Lemma 12. We choose real parameters P_0, P_1 and a positive integer R_0 so that

$$P_0 \geq 250, \qquad P_1 > 2P_0^2, \qquad R_0 \geq 1 + \frac{\log\left(1 + \frac{0.26P_0}{\log P_1}\right)}{2}, \tag{8.1}$$

and also that

$$15\frac{\log P_1}{P_0} + \frac{5\log N}{2P_1} \leq \mu. \tag{8.2}$$

For $P_0/2 < p \leq P_0$, let S_p be the set of integers in $(-p/2, p/2)$. By Lemma 14 and (8.1), for each prime $q \in (P_1/2, P_1]$, there is a multiset $T = S_q$ of residues modulo q such that

$$|f_{S_q}| \leq 15\frac{\log(P_1)}{P_0} := \varepsilon_1. \tag{8.3}$$

We have $|S_q| = S$ for all q, where $S = R_0 \sum_{P_0/2<p\leq P_0} p$. Now define a multiset $\{z_1, \ldots, z_n\}$ as a union of multisets $\{e(s/q) : s \in S_q, q \in (P_1/2, P_1]\}$. We have, for $1 \leq k \leq N$,

$$\sum_{j=1}^{n} z_j^k = \sum_{P_1/2<q\leq P_1} B(q,k), \qquad B(q,k) = \sum_{s\in S_q} e\left(\frac{ks}{q}\right).$$

If $q|k$, then $B(q,k) = S$. When $q \nmid k$, by (8.3), $|B(q,k)| \leq \varepsilon_1 S$. Therefore, we have

$$\sum_{q\nmid k} |B(q,k)| \leq \varepsilon_1 n. \tag{8.4}$$

The sum over $q|k$ is estimated in the same way as in Lemma 12:

$$\sum_{q|k} |B(q,k)| \leq \frac{\log N}{\log(P_1/2)} S. \tag{8.5}$$

Combining (8.4), (8.5), and using Proposition 4, we arrive at

$$\frac{1}{n}\left|\sum_{j=1}^{n} z_j^k\right| \leq \varepsilon_1 + \frac{5\log N}{2P_1},$$

as required. Moreover, by Proposition 4, we have

$$n \le (0.76)^2 R_0 \frac{P_1 P_0^2}{(\log P_0)(\log P_1)}.$$

Now we take R_0, P_0, P_1 the same as in the proof of Theorem 2 so that (8.2) follows immediately. The condition (1.14) implies (8.1) for large enough N. □

Remark 10
As in [1], one can construct thin sets T modulo N with $|T| = o(L_1 L_2)$ and $|f_T|$ small by iterating Lemma 12. Roughly speaking, applying Lemma 14 followed by r iterations of Lemma 12 produces sets T, with small $|f_T|$ as small as $|T| = O(L_1 L_{r+1})$, where L_j is the jth iterate of the logarithm of N. We omit the details.

Acknowledgments. The authors thank Ronald DeVore, Zeev Dvir, Venkatesan Guruswami, Piotr Indyk, Sina Jafarpour, Boris Kashin, Howard Karloff, Imre Leader, Igor Shparlinski, and Avi Wigderson for helpful conversations. The research was finished while the third and fourth authors were visiting the Institute for Advanced Study. The last three authors thank the Institute for Advanced Study for hospitality and excellent working conditions.

References

[1] M. AJTAI, H. IWANIEC, J. KOMLÓS, J. PINTZ, and E. SZEMERÉDI, *Construction of a thin set with small Fourier coefficients*, Bull. Lond. Math. Soc. **22** (1990), 583–590. MR 1099009

[2] N. ALON, O. GOLDREICH, J. HÅSTAD, and R. PERALTA, *Simple constructions of almost k-wise independent random variables*, Random Structures Algorithms **3** (1992), 289–304. MR 1164842

[3] J. ANDERSSON, *Explicit solutions to certain inf max problems from Turán power sum theory*, Indag. Math. (N.S.) **18** (2007), 189–194. MR 2352674

[4] ———, "On the solutions to a power sum problem" in *Analytic and Probabilistic Methods in Number Theory*, TEV, Vilnius, 2007. MR 2397135

[5] ———, *On some power sum problems of Montgomery and Turán*, Int. Math. Res. Not. IMRN (2008), no. 8, art. ID rnn015. MR 2428149

[6] R. BARANIUK, M. DAVENPORT, R. DEVORE, and M. WAKIN, *A simple proof of the restricted isometry property for random matrices*, Constr. Approx. **28** (2008), 253–263. MR 2453366

[7] A. BEN-AROYA and A. TA-SHMA, "Constructing small-bias sets from algebraic-geometric codes" in *2009 50th Annual IEEE Symposium on Foundations of Computer Science (Atlanta, 2009)*, IEEE Computer Soc., Los Alamitos, Calif., 2009, 191–197. MR 2648401

[8] R. BERINDE, A. GILBERT, P. INDYK, H. KARLOFF, and M. STRAUSS, *Combining geometry and combinatorics: A unified approach to sparse signal recovery*, preprint, 2008.

