EXPLICIT RIP MATRICES: AN UPDATE
KEVIN FORD, DENKA KUTZAROV A, AND GEORGE SHAKAN

ABSTRACT. Leveraging recent advances in additive combinatorics, we exhibit explicit matrices satisfying the Restricted Isometry Property with better parameters. Namely, for $\varepsilon = 3.26 \cdot 10^{-7}$, large $k$ and $k^{2-\varepsilon} \leq N \leq k^{2+\varepsilon}$, we construct $n \times N$ RIP matrices of order $k$ with $k = \Omega(n^{1/2+\varepsilon/4})$.

1. INTRODUCTION

Suppose $1 \leq k \leq n \leq N$ and $0 < \delta < 1$. A ‘signal’ $x = (x_j)_{j=1}^N$ is said to be $k$-sparse if $x$ has at most $k$ nonzero coordinates. An $n \times N$ matrix $\Phi$ is said to satisfy the Restricted Isometry Property (RIP) of order $k$ with constant $\delta$ if for all $k$-sparse vectors $x$ we have

$$ (1 - \delta)\|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta)\|x\|_2^2. $$

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

We know from Candès, Romberg and Tao that matrices satisfying RIP have application to sparse signal recovery (see [7, 8, 9]). Given $n, N, \delta$, we wish to find $n \times N$ RIP matrices of order $k$ with constant $\delta$, and with $k$ as large as possible. If the entries of $\Phi$ are independent Bernoulli random variables with values $\pm 1/\sqrt{n}$, then with high probability, $\Phi$ will have the required properties for $k$ of order close to $\delta n$; in different language, this was first proved by Kashin [13].

It is an open problem to find good explicit constructions of RIP matrices; see Tao’s Weblog [17] for a discussion of the problem. All existent explicit constructions of RIP matrices are based on number theory. Prior to the work of Bourgain, Dilworth, Ford, Konyagin and Kutzarova [3], there were many constructions, e.g. Kashin [12], DeVore [10] and Nelson and Temlyakov [15], producing matrices with $\delta$ small and order

$$ k \approx \delta \sqrt{n \log n \log N}. $$

The $\sqrt{n}$ barrier was broken by the aforementioned authors in [3]:

**Theorem A.** [3]. There are effective constants $\varepsilon > 0$, $\varepsilon' > 0$ and explicit numbers $k_0, c > 0$ such that for any positive integers $k \geq k_0$ and $k^{2-\varepsilon} \leq N \leq k^{2+\varepsilon}$, there is an explicit $n \times N$ RIP matrix of order $k$ with $k \geq cn^{1/2+\varepsilon/4}$ and constant $\delta = k^{-\varepsilon'}$.

As reported in [4], the construction in [3] produces a value $\varepsilon \approx 2 \cdot 10^{-22}$. An improved construction was presented in [4], giving Theorem A with $\varepsilon = 3.6 \cdot 10^{-15}$. The values of $\varepsilon$ depend on two constants in additive combinatorics, which have since been improved. Incorporating these improvements into the argument in [4], we will deduce the following.
Theorem 1. Let \( \varepsilon = 3.26 \cdot 10^{-7} \). There is \( \varepsilon' > 0 \) and effective numbers \( k_0, c > 0 \) such that for any positive integers \( k \geq k_0 \) and \( k^{2-\varepsilon} \leq N \leq k^{2+\varepsilon} \), there is an explicit \( n \times N \) RIP matrix of order \( k \) with \( k \geq c n^{1/2+\varepsilon/4} \) and constant \( \delta = k^{-\varepsilon'} \).

As of this writing, the constructions in [3] and [4] remain the only explicit constructions of RIP matrices which exceed the \( \sqrt{n} \) barrier for \( k \).

The proof of Theorem 1 depends on two key results in additive combinatorics. For subsets \( A, B \) of an additive finite group \( G \), we write

\[
A + B = \{ a + b : a \in A, b \in B \},
\]

\[
E(A, B) = \# \{(a_1, a_2, b_1, b_2) : a_1 + b_1 = a_2 + b_2; a_1, a_2 \in A; b_1, b_2 \in B \}.
\]

Also set \( x \cdot B = \{ xb : b \in B \} \). Here we will mainly work with the group of residues modulo a prime \( p \).

