Breaking the k^2 Barrier for Explicit RIP Matrices

[Extended Abstract] *

Jean Bourgain
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540
bourgain@math.ias.edu

S. J. Dilworth
Department of Mathematics
University of South Carolina
Columbia, SC 29208
dilworth@math.sc.edu

Kevin Ford
Department of Mathematics
University of Illinois
Urbana, IL 61801
ford@math.uiuc.edu

Sergei V. Konyagin
Steklov Mathematical Institute
8 Gubkin Street
Moscow, 119991, Russia
konyagin@mi.ras.ru

Denka Kutzarova
Institute of Mathematics
Bulgarian Acad. Sciences
Sofia, Bulgaria.
denka@math.uiuc.edu

ABSTRACT

We give a new explicit construction of $n \times N$ matrices satisfying the Restricted Isometry Property (RIP). Namely, for some $\varepsilon > 0$, large k and $k^{2-\varepsilon} \le N \le k^{2+\varepsilon}$, we construct RIP matrices of order k with $n = O(k^{2-\varepsilon})$. This overcomes the natural barrier $n \gg k^2$ 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.

Categories and Subject Descriptors

E.4 [**Coding and information theory**]: Data compaction and compression

Keywords

Compressed sensing, restricted isometry property

General Terms

Theory

1. INTRODUCTION

Suppose $1 \le k \le n \le N$ 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[1]. An $n \times N$ matrix Φ is said to satisfy the Restricted Isometry Property (RIP) of order k with constant δ if, for all k-sparse vectors $\mathbf{x}$, we have

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

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), 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) with the same parameters k, δ.

We know from Candès, Romberg and Tao that matrices satisfying RIP have application to sparse signal recovery (see [9, 10, 11]). A variant of RIP (with the ℓ_2 norm in (1) replaced by the ℓ_1 norm) is also useful for such problems [3]. A weak form of RIP, where (1) holds for most k-sparse $\mathbf{x}$ (called Statistical RIP) is studied in [17]. Other applications of RIP matrices may be found in [24, 25, 27].

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 with high probability, Φ will have the required properties for k of order $\delta n / \log(2N/n)$. See [10, 26]; also [2] for a proof based on the Johnson-Lindenstrauss lemma [19]. The first result of similar type for these matrices is due to Kashin [22]. See also [12, 29] 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

$$k = O\left(\frac{\delta n}{\log(2N/n)}\right)$$

for every RIP matrix [28].

It is an open problem to find good *explicit* constructions of RIP matrices; see T. Tao's Weblog [30] 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

$$\mu := \max_{r \ne s} |\langle \mathbf{u}_r, \mathbf{u}_s \rangle|. \qquad (2)$$

Systems of vectors with small coherence are also known as *spherical codes*. Some other applications of matrices with

*A full version of this paper is available as *Explicit constructions of RIP matrices and related problems* at `arXiv:1008.4535`, and will appear [6].

[1] We use $\mathbb{C}$ for the set of complex numbers.

STOC'11, June 6–8, 2011, San Jose, California, USA.

small coherence may be found in [14, 15, 25]. For any k-sparse vector $\mathbf{x}$,

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

Thus, if Φ has coherence μ, then Φ satisfies RIP of order k with constant $\delta = (k-1)\mu$.

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

$$\mu = O\left(\frac{\log N}{\sqrt{n}\log n}\right). \tag{3}$$

In particular, such examples have been constructed by Kashin [21], Alon, Goldreich, Håstad and Peralta [1], DeVore [13], and Nelson and Temlyakov [28]. Therefore, these matrices satisfy RIP with constant δ and order [2]

$$k \asymp \delta \frac{\sqrt{n}\log n}{\log N}. \tag{4}$$

By contrast, there is a universal lower bound

$$\mu \gg \left(\frac{\log N}{n\log(n/\log N)}\right)^{1/2} \ge \frac{1}{\sqrt{n}}, \tag{5}$$

valid for $2\log N \le n \le N/2$ and all Φ, due to Levenshtein [23] (see also [16] and [28]). 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 are effective constants $\varepsilon > 0$, $\varepsilon' > 0$ and an explicit number k_0 such that for any positive integers $k \ge k_0$ and $k^{2-\varepsilon} \le N \le k^{2+\varepsilon}$, there is an explicit $n \times N$ RIP matrix of order k with $n = O(k^{2-\varepsilon})$ and constant $\delta = k^{-\varepsilon'}$.*

REMARK 1. *For application to sparse signal recovery, it is sufficient to take fixed $\delta < \sqrt{2} - 1$ [9].*

The proof of Theorem 1 uses a result on additive energy of sets (Corollary 1), estimates for sizes of sumsets in product sets (Theorem 2), and bounds for exponential sums over products of sets possessing special additive structure (Lemma 8).

The construction given in this paper is a bit different that that given in the authors' paper [6], and provides a larger value of ε. The value of ε depends on several results from additive combinatorics, in particular a constant c_0 (Proposition 1, Section 3.2)) and a constant from the Balog–Szemerédi–Gowers lemma (see Lemma 6 in Section 3.2). The construction in [6] gives ε proportional to c_0^3, while the construction in this paper gives $\varepsilon = c_0^2/2530000$. The best known value for c_0 is $c_0 = \frac{1}{10430}$ [8] and this implies $\varepsilon \approx 3.6 \cdot 10^{-15}$ in Theorem 1, vs. the value $\varepsilon \approx 2 \cdot 10^{-22}$ in [6]. It is possible that c_0 can be taken close to 1, and this would give a much better constant $\varepsilon \approx 3 \cdot 10^{-7}$.