[9] B. BOLLOBÁS and I. LEADER, *Sums in the grid*, Discrete Math. **162** (1996), 31 – 48. MR 1425777

[10] J. BOURGAIN, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. **18** (2009), 1477 – 1502. MR 2481734

[11] J. BOURGAIN and M. Z. GARAEV, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. **146** (2009), 1 – 21. MR 2461864

[12] J. BOURGAIN and A. A. GLIBICHUK, *Multilinear exponential sum estimate in an arbitrary finite field*, preprint, to appear in J. Anal. Math.

[13] E. J. CANDÈS, *The restricted isometry property and its implications for compressed sensing*, C. R. Math. Acad. Sci. Paris **346** (2008), 589 – 592. MR 2412803

[14] E. J. CANDÈS, J. K. ROMBERG, and T. TAO, *Stable signal recovery from incomplete and inaccurate measurements*, Comm. Pure Appl. Math. **59** (2006), 1207 – 1223. MR 2230846

[15] E. J. CANDÈS and T. TAO, *Decoding by linear programming*, IEEE Trans. Inform. Theory **51** (2005), 4203 – 4215. MR 2243152

[16] ———, *Near-optimal signal recovery from random projections: Universal encoding strategies?* IEEE Trans. Inform. Theory **52** (2006), 5406 –5425. MR 2300700

[17] R. A. DEVORE, *Deterministic constructions of compressed sensing matrices*, J. Complexity **23** (2007), 918 – 925. MR 2371999

[18] D. L. DONOHO, M. ELAD, and V. N. TEMLYAKOV, *On the Lebesgue-type inequalities for greedy approximation*, J. Approx. Theory **147** (2007), 185 – 195. MR 2344318

[19] P. ERDÖS and A. RÉNYI, *A probabilistic approach to problems of Diophantine approximation*, Illinois J. Math. **1** (1957), 303 – 315. MR 0089226

[20] A. C. GILBERT, S. MUTHUKRISHNAN, and M. J. STRAUSS, "Approximation of functions over redundant dictionaries using coherence" in *The 14th Annual ACM-SIAM Symposium on Discrete Algorithms* (*Baltimore, 2003*), ACM, New York, 2003, 243 –252. MR 1974925

[21] E. D. GLUSKIN, *An octahedron is poorly approximated by random subspaces* (in Russian), Funktsional. Anal. i Prilozhen. **20**, no. 1 (1986), 14 – 20, 96; English translation in Funct. Anal. Appl. **20**, no. 1 (1986), 11 – 16. MR 0831044 149, 150, 151, 182 147 149 149 151 146 148, 149 146 165 161 160 161 146, 148 146 146 146 147 147 151 147 148

[22] S. GUREVICH and R. HADANI, *The statistical restricted isometry property and the Wigner semicircle distribution of incoherent dictionaries*, preprint, arXiv:0812.2602v1 [CS.IT]

[23] V. GURUSWAMI and M. SUDAN, "List decoding algorithms for certain concatenated codes" in *Thirty-Second Annual ACM Symposium on Theory of Computing (Portland, 2000)*, ACM, New York, 2000. 181 – 190. MR 2114510

[24] K. F. IRELAND and M. I. ROSSEN, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math. **84**, Springer, New York, 1982. MR 0661047

[25] W. B. JOHNSON and J. LINDENSTRAUSS, "Extensions of Lipschitz mappings into a Hilbert space" in *Conference in Modern Analysis and Probability (New Haven, 1982)*, Contemp. Math. **26**, Amer. Math. Soc., Providence, 1984, 189 – 206. MR 0737400 146 148 156 146

[26] B. S. KASHIN, *The diameters of octahedra*, Uspekhi Mat. Nauk **30** (1975), 251 – 252.

[27] ———, *Diameters of some finite-dimensional sets and classes of smooth functions* (in Russian), Izv. Ross. Akad. Nauk Ser. Mat. **41** (1977), 334 – 351; English translation in Math. USSR Izv. **11** (1977), 317 – 333.