Proposition 1. For some \( c_0 \), the following holds. Assume \( A, B \) are subsets of residue classes modulo \( p \), with \( 0 \notin B \) and \( |A| \geq |B| \). Then

\[
\sum_{b \in B} E(A, b \cdot A) = O \left( (\min(p/|A|, |B|))^{-c_0} |A|^3 |B| \right).
\]

This theorem, without an explicit \( c_0 \), was proved by Bourgain [2]. The first explicit version of Proposition 1 with \( c_0 = 1/10430 \), is given in Bourgain and Glibuchuk [6], and this is the value used in the papers [3, 4]. Murphy and Petridis [14] Lemma 13] made a great improvement, showing that Proposition 1 holds with \( c_0 = 1/3 \). It is conceivable that \( c_0 \) may be taken to be any number less than 1. Taking \( A = B \) we see that \( c_0 \) cannot be taken larger than 1.

We also need a version of the Balog–Szemerédi–Gowers lemma, originally proved by Balog and Szemerédi [11] and later improved by Gowers [11]. The version we use is a later improvement due to Schoen [16].

Proposition 2. For some positive \( c_1, c_2, c_3 \) and \( c_4 \), the following holds. If \( E(A, A) = |A|^3/K \), then there exists \( A', B' \subseteq A \) with \( |A'|, |B'| \geq c_2 |A|^{1/2} \) and \( |A' - B'| \leq c_3 K c_1 |A'|^{1/2} |B'|^{1/2} \).

The constants \( c_2, c_3 \) are relatively unimportant. The best result to date is due to Schoen [16], who showed that any \( c_1 > 7/2 \) and \( c_4 > 3/4 \) is admissible. It is conjectured that \( c_1 = 1 \) is admissible. The papers [3, 4] used Proposition 2 with the weaker values \( c_1 = 9 \) and \( c_4 = 1 \), this deducible from Bourgain and Garaev [5, Lemma 2.2].

2. Construction of the matrix

Our construction is identical to that in [4]. We fix an even integer \( m \geq 100 \) and let \( p \) be a large prime. For \( x \in \mathbb{Z} \), let \( e_p(x) = e^{2\pi i x/p} \). Let

\[
u_{a, b} = \frac{1}{\sqrt{p}} (e_p(ax^2 + bx))_{1 \leq x \leq p}.
\]

We take

\[
\alpha = \frac{1}{2m}, \quad \mathcal{A} = \{1, 2, \ldots, [p^\alpha] \}.
\]

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

\[
\beta = \frac{1}{2.01m}, \quad r = \left\lfloor \frac{\beta \log p}{\log 2} \right\rfloor, \quad M = [2^{2.01m-1}],
\]
Lemma 3.1. Assume that \( \delta \)

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

We interpret \( \mathcal{A}, B \) as sets of residue classes modulo \( p \). We notice that all elements of \( B \) are at most \( p/2 \), and \( |\mathcal{A}|/|B| \) lies between two constant multiples of \( p^{1+\alpha-\beta} = p^{1/402m} \).

Given large \( k \) and \( k^{2-\epsilon} \leq N \leq k^{2+\epsilon} \), let \( p \) be a prime in the interval \([k^{2-\epsilon}, 2k^{2-\epsilon}]\) (such \( p \) exists by Bertrand’s postulate). Let \( \Phi_p \) be a \( p \times (|\mathcal{A}| \cdot |B|) \) matrix formed by the column vectors \( u_{a,b} \) for \( a \in \mathcal{A}, b \in B \) (the columns may appear in any order). We also have

\[
\text{if } \epsilon \leq \frac{1}{403m} \text{, then } N \leq p^{2-\epsilon} \leq |\mathcal{A}|/|B|.
\]

Take \( \Phi \) to be the matrix formed by the first \( N \) columns of \( \Phi_p \). Let \( n = p \). Our task is to show that \( \Phi \) satisfies the RIP condition with \( \delta = p^{-\epsilon'} \) for some constant \( \epsilon' > 0 \), and of order \( k \).

3. Main Tools

**Lemma 3.1.** Assume that \( c_0 \leq 1 \) and that Proposition [4] holds. Fix an even integer \( m \geq 100 \), and define \( \alpha, \mathcal{A}, B \) by (2.3) and (2.4). Suppose that \( p \) is sufficiently large in terms of \( m \). Assume also that for some constant \( c_5 > 0 \) and constant \( 0 < \gamma \leq \frac{1}{4m} \), \( B \) satisfies

\[
\forall S \subseteq B \text{ with } |S| \geq p^{0.49}, E(S, S) \leq c_5 p^{-\gamma} |S|^{3/2}.
\]

Define the vectors \( u_{a,b} \) by (2.1). Then for any disjoint sets \( \Omega_1, \Omega_2 \subset \mathcal{A} \times B \) such that \( |\Omega_1| \leq \sqrt{p} \), \( |\Omega_2| \leq \sqrt{p} \), the inequality

\[
\left| \sum_{(a_1,b_1) \in \Omega_1} \sum_{(a_2,b_2) \in \Omega_2} \langle u_{a_1,b_1}, u_{a_2,b_2} \rangle \right| = O \left( p^{1/2-\epsilon_1} (\log p)^2 \right)
\]

holds, where

\[
\epsilon_1 = \frac{c_0 \gamma}{8} - \frac{47\gamma - 23\gamma}{2m}.
\]

The constant implied by the \( O \)-symbol depends only on \( c_0, \gamma \) and \( m \).