2. OUTLINE OF THE NEW METHOD

2.1 Construction of the matrix in Theorem 1

We fix a positive integer $m \ge 100$ and let p be a large prime. By $\mathbb{F}_p$ we denote the field of the residues modulo p, and 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 $\mathbf{u}_{a,b}, a \in \mathscr{A} \subset \mathbb{F}_p, b \in \mathscr{B} \subset \mathbb{F}_p$ where

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

We take

$$\alpha = \frac{1}{2m}, \qquad \mathscr{A} = \{1, 2, \dots \lfloor p^\alpha \rfloor\}. \tag{6}$$

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

$$\beta = \frac{1}{2.01m}, \quad r = \left\lfloor \frac{\beta \log p}{\log 2} \right\rfloor, \quad M = \lfloor 2^{2.01m-1} \rfloor,$$

and let

$$\mathscr{B} = \left\{ \sum_{j=1}^{r} x_j (2M)^{j-1} \,:\, x_1, \dots, x_r \in \{0, \dots, M-1\} \right\}. \tag{7}$$

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

$$|\mathscr{B}| \asymp p^{1-\beta}. \tag{8}$$

It follows from (6) and (8) that

$$|\mathscr{A}||\mathscr{B}| \asymp p^{1+\alpha-\beta} \asymp p^{1+1/(402m)}.$$

Given large k and $k^{2-\varepsilon} \le N \le k^{2+\varepsilon}$, let p be a prime in the interval $[k^{2-\varepsilon}, 2k^{2-\varepsilon}]$ (such p exists by Bertrand's postulate). Our ε will satisfy $\varepsilon < \frac{1}{402m}$, hence $N \le |\mathscr{A}||\mathscr{B}|$. Take Φ to be the matrix formed by the first N columns of Φ_p.

2.2 Proof of Theorem 1: Overview

The proof that the matrix Φ defined above has the required properties for Theorem 1 proceeds in several stages. First, we show that in (1) we need only consider vectors $\mathbf{x}$ whose components are 0 or 1 (so-called *flat* vectors).

LEMMA 1 ([6, LEMMA 1]). *Let $k \ge 2^{10}$ and 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 $J_1, J_2 \subset \{1, \dots, N\}$ 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 property of order $2sk$ with constant $44s\sqrt{\delta}\log k$.

Next, we show that Φ satisfies (1) with flat vectors, order $k = \lfloor \sqrt{p} \rfloor$ and $\delta \le p^{-\varepsilon'}$ for some $\varepsilon' > 0$. We prove the required estimates for matrices formed from more general sets $\mathscr{A}$ and $\mathscr{B}$ (actually, sequences of sets depending on p) having certain additive properties. Namely, fix an even, positive integer m and a positive real number $\alpha < \frac{1}{2m-1}$, and for large p, suppose $|\mathscr{A}'| \le p^\alpha$. Also suppose that for every $\eta > 0$ there is a constant $C(\eta)$ (independent of p), so

[2] For convenience, we utilize the Vinogradov notation $a \ll b$, which means $a = O(b)$, and the Hardy notation $a \asymp b$, which means $b \ll a \ll b$; that is, a and b have the same order.

that for each $a \in \mathscr{A}$, $\mathscr{A}' \subseteq \mathscr{A}$ and $m' \le m$, the number, $N(a, \mathscr{A}', m')$, of solutions of the congruence

$$\sum_{j=1}^{m'} \frac{1}{a-a_j} \equiv \sum_{j=m'+1}^{2m'} \frac{1}{a-a_j} \pmod p$$

with $a_1, \dots, a_{2m'} \in \mathscr{A}' \backslash \{a\}$, satisfies

$$N(a, \mathscr{A}', m') \le C(\eta) |\mathscr{A}'|^{m'} p^{\eta}. \qquad (9)$$

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

$$\forall S \subset \mathscr{B}, \quad \text{if} \quad |S| \ge p^{0.49} \quad \text{then} \quad E(S,S) \le p^{-\gamma}|S|^3 \quad (10)$$

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

We will show in Sections 3.1 and 3.2 the following two properties of the sets $\mathscr{A}$, $\mathscr{B}$.

Lemma 2. *For the set $\mathscr{A}$ defined in Section 2.1,* (9) *holds.*

Lemma 3. *Fix even $m \ge 100$ and let $p \ge p(m)$ be a sufficiently large prime. Let $\mathscr{B} \subset \mathbb{F}_p$ be the set defined in Section 2.1. Then* (10) *holds with $\gamma = \beta/20.59 > 1/(41.4m)$.*

Using Lemmas 2 and 3, we can deduce the required cancellation in the phases of the quantities $\langle \mathbf{u}_{a_1,b_1}, \mathbf{u}_{a_2,b_2} \rangle$.

Lemma 4. *Let m be an even, positive integer, suppose $0 < \alpha \le \frac{1}{100}$, $0 < \gamma \le \min(\alpha, \frac{1}{4m})$, and p is sufficiently large in terms of m, α, γ. Assume $\mathscr{A}$ satisfies $|\mathscr{A}| \le p^{\alpha}$ and for every $\eta > 0$ there is a constant $C(\eta)$ such that for any $\mathscr{A}' \subseteq \mathscr{A}$ and $m' \le m$* (9) *holds. Assume also that $\mathscr{B}$ satisfies* (10). *Then for any disjoint sets $\Omega_1, \Omega_2 \subset \mathscr{A} \times \mathscr{B}$ such that $|\Omega_1| \le \sqrt{p}$, $|\Omega_2| \le \sqrt{p}$, the inequality*

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

holds, where

$$\varepsilon_1 = \frac{\frac{c_0\gamma}{8} - \frac{47\alpha - 23\gamma}{2m}}{1 + 93/m + c_0/2}. \qquad (11)$$

Next, we show how to deduce Theorem 1 from Lemma 4. By Lemma 3, condition (10) holds with $\gamma = 1/(41.4m)$. We take

$$m = 2\left\lceil \frac{8(47(20.7) - 23)}{2c_0} \right\rceil = 2\left\lceil \frac{3799.6}{c_0} \right\rceil.$$

so that, by (11) and Lemma 3,

$$\varepsilon_1 = \frac{\frac{c_0}{m} - \frac{3799.6}{m^2}}{331.2(1 + 93/m + c_0/2)} > \frac{c_0^2}{5059600} \qquad \left(c_0 \le \frac{1}{100}\right).$$