[28] N. M. KATZ, *An estimate for character sums*, J. Amer. Math. Soc. **2** (1989), 197 – 200. MR 0965007

[29] V. I. LEVENSHTEĬN, *Bounds for packings of metric spaces and some of their applications* (in Russian), Problemy Tekhn. Kibernet. Robot. **40** (1983), 43 – 110. MR 0717357

[30] E. LIU and V. N. TEMLYAKOV, *Orthogonal super greedy algorithm and applications in compressed sensing*, preprint, 2010.

[31] E. LIVSHITZ, *On efficiency of orthogonal matching pursuit*, preprint, arXiv:1004.3946vl [math.NA] 147 146 150, 151 148 146 147

[32] S. MENDELSON, A. PAJOR, and N. TOMCZAK-JAEGERMANN, *Reconstruction and subgaussian operators in asymptotic geometric analysis*, Geom. Funct. Anal. **17** (2007), 1248 – 1282. MR 2373017

[33] H. L. MONTGOMERY, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Reg. Conf. Sec. Math. **84**, Amer. Math. Soc., Providence, 1994. MR 1297543

[34] D. NEEDLE and R. VERSHYNIN, *Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit*, Found. Comput. Math. **9** (2009), 317 – 334. MR 2496554 146 149 146

[35] J. NELSON and V. N. TEMLYAKOV, *On the size of incoherent systems*, preprint, to appear in J. Approx. Theory. 146, 147, 148

[36] G. I. PEREL'MUTER and I. E. SHPARLINSKIĬ, *Distribution of primitive roots in finite fields* (in Russian), Uspekhi Mat. Nauk **45**, no. 1 (1990), 185 – 186; English translation in Russian Math. Surveys **45**, no. 1 (1990), 223 – 224. MR 1050940 150

[37] A. PRÉKOPA, *Logarithmic concave measures with application to stochastic programming*, Acta Sci. Math. (Szeged) **32** (1971), 301 – 316. MR 0315079 166

[38] A. RAZBOROV, E. SZEMERÉDI, and A. WIGDERSON, *Constructing small sets that are uniform in arithmetic progressions*, Combin. Probab. Comput. **2** (1993), 513 – 518. MR 1264723 150

[39] J. B. ROSSER and L. SCHOENFELD, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64 – 94. MR 0137689 178

[40] M. RUDELSON and R. VERSHYNIN, *On sparse reconstruction from Fourier and Gaussian measurements*, Comm. Pure Appl. Math. **61** (2008), 1025 – 1045. MR 2417886 146

[41] S. B. STECHKIN, *Some extremal properties of trigonometric sums* (in Russian), Mat. Zametki **55**, no. 2 (1994), 130 – 143; English translation in Math. Notes **55** nos. 1 – 2 (1994), 195 – 203. MR 1275328

[42] ———, *The Turán problem for trigonometric sums* (in Russian), Tr. Mat. Inst. Steklova **219** (1997), 335 – 339; English translation in Proc. Steklov Inst. Math. **219**, no. 4 (1997), 329 – 333. MR 1642288

[43] T. TAO, *Open question: deterministic uup matrices*, preprint, http://www.terrytao.wordpress.com/2007/07/02/open-question-deterministic-uup-matrices (accessed 5 May 2011).

[44] T. TAO and V. VU, *Additive Combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge Univ. Press, Cambridge, 2006. MR 2289012

[45] P. TURÁN, *On a New Method of Analysis and its Applications*, Pure Appl. Math. (New York), John Wiley, New York, 1984. MR 0749389

[46] I. M. VINOGRADOV, *An Introduction to the Theory of Numbers*, Pergamon Press, London and New York, 1955. MR 0070644

[47] D. R. WOODALL, *A theorem on cubes*, Mathematika **24** (1977), 60 – 62. MR 0453568 149 149 147 160, 163 149 169 165

Bourgain
School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA; bourgain@math.ias.edu

Dilworth
Department of Mathematics, University of South Carolina, Columbia, South Carolina 29208, USA; dilworth@math.sc.edu

Ford
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA; ford@math.uiuc.edu

Konyagin
Steklov Mathematical Institute, Moscow 119991, Russia; konyagin@mi.ras.ru

Kutzarova
Institute of Mathematics, Bulgarian Academy of Sciences, Sofia, Bulgaria;
current: Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA; denka@math.uiuc.edu