Lemma 3.1 follows by combining Lemmas 2 and 4 from [4]; the assumption of Proposition [4] is inadvertently omitted in the statement of [4] Lemma 4.

Using Lemma 3.1, we shall show the following.

**Theorem 2.** Assume the hypotheses of Lemma 3.1 let \( \epsilon = 2\epsilon_1 - 2\epsilon_2^2 \) and assume that \( \epsilon \leq \frac{1}{403m} \). There is \( \epsilon' > 0 \) such that for sufficiently large \( k \) and \( k^{2-\epsilon} \leq N \leq k^{2+\epsilon} \), there is an explicit \( n \times N \) RIP matrix of order \( k \) with \( n = O(k^{2-\epsilon}) \) and constant \( \delta = k^{-\epsilon'} \).

To prove Theorem 2 we first recall another additive combinatorics result from [4].

**Lemma 3.2 (4 Theorem 2, Corollary 2).** Let \( M \) be a positive integer. For the set \( B \subset \mathbb{F}_p \) defined in (2.3) and for any subsets \( A, B \subset B \), we have \( |A - B| \geq |A|^\tau |B|^\tau \), where \( \tau \) is the unique positive solution of

\[
\left( \frac{1}{M} \right)^{2\tau} + \left( \frac{M-1}{M} \right)^{\tau} = 1.
\]
From [4] we have the easy bounds
\[
\frac{\log 2}{\log M} \left(1 - \frac{1}{\log M}\right) \leq 2\tau - 1 \leq \frac{\log 2}{\log M}.
\]

**Corollary 1.** Take $\mathcal{B}$ as in (2.3) and assume Proposition [2]. Then (3.1) holds with
\[
\gamma = \frac{0.49(2\tau - 1)}{c_1 + c_4(2\tau - 1)}.
\]

**Proof.** Just like the proof of [4, Lemma 3], except that we incorporate Proposition [2]. Suppose that $S \subseteq \mathcal{B}$ with $|S| \geq p^{0.49}$ and $E(S, S) = |S|^3/K$. By Proposition [2] there are sets $T_1, T_2 \subseteq S$ such that $|T_1|, |T_2| \geq c_2 \frac{|S|}{K^{c_4}}$ and $|T_1 - T_2| \leq c_3 K^{-c_1} |T_1|^{1/2} |T_2|^{1/2}$. By Lemma 3.2,
\[
c_3 K^{-c_1} |T_1|^{1/2} |T_2|^{1/2} \geq |T_1 - T_2| \geq |T_1|^\tau |T_2|^\tau,
\]
and hence
\[
c_3 K^{-c_1} \geq (|T_1| \cdot |T_2|)^{\tau - 1/2} \geq \left(\frac{c_2 p^{0.49}}{K^{c_4}}\right)^{2\tau - 1}.
\]
It follows that $K \geq (1/c_3)p^{-\gamma}$ for an appropriate constant $c_3 > 0$. \hfill \Box

Finally, we need a tool from [3] which states that in (1.1) we need only consider vectors $x$ whose components are 0 or 1 (so-called flat vectors).

**Lemma 3.3** ([3, Lemma 1]). Let $k \geq 2^{10}$ and $s$ be a positive integer. Assume that for all $i \neq j$ we have $\langle u_i, u_j \rangle \leq 1/k$. Also, assume that for some $\delta \geq 0$ and any disjoint $J_1, J_2 \subseteq \{1, \ldots, N\}$ with $|J_1| \leq k, |J_2| \leq k$ we have
\[
\left| \sum_{j \in J_1} u_j, \sum_{j \in J_2} u_j \right| \leq \delta k.
\]
Then $\Phi$ satisfies the RIP property of order $2sk$ with constant $44s\sqrt{\delta \log k}$.