Thus, Φ_p satisfies the conditions of Lemma 1 with $k = \lfloor \sqrt{p} \rfloor$ and $\delta = O(p^{-\varepsilon_1} \log^2 p)$. Let $\varepsilon_0 < \varepsilon_1/2$ and take $s = 2\lfloor p^{\varepsilon_0} \rfloor$. By Lemma 1, Φ_p satisfies RIP with order $\ge p^{1/2+\varepsilon_0}$ and constant $O(p^{-\varepsilon_1/2+\varepsilon_0}(\log p)^3)$. If ε_0 is sufficiently close to $\varepsilon_1/2$, Theorem 1 follows with

$$\varepsilon = 2 - \frac{2}{1+2\varepsilon_0} > 4\varepsilon_0 - 8\varepsilon_0^2 > \frac{c_0^2}{2530000}.$$

The proof of Lemma 4 is quite long, and will be detailed in Section 3.3. We do, however, outline some of the main ideas 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, for example, [18], Proposition 6.31), we have for $a_1 \ne a_2$ the equality

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

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

where $(\frac{d}{p})$ is the Legendre symbol[3], and $\sigma_p = 1$ or i according as $p \equiv 1$ 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 ≥ 3. Consequently, the assertion of Lemma 4 can be rewritten as

$$\left| \sum_{\substack{(a_1,b_1)\in\Omega_1 \\ (a_2,b_2)\in\Omega_2}} \left(\frac{a_1-a_2}{p} \right) e_p\left(\frac{(b_1-b_2)^2}{4(a_1-a_2)} \right) \right| \ll p^{1-\varepsilon_1} (\log p)^2, \qquad (12)$$

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

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

To prove (12) it is enough to show that

$$|S(A_1, A_2)| \ll p^{1-\varepsilon_1}, \qquad (13)$$

where

$$S(A_1, A_2) = \sum_{\substack{a_1\in A_1, \\ a_2\in A_2}} \sum_{\substack{b_1\in\Omega_1(a_1), \\ b_2\in\Omega_2(a_2)}} \left(\frac{a_1-a_2}{p} \right) e_p\left(\frac{(b_1-b_2)^2}{4(a_1-a_2)} \right),$$

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

$$M_i < |\Omega_i(a_i)| \le 2M_i, \qquad |A_i| M_i \le \sqrt{p}. \qquad (14)$$

Indeed, there are $O(\log^2 p)$ choices for M_1, M_2. To prove the cancellation in (13), we basically split into two cases: (i) some $B' = \Omega_i(a_j)$ has additive structure (that is, $E(B', B')$ 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 (9)). Incidentally, oscillations of the factor $(\frac{a_1-a_2}{p})$ play no role in the argument.

3. DETAILS OF SOME PROOFS

3.1 Sums of reciprocals: Proof of Lemma 2

The main idea is to recast the problem as a problem of counting solutions of a corresponding equation in rational numbers.

Lemma 5. *Suppose $m \ge 2$, $\mathscr{N}_1, \dots, \mathscr{N}_m$ are sets of positive integers in the intervals $[1, N_1], \dots, [1, N_m]$, respectively.*

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

For any choice of signs $\sigma_i \in \{-1, 1\}$ and any $\eta > 0$, the number of solutions of

$$\sum_{i=1}^{m} \frac{\sigma_i}{n_i} = 0 \qquad (n_i \in \mathscr{N}_i, 1 \le i \le m)$$

does not exceed $C(m, \eta)(|\mathscr{N}_1| \cdots |\mathscr{N}_m|)^{1/2}(N_1 \cdots N_m)^{\eta}$, for some constant $C(m, \eta)$.

Proof. The proof is based on an idea from Karatsuba [20]. For each solution $(n_1, \dots, n_m)$, mutiplying through by $n_1 \cdots n_m$ shows that

$$n_i \Big| \prod_{j \ne i} n_j \qquad (1 \le i \le m). \tag{15}$$

By induction on P, the largest prime factor of

$$Z := \prod_{i=1}^{m} \prod_{n_i \in \mathscr{N}_i} n_i,$$

(with $P = 1$ if $Z = 1$), we will show that the number of solutions of (15) does not exceed

$$K(P, m, \eta)(|\mathscr{N}_1| \cdots |\mathscr{N}_m|)^{1/2}(N_1 \cdots N_m)^{\eta},$$

where

$$K(P, m, \eta) = \prod_{p \le \min(P, (m+1)^{1/\eta})} \left(\frac{1}{1 - p^{-\eta}} \right)^{m}. \tag{16}$$

The lemma then follows with $C(m, \eta) = \max_P K(P, m, \eta)$. First, if $\mathscr{N}_i = \{1\}$ for all i, then there is exactly 1 solution of (15) and the claim holds when $P = 1$. Now suppose $P \ge 2$ is a prime, and the claim holds if the largest prime factor of Z is at most P', the largest prime smaller than P (set $P' = 1$ if $P = 2$). Suppose $\mathscr{N}_i$ are sets with $Z = P$. For solutions of (15), we observe that

$$P | n_1 \cdots n_m \implies P \text{ divides at least two of the } n_i. \tag{17}$$

Writing $\hat{n}_i = n_i / P^a$ where $P^a \| n_i$ (as usual, $a^j \| n$ means $a^j | n$ and $a^{j+1} \nmid n$),

$$\hat{n}_i \Big| \prod_{j \ne i} \hat{n}_j \quad (1 \le i \le m). \tag{18}$$

For each solution of (15), let $I = \{i : P | n_i\}$. By (17), I is empty or $|I| \ge 2$. For each i, let $\mathscr{N}_i{}' = \{n_i \in \mathscr{N}_i : P | n_i\}$, and for $j \ge 1$ let $\tilde{\mathscr{N}}_{i,j} = \{n_i / P^j : n_i \in \mathscr{N}_i, P^j \| n_i\}$ Set $u_i = |\mathscr{N}_i{}'| / |\mathscr{N}_i|$ for each i. Partition the solutions of (15) according to the set I and the power j_i such that $P^{j_i} \| n_i$. By (18), $\tilde{\mathscr{N}}_{i,j_i} \subseteq [1, N_i / P^{j_i}]$ and the induction assumption, the number of solutions of (15) is

$$\begin{aligned}
&\le \sum_{I} \sum_{j_i \ge 1, i \in I} K(P', m, \eta) \left(\prod_{i \in I} u_i |\mathscr{N}_i| \prod_{i \notin I} (1 - u_i) |\mathscr{N}_i| \right)^{\frac{1}{2}} \\
&\qquad \times (N_1 \cdots N_m)^{\eta} \, P^{-\eta \sum_{i \in I} j_i} \\
&\le K(P', m, \eta) \left(|\mathscr{N}_1| \cdots |\mathscr{N}_m| \right)^{1/2} (N_1 \cdots N_m)^{\eta} \\
&\qquad \times \sum_{I} \left(\prod_{i \in I} u_i \prod_{i \notin I} (1 - u_i) \right)^{\frac{1}{2}} \left(\frac{P^{-\eta}}{1 - P^{-\eta}} \right)^{|I|}.
\end{aligned}$$

If $P < (m+1)^{1/\eta}$, we estimate the sum on I using the binomial theorem. Thus,

$$\begin{aligned}
\sum_{I} \left(\prod_{i \in I} u_i \prod_{i \notin I} (1 - u_i) \right)^{\frac{1}{2}} \left(\frac{P^{-\eta}}{1 - P^{-\eta}} \right)^{|I|} &\le \sum_{I} \left(\frac{P^{-\eta}}{1 - P^{-\eta}} \right)^{|I|} \\
&= \left(\frac{1}{1 - P^{-\eta}} \right)^{m}.
\end{aligned}$$

The claim follows in this case.

If $P \ge (m+1)^{1/\eta}$, we examine two subcases. If I is empty, then

$$\left(\prod_{i=1}^{m} (1 - u_i) \right)^{1/2} \le \left(\prod_{i=1}^{m} (1 - u_i) \right)^{1/m} \le 1 - \frac{u_1 + \cdots + u_m}{m}$$

by the arithmetic mean - geometric mean inequality. Similarly, if $|I| \ge 2$, then

$$\left(\prod_{i \in I} u_i \right)^{1/2} \le \left(\prod_{i \in I} u_i \right)^{1/|I|} \le \frac{1}{|I|} \sum_{i \in I} u_i.$$

Hence, writing $\xi = P^{-\eta} / (1 - P^{-\eta})$,

$$\begin{aligned}
\sum_{|I| \ge 2} \left(\prod_{i \in I} u_i \prod_{i \notin I} (1 - u_i) \right)^{1/2} \xi^{|I|} &\le \sum_{k=2}^{m} \frac{\xi^k}{k} \sum_{|I| = k} \sum_{i \in I} u_i \\
&= (u_1 + \cdots + u_m) \sum_{k=2}^{m} \frac{\xi^k}{k} \binom{m-1}{k-1} \\
&= \frac{u_1 + \cdots + u_m}{m} \sum_{k=2}^{m} \xi^k \binom{m}{k} \\
&= \frac{u_1 + \cdots + u_m}{m} \left((1 + \xi)^m - 1 - m\xi \right).
\end{aligned}$$

By assumption, $\xi \le 1/m$, thus $(1 + \xi)^m - 1 - m\xi < 1$, therefore the number of solutions of (15) is at most

$$K(P', m, \eta)(|\mathscr{N}_1| \cdots |\mathscr{N}_m|)^{1/2}(N_1 \cdots N_m)^{\eta},$$

as claimed. □

Proof of Lemma 2. Multiplying both sides of the congruence (9) by $\prod_{i=1}^{2m'} (a - a_i)$ yields

$$\sum_{i=1}^{2m'} \prod_{\substack{1 \le j \le 2m' \\ j \ne i}} \sigma_i (a - a_j) \equiv 0 \pmod{p},$$

with $\sigma_i = 1$ if $i \le m'$ and $\sigma_i = -1$ if $i > m'$. The absolute value of the left side of the congruence is at most $2m' p^{(2m'-1)\alpha} < p$ by assumption, hence the left side is zero (not just zero mod p). In other words,

$$\sum_{i=1}^{m'} \frac{1}{a - a_i} = \sum_{i=m'+1}^{2m'} \frac{1}{a - a_i}.$$

Write $\mathscr{A}' = \mathscr{A}'_+ \cup \mathscr{A}'_-$, where $\mathscr{A}'_+ = \{a' \in \mathscr{A}' : a' > a\}$, $\mathscr{A}'_- = \{a' \in \mathscr{A}' : a' < a\}$. Applying Lemma 5 with $m = 2m'$ and $\mathscr{N}_i \in \{\mathscr{A}'_+, \mathscr{A}'_-\}$, we see that the number of solutions of the above equation is, for any $\eta > 0$, at most

$$2^{2m'} C(2m', \eta/2m') |\mathscr{A}'|^{m'} p^{\eta}.$$

Taking $C(\eta) = \max_{m' \le m} 2^{2m'} C(2m', \eta/2m')$ completes the proof. □

3.2 Some definitions and results from additive combinatorics

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

$$A \pm B = \{a \pm b : \, a \in A, b \in B\}.$$

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 $\mathscr{B} \subset G$ be the set defined in Section 2.1. There is a natural bijection Ψ between $\mathscr{B}$ and the cube $\mathscr{C}_{M,r} = \{0, \dots, M-1\}^r$ defined by

$$\Psi\left(\sum_{j=1}^{r} x_j (2M)^{j-1}\right) = (x_1, \dots, x_r).$$

Moreover, it is trivial that $b_1 + b_2 = b_3 + b_4$ if and only if $\Psi(b_1) + \Psi(b_2) = \Psi(b_3) + \Psi(b_4)$. In the language of additive combinatorics, Ψ is a Freiman isomorphism between $\mathscr{B}$ and $\mathscr{C}_{M,r}$. Thus, $|B_1 + B_2| = |\Psi(B_1) + \Psi(B_2)|$ for any $B_1 \subseteq \mathscr{B}$, $B_2 \subseteq \mathscr{B}$. The problem of the size of sumsets in $\mathscr{C}_{M,r}$ will be investigated below.