Now we show how to deduce Theorem [2] By Lemma 3.1 and standard bounds for Gauss sums, $\Phi$ satisfies the conditions of Lemma 3.3 with $k = \sqrt{p}$ and $\delta = O(p^{-\frac{1}{2}} \log^2 p)$. Let $\varepsilon_0 < \varepsilon_1/2$ and take $s = \lceil p^{0.6} \rceil$. By Lemma 3.4 $\Phi$ satisfies RIP with order $\geq p^{1/2+\varepsilon_0}$ and constant $O(p^{-\varepsilon_1/2+\varepsilon_0}(\log p)^3)$. If $\varepsilon_0$ is sufficiently close to $\varepsilon_1/2$, Theorem 2 follows with
\[
\varepsilon = 2 - \frac{2}{1 + 2\varepsilon_0} = \frac{4\varepsilon_0}{1 + 2\varepsilon_0} > 2\varepsilon_1 - 2\varepsilon_1^2.
\]
To prove Theorem 1 we take the construction in Section 2. We have (3.1) by Corollary 1. Also take
\[
\eta = 10^{-100}, \quad c_0 = \frac{1}{3}, \quad c_1 = 7/2 + \eta, \quad c_4 = 3/4 + \eta, \quad m = 7586.
\]
These values were optimized with a computer search. By Corollary 1 and (3.3), we have $\gamma \geq 9.182 \cdot 10^{-6}$. It is readily verified that $\gamma \leq \frac{1}{4m}, \varepsilon_1 > 1.631 \cdot 10^{-7}$ and $\varepsilon = 2\varepsilon_1 - 2\varepsilon_1^2$ satisfies $3.26 \cdot 10^{-7} \leq \varepsilon \leq \frac{1}{403m}$, Theorem 1 now follows.

4. ACKNOWLEDGMENTS

The first author was partially supported by NSF Grant DMS-1802139. The second author is supported by a Simons Travel grant. The third author is supported by Ben Green’s Simons Investigator Grant 376201.
REFERENCES

[1] A. Balog, E. Szemerédi, A statistical theorem of set addition, Combinatorica, 14 (1994), 263–268.
[2] J. Bourgain. Multilinear exponential sums in prime fields under optimal entropy condition on the sources. Geom. Funct. Anal., 18(5):1477–1502, 2009.
[3] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova. Explicit constructions of RIP matrices and related problems. Duke Math. J., 159(1):145–185, 2011.
[4] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova. Breaking the $k^2$ barrier for explicit RIP matrices. Symposium on the Theory of Computing (STOC ’11), (2011), 637-644.
[5] 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.
[6] J. Bourgain and A. A. Glibichuk. Exponential sum estimate over subgroup in an arbitrary finite field. J. d’Analyse Math., to appear.
[7] E. J. Candès. The restricted isometry property and its implications for compresses sensing. C. R. Math. Acad. Sci. Paris, 346:589–592, 2008.
[8] E. J. Candès, J. Romberg, and T. Tao. Stable signal recovery from incomplete and inaccurate measurements. Comm. Pure Appl. Math., 59:1208–1223, 2006.
[9] E. J. Candès and T. Tao. Decoding by linear programming. IEEE Trans. Inform. Theory, 51:4203–4215, 2005.
[10] R. DeVore. Deterministic constructions of compressed sensing matrices. J. Complexity, 23:918–925, 2007.
[11] W. T. Gowers, A new proof of Szemerédi’s theorem, Geom. Funct. Anal. 11 (2001), 465–588.
[12] B. S. Kashin. On widths of octahedron. Uspekhi Matem. Nauk, 30:251–252, 1975. Russian.
[13] 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.
[14] B. Murphy and G. Petridis. A second wave of expanders in finite fields. Combinatorial and additive number theory. II, 215–238, Springer Proc. Math. Stat., 220, Springer, Cham, 2017.
[15] J. Nelson and V. N. Temlyakov. On the size of incoherent systems. J. Approx. Th., 163 (2011), no. 9, 1238–1245.
[16] T. Schoen, New bounds in the Balog-Szemerédi-Gowers lemma, Combinatorica 35 (2015), no. 6, 695–701.
[17] T. Tao. Open question: deterministic upp matrices.
https://terrytao.wordpress.com/2007/07/02/open-question-deterministic-upp-matrices/

DEPARTMENT OF MATHEMATICS, 1409 WEST GREEN STREET, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801, USA
Email address: ford@math.uiuc.edu

DEPARTMENT OF MATHEMATICS, 1409 WEST GREEN STREET, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801, USA
Email address: denka@math.uiuc.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OXFORD, RADCLLFE OBSERVATORY, ANDREW WILES BUILDING, WOODSTOCK RD, OXFORD OX2 6GG, UK
Email address: george.shakan@gmail.com