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

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

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

Lemma 6. *If $E(A, A) \ge |A|^3/K$ then there exists a set $A' \subset A$ such that $|A'| \ge |A|/(20K)$ and $|A' - A'| \le 10^7 K^9 |A|$.*

Proof. By Lemma [31, Lemma 2.30], there exists $F \subset A \times A$ such that $|F| \ge |A|^2/(2K)$ and $|\{a + a' : (a, a') \in F\}| \le 2K|A|$. Consequently, a set A' exists with the required properties by a version of the Balog–Szemerédi–Gowers lemma [7, Lemma 2.2]. □

For a function $f : \mathbb{F}_p \to \mathbb{C}$ and a number $r \ge 1$ we define the ℓ_r norm of f:

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

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

$$E(A, B) = E(A, -B) = \|1_A * 1_B\|_2^2. \tag{19}$$

We say that a function $f : \mathbb{F}_p \to [0, \infty)$ 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 1 ([5, Theorem C]). *Assume $A \subset \mathbb{F}_p$ and $B \subset \mathbb{F}_p^*$, where $|A| \ge |B|$. For some $c_0 > 0$,*

$$\sum_{b \in B} E(A, bA) \ll (\min(p/|A|, |B|)^{-c_0} |A|^3 |B|. \tag{20}$$

Remark 2. *An explicit version of Proposition 1, with $c_0 = 1/10430$, is given in [8].*

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

Corollary 1 ([6, Corollary 2]). *For any $A \subset \mathbb{F}_p$ and a probability measure λ we have*

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

We deduce Lemma 3 from a general result about sumsets of product sets.

Theorem 2 ([6, Theorem 5]). *Let r and M be positive integers, $M \ge 2$ and $\mathscr{C} = \mathscr{C}_{M,r} = \{0, \dots, M-1\}^r$. Let $\tau = \tau_M$ be the solution of the equation*

$$\left(\frac{1}{M}\right)^{2\tau} + \left(\frac{M-1}{M}\right)^{\tau} = 1. \tag{21}$$

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

$$|A + B| \ge (|A||B|)^{\tau}. \tag{22}$$

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

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

By Theorem 2, $\tau \le \tau'$. On the other hand,

$$\tau_M \ge \frac{1}{2} + \frac{\log 2}{2 \log M}\left(1 - \frac{1}{\log M}\right). \tag{23}$$

To show (23), it suffices to show that when τ equals the right side of (23), the left side of (21) is ≥ 1; that is, we must show

$$\frac{2^{1/\log M}}{2M} + \left(1 - \frac{1}{M}\right)^{1/2} 2^{\frac{1}{2 \log M}(1 - 1/\log M) \log(1 - 1/M)} \ge 1.$$

This follows for small M by direct calculation. For $M \ge 32$, the second power of 2 is

$$\ge 2^{-1/(2M \log M)} \ge 1 - \frac{\log 2}{2M \log M},$$

$(1 - 1/M)^{1/2} \ge 1 - \frac{1}{2M} - \frac{1}{4M^2}$ and $2^{1/\log M} \ge 1 + \frac{\log 2}{\log M} + \frac{(\log 2)^2}{2 \log^2 M}$. So, the asymptotic behavior of $2\tau_M - 1$ as $M \to \infty$ is sharp. Likely, inequality (22) holds with $\tau = \tau'_M$. This was proved in the case $M = 2$ by Woodall [32]. Results of a similar spirit, concerning addition of subsets of ${\mathbb{F}_p}^r$ and related groups, are considered in [4].

Corollary 2. *Let m be a positive integer. For the set $\mathscr{B} \subset \mathbb{F}_p$ defined in (7) and for any subset $B \subset \mathscr{B}$, we have $|B - B| \ge |B|^{2\tau_M}$.*

Proof. The set $-B$ is a translate of some set $B' \subset \mathscr{B}$, and $\mathscr{B}$ is Freiman isomorphic to $\mathscr{C}_{M,r}$. Hence, for any $B \subset \mathscr{B}$ we have $|B - B| = |B + B'| \ge |B|^{2\tau_M}$. □

Proof of Lemma 3. Let $E(S, S) = |S|^3/K$. By Lemma 6, there is a set $B \subset S$ such that $|B| \ge |S|/(20K)$ and $|B - B| \le 10^7 K^9 |S|$. By Corollary 2, $|B - B| \ge |B|^{2\tau_M} \ge (|S|/20K)^{2\tau_M}$, hence

$$p^{0.49(2\tau_M - 1)} \le |S|^{2\tau_M - 1} \le 10^7 K^9 (20K)^{2\tau_M}.$$

Therefore,

$$K \gg p^{\gamma}, \quad \gamma = \frac{0.49(2\tau_M - 1)}{9 + 2\tau_M}.$$

Since $M = \lfloor 2^{2.01m-1} \rfloor \geq 2^{200} - 1$, inequality (23) gives $\gamma \geq \beta/20.59$. □

3.3 The proof of Lemma 4

We may assume $\varepsilon_1 > 0$, otherwise there is nothing to prove. Adopt the notation $(A_i, M_i, \Omega_i(a))$ from Section 2.2. If $|A_i|M_i < p^{1/2-\varepsilon_1}$, then by (14), $|S(A_1, A_2)| \leq p^{1-\varepsilon_1}$ and (13) holds. Thus, we can assume that $|A_i|M_i \geq p^{1/2-\varepsilon_1}$, which implies, by $|\mathscr{A}| \leq p^{\alpha}$, that

$$M_1 \geq p^{1/2-\alpha-\varepsilon_1}, \quad M_2 \geq p^{1/2-\alpha-\varepsilon_1}. \tag{24}$$

Lemma 7 ([6, Lemma 9]). *For any $\theta \in \mathbb{F}_p^*$, $B_1 \subset \mathbb{F}_p$, $B_2 \subset \mathbb{F}_p$ we have*

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

By (14) and (24), $|\Omega_i(a_i)| \geq p^{0.49}$, and by Lemma 7 and (10),

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

Also, by (14), we have

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

Thus, if $|A_1| < p^{\gamma - 4\varepsilon_1}$ and $|A_2| < p^{\gamma - 4\varepsilon_1}$, then $|S(A_1, A_2)| \leq p^{1-\varepsilon_1}$ and (13) follows. Otherwise, without loss of generality we may assume that

$$|A_2| \geq p^{\gamma - 4\varepsilon_1}. \tag{25}$$

The following lemma gives the necessary estimates to complete the proof of Lemma 4. For $a_1 \in A_1$, define

$$\begin{aligned} T(A, B) &= T_{a_1}(A, B) \\ &= \sum_{\substack{b_1 \in B \\ a_2 \in A, b_2 \in \Omega_2(a_2)}} \left(\frac{a_1 - a_2}{p}\right) e_p\left(\frac{(b_1 - b_2)^2}{4(a_1 - a_2)}\right) \end{aligned}$$

Lemma 8. *If $a_1 \in A_1$, $0 < \alpha \leq \frac{1}{100}$, $0 < \gamma \leq \min(\alpha, \frac{1}{4m})$, conditions (14) and (25) are satisfied and a set $B \subset \mathbb{F}_p$ is such that*

$$\frac{1}{20} p^{1/2 - (11\alpha - 4\gamma + 35\varepsilon_1)/3} \leq |B| \leq p^{1/2} \tag{26}$$

and

$$|B - B| \leq 2 \cdot 10^8 p^{20\alpha - 10\gamma + 80\varepsilon_1} |B|, \tag{27}$$

then, for large p we have

$$|T(A_2, B)| \leq |B| p^{(1/2) - \varepsilon_1}. \tag{28}$$

Remark 4. *The proof of Lemma 8 is nearly identical to the proof of Lemma 10 in [6], and applies to more general sums, e.g. 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 ≤ 1, and one may replace $\frac{1}{a_1 - a_2}$ with different quantities $g(a_1, a_2)$ having the dissociative property (the analog of (9) holds).*

Postponing the proof of Lemma 8, we show first how to deduce Lemma 4.

We take a maximal subset $B_0 \subset \Omega_1(a_1)$ so that (28) holds for $B = B_0$. Denote $B_1 = \Omega_1(a_1) \setminus B_0$. By Lemma 7, (10) and (14),

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

Consider the case when

$$E(B_1, B_1) \leq M_1^3 / K, \qquad K = p^{2\alpha - \gamma + 8\varepsilon_1}. \tag{29}$$

Then we have, due to (14),

$$|T_{a_1}(A_2, B_1)| \leq M_1^{7/8} p^{(9/16) - \varepsilon_1 - \alpha/8}. \tag{30}$$

Now assume that (29) does not hold. By (14), we get

$$|B_1| > K^{-1/3} M_1, \quad E(B_1, B_1) \geq |B_1|^3 / K.$$

Applying Lemma 6 and (14), we obtain the existence of a set $B_1' \subset B_1$ such that

$$|B_1'| \geq \frac{|B_1|}{20K} \geq \frac{M_1}{20K^{4/3}} \geq \frac{1}{20} p^{1/2 - (11\alpha - 4\gamma + 35\varepsilon_1)/3}$$

and $|B_1' - B_1'| \leq 10^7 K^9 |B_1| \leq 2 \cdot 10^8 K^{10} |B_1'|$. Using Lemma 8 we get inequality (28) for $B = B_1'$. Therefore, (28) is also satisfied for $B = B_0 \cup B_1'$, contradicting the choice of B_0.

Thus, we have shown that (29) must hold. Using (28) for $B = B_0$ and (30) we get

$$|T_{a_1}(A_2, \Omega_1(a_1))| \leq M_1 p^{(1/2) - \varepsilon_1} + 2M_1^{7/8} p^{(9/16) - \varepsilon_1 - \alpha/8}.$$

Summing on $a_1 \in A_1$ and using (14), we obtain

$$\begin{aligned} |S(A_1, A_2)| &\leq |A_1| \left(M_1 p^{(1/2) - \varepsilon_1} + M_1^{7/8} p^{(9/16) - \varepsilon_1 - \alpha/8} \right) \\ &\leq p^{1 - \varepsilon_1} + |A_1|^{1/8} p^{1 - \varepsilon_1 - \alpha/8} \leq 2p^{1 - \varepsilon_1}, \end{aligned}$$

completing the proof of Lemma 4.

Proof of Lemma 8. By the Cauchy-Schwarz inequality we have

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

where

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

Consequently, by Hölder's inequality,

$$|T(A_2, B)|^2 \leq \sqrt{p} |B|^{2 - 2/m} \left(\sum_{b_1, b \in B} |F(b, b_1)|^m \right)^{\frac{1}{m}}. \tag{31}$$

Next,

$$\sum_{\substack{b_1\in B\\ b\in B}}|F(b,b_1)|^m \le \sum_{\substack{x\in B+B,\\ y\in B-B}}\left|\sum_{\substack{a_2\in A_2,\\ b_2\in\Omega_2(a_2)}} e_p\left(\frac{2xy-b_2y}{2(a_1-a_2)}\right)\right|^m$$
$$\le \sum_{y\in B-B}\sum_{\substack{a_2^{(i)}\in A_2\\ b_2^{(i)}\in\Omega_2(a_2^{(i)})\\ 1\le i\le m}}\left|\sum_{x\in B+B} e_p\left(\frac{xy}{4}\sum_{i=1}^m\frac{\sigma_i}{a_1-a_2^{(i)}}\right)\right|,$$

where $\sigma_i=1$ for $i\le\frac{m}{2}$ and $\sigma_i=-1$ for $\frac{m}{2}<i\le m$. Hence, for some complex numbers $\varepsilon_{y,\xi}$ of modulus ≤ 1,

$$\sum_{b_1,b\in B}|F(b,b_1)|^m \le M_2^m\sum_{y\in B-B}\sum_{\xi\in\mathbb{F}_p}\lambda(\xi)\varepsilon_{y,\xi}\sum_{x\in B+B}e_p\left(\frac{xy\xi}{4}\right), \tag{32}$$

where $\lambda(\xi)$ is the number of solutions of the congruence

$$\sum_{i=1}^{m/2}\left(\frac{1}{a_1-a^{(i)}}-\frac{1}{a_1-a^{(i+m/2)}}\right)\equiv\xi \pmod p$$

with $a^{(1)},\dots,a^{(m)}\in A_2$.

By (9), for small η, which we shall choose later,

$$\lambda(0)\le C(\eta)|A_2|^{m/2}p^{\eta}. \tag{33}$$

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,

$$\left|\sum_{y\in B-B}\sum_{\xi\in\mathbb{F}_p^*}\lambda(\xi)\varepsilon_{y,\xi}\sum_{x\in B+B}e_p\left(\frac{xy\xi}{4}\right)\right| = \left|\sum_{\substack{x\in B+B\\ z\in\mathbb{F}_p}}\zeta'(z)e_p\left(\frac{xz}{4}\right)\right|$$
$$\le |B+B|^{\frac34}\left(\sum_{x\in\mathbb{F}_p}\left|\sum_{z\in\mathbb{F}_p}\zeta'(z)e_p\left(\frac{xz}{4}\right)\right|^4\right)^{\frac14}$$
$$= |B+B|^{\frac34}\left(\sum_{x\in\mathbb{F}_p}\left|\sum_{z'\in\mathbb{F}_p}(\zeta'*\zeta')(z')e_p\left(\frac{xz'}{4}\right)\right|^2\right)^{\frac14}$$
$$= |B+B|^{\frac34}\|\zeta'*\zeta'\|_2^{1/2}p^{\frac14}$$
$$\le |B+B|^{\frac34}\|\zeta*\zeta\|_2^{1/2}p^{\frac14}. \tag{34}$$

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

$$\|\zeta*\zeta\|_2\le\sum_{\xi,\xi'\in\mathbb{F}_p^*}\lambda(\xi)\lambda(\xi')\|1_{\xi(B-B)}*1_{\xi'(B-B)}\|_2$$
$$=\sum_{\xi,\xi'\in\mathbb{F}_p^*}\lambda(\xi)\lambda(\xi')\|1_{B-B}*1_{(\xi'/\xi)(B-B)}\|_2. \tag{35}$$

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 congruence

$$\sum_{i=1}^{m}\left(\frac{1}{a_1-a^{(i)}}-\frac{1}{a_1-a^{(m+i)}}\right)\equiv 0 \pmod p$$

with $a^{(1)},\dots,a^{(2m)}\in A_2$. By (9),

$$\sum_{\xi\in\mathbb{F}_p}\lambda(\xi)^2\le C(\eta)|A_2|^m p^{\eta}. \tag{36}$$

Now we are in position to apply Corollary 1, which gives for any $\xi'\in\mathbb{F}_p^*$

$$\sum_{\xi\in\mathbb{F}_p^*}\lambda_1(\xi)\|1_{B-B}*1_{(\xi'/\xi)(B-B)}\|_2\ll|B-B|^{\frac32}$$
$$\times\left(\|\lambda_1\|_2+|B-B|^{-\frac12}+|B-B|^{\frac12}p^{-\frac12}\right)^{c_0}. \tag{37}$$

By (25) and (36),

$$\|\lambda_1\|_2\le C(\eta)^{1/2}|A_2|^{-m/2}p^{\eta/2}\ll p^{(\eta/2)-(m/2)(\gamma-4\varepsilon_1)}.$$

By (26) and $\alpha\le\frac{1}{100}$,

$$|B-B|\ge|B|\ge(1/20)p^{1/2-(11\alpha-4\gamma+35\varepsilon_1)/3}\ge p^{1/3}.$$

On the other hand, it follows from (26) and (27) that

$$|B-B|\ll p^{1/2+20\alpha-10\gamma+80\varepsilon_1}\le p^{3/4}.$$

Since $m\gamma\le 1/4$ we get

$$\|\lambda_1\|_2+|B-B|^{-1/2}+|B-B|^{1/2}p^{-1/2}\ll p^{(\eta/2)-(m/2)(\gamma-4\varepsilon_1)}.$$

So, by (35) and (37),

$$\|\zeta*\zeta\|_2\le|A_2|^{2m}\sum_{\xi'\in\mathbb{F}_p^*}\lambda_1(\xi')\sum_{\xi\in\mathbb{F}_p^*}\lambda_1(\xi)\|1_{B-B}*1_{(\xi'/\xi)(B-B)}\|_2$$
$$\ll|A_2|^{2m}p^{-(c_0/2)(m\gamma-4m\varepsilon_1-\eta)}|B-B|^{3/2}.$$

Subsequent application of (32), (33) and (34) gives

$$\sum_{b_1,b\in B}|F(b,b_1)|^m\ll p^{\eta}(M_2|A_2|)^m|A_2|^{-\frac{m}{2}}|B-B||B+B|$$
$$+p^{\eta c_0/2}M_2^m|A_2|^m|B-B|^{\frac34}|B+B|^{\frac34}p^{-(c_0/4)m(\gamma-4\varepsilon_1)}p^{\frac14}.$$

By a particular case of Plünecke – Ruzsa estimates ([31], Exercise 6.5.15), $|B+B|\le|B-B|^2/|B|$. Together with condition (27), this gives $|B+B|\le p^{40\alpha-20\gamma+160\varepsilon_1}|B|$. By (26), $p^{1/4}\le|B|^{1/2}p^{(11\alpha-4\gamma+35\varepsilon_1)/6}$. Recalling $\gamma\le\alpha$, (14), (25) and (27), we conclude that for small enough η,

$$\sum_{b_1,b\in B}|F(b,b_1)|^m\ll|B|^2p^{\eta+\frac{m}{2}}\Big(p^{-\frac{m}{2}(\gamma-4\varepsilon_1)+60\alpha-30\gamma+240\varepsilon_1}$$
$$+p^{\frac{281}{6}\alpha-\frac{139}{6}\gamma+\frac{1115}{6}\varepsilon_1-c_0\frac{m}{4}(\gamma-4\varepsilon_1)}\Big)$$
$$\ll|B|^2p^{\frac{m}{2}+\frac{281}{6}\alpha-23\gamma+186\varepsilon_1-c_0\frac{m}{4}(\gamma-4\varepsilon_1)}.$$

Plugging the last estimate into (31), we get

$$|T(A_2,B)|^2\ll|B|^2p^{1+\frac{1}{m}(\frac{281}{6}\alpha-23\gamma+186\varepsilon_1)-(c_0/4)(\gamma-4\varepsilon_1)}.$$

By (11), for large p we have $|T(A_2,B)|\le|B|p^{1/2-\varepsilon_1}$, as claimed. □

4. 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 first author was partially supported by NSF Grants DMS-0808042 and DMS-0835373, the second author was supported by NSF Grant DMS-0701552 and the third author was supported by NSF grant DMS-0901339. The second, third and fifth authors were supported by the Workshop in Analysis and Probability at Texas A& M University, 2008. The research was finished while the third and fourth authors were visiting the Institute for Advanced Study, the third author supported by grants from the Ellentuck Fund and The Friends of the Institute For Advanced Study. The last three authors thank the IAS for its hospitality and excellent working conditions.

5. REFERENCES

[1] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures and Algorithms*, 3(3):289–303, 1992.

[2] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin. A simple proof of the restricted isometry property for random matrices. *Constr. Approx.*, 28(3):253–263, 2008.

[3] R. Berinde, A. Gilbert, P. Indyk, H. Karloff, and M. Strauss. Combining geometry and combinatorics: a unified approach to sparse signal recovery. In *Proc. 46th Annual Allerton Conference on Communication, Control and Computing*, pages 798–805, 2008.

[4] B. Bollobas and I. Leader. Sums in the grid. *Discrete Math.*, 162:31–48, 1996.

[5] J. Bourgain. Multilinear exponential sums in prime fields under optimal entropy condition on the sources. *Geom. Funct. Anal.*, 18(5):1477–1502, 2009.

[6] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova. Explicit constructions of RIP matrices and related problems. *Duke Math. J.*, 2011. to appear. arXiv: `1008.4535`.

[7] J. Bourgain and M. Z. Garaev. On a variant of sum-product estimates and explicit exponential sum bounds in finite fields. *Math. Proc. Cambridge Philos. Soc.*, 146(1):1–21, 2009.

[8] J. Bourgain and A. A. Glibichuk. Exponential sum estimate over subgroup in an arbitrary finite field. *preprint*, 2010.

[9] E. J. Candès. The restricted isometry property and its implications for compresses sensing. *C. R. Math. Acad. Sci. Paris*, 346:589–592, 2008.

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

[11] E. J. Candès and T. Tao. Decoding by linear programming. *IEEE Trans. Inform. Theory*, 51:4203–4215, 2005.

[12] E. J. Candès and T. Tao. Near-optimal signal recovery from random projections: universal encoding strategies. *IEEE Trans. Inform. Theory*, 52(2):489–509, 2006.

[13] R. DeVore. Deterministic constructions of compressed sensing matrices. *J. Complexity*, 23:918–925, 2007.

[14] D. Donoho, M. Elad, and V. N. Temlyakov. On the lebesgue type inequalities for greedy approximation. *J. Approximation Theory*, 147:185–195, 2007.

[15] A. C. Gilbert, S. Mutukrishnan, and M. J. Strauss. Approximation of functions over redundant dictionaries using coherence. In *Proc. 14th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 243–252, 2003.

[16] E. D. Gluskin. An octahedron is poorly approximated by random subspaces. *Funktsional. Anal. i Prilozhen.*, 20(1):14–20, 96, 1986.

[17] S. Gurevich and R. Hadani. The statistical restricted isometry property and the Wigner semicircle distribution of incoherent dictionaries. preprint, arXiv:0812.2602.

[18] K. Ireland and M. Rossen. *A classical introduction to modern number theory.* Springer - Verlag, 1982.

[19] W. B. Johnson and J. Lindenstrauss. Extensions of Lipschitz mappings into a Hilbert space. In *Conference in Modern Analysis and Probability*, pages 189–206, 1984.

[20] A. A. Karatsuba. Double Kloosterman sums. *Mat. Zametki*, 66(5):682–687, 1999. Russian. English translation in Math. Notes **66** (1999), no. 5-6, 565–569.

[21] B. S. Kashin. On widths of octahedron. *Uspekhi Matem. Nauk*, 30:251–252, 1975. Russian.

[22] B. S. Kashin. Widths of certain finite-dimensional sets and classes of smooth functions. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 41:334–351, 1977. Russian. English transl. in Math. USSR Izv. **11** (1978), 317–333.

[23] V. I. Levenshtein. Bounds for packings of metric spaces and some of their applications. *Problemy Kibernet*, (40):43–110, 1983. Russian.

[24] E. Liu and V. N. Temlyakov. Orthogonal super greedy algorithm and applications in compressed sensing. preprint, 2010.

[25] E. Livshitz. On efficiency of Orthogonal Matching Pursuit. preprint, 2010, ArXiv: 1004.3946.

[26] S. Mendelson, A. Pajor, and N. Tomczak-Jaegermann. Reconstruction and subgaussian operators in asymptotic geometric analysis. *Geom. Funct. Anal.*, 17:1248–1282, 2007.

[27] D. Needle and R. Vershynin. Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit. *Found. Comput. Math.*, 9(3):317–334, 2009.

[28] J. Nelson and V. N. Temlyakov. On the size of incoherent systems. preprint, 2010.

[29] M. Rudelson and R. Vershynin. On sparse reconstruction from Fourier and Gaussian measurements. *Comm. Pure Appl. Math.*, 61(8):1025–1045, 2008.

[30] T. Tao. Open question: deterministic uup matrices. `http://terrytao.wordpress.com` (2007, July 02).

[31] T. Tao and V. Vu. *Additive Combinatorics.* Cambridge University Press, 2006.

[32] D. R. Woodall. A theorem on cubes. *Mathematika*, 24:60–62, 1977.