New explicit constructions of RIP matrices

Jean Bourgain[1] Steven J. Dilworth[2] Kevin Ford[3]
Sergei Konyagin[4] Denka Kutzarova[5]

[1]Institute For Advanced Study
[2]University of South Carolina
[3]University of Illinois
[4]Steklov Mathematical Institute
[5]Bulgarian Academy of Sciences

July 20-22, 2011

RIP matrices

Definition

An $n \times N$ matrix (with $n < N$) Φ has the Restricted Isometry Property (RIP) of order k with constant δ if, for all $\mathbf{x}$ with at most k nonzero coordinates, we have

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

Application: sparse signal recovery

- $\mathbf{x} \in \mathbb{C}^N$ is a signal with at most k nonzero components
- $\Phi\mathbf{x}$ is a lower dimensional linear measurement
- Candès, Romberg and Tao (2005-6) showed that given $\Phi\mathbf{x}$, one can effectively recover $\mathbf{x}$ by linear programming;
- It suffices, for sparse signal recovery, that Φ satisfies RIP with fixed constant $\delta < \sqrt{2} - 1$ (Candès, 2008).

Fundamental Problem

Given N, n (fix $\delta = \frac{1}{3}$, say), find a RIP matrix Φ with maximal k (Alternatively, minimize n given N, k).

Theorem (Kashin (1977); Garnaev-Gluskin (1984))

Suppose $n \leqslant N/2$. Choose entries of Φ as independent random variables. With positive probability, Φ will satisfy RIP of order k, for $k = \dfrac{cn}{\log(N/n)}$.

Remarks: Baraniuk, Davenport, DeVore and Wakin (2008) gave a proof using the Johnson-Lindenstrauss lemma.

Other random constructions given by Candès - Tao (2005), Rudelson/Vershinin (2008), Mendelson, Pajor and Tomczak-Jaegermann (2007).

The problem is closely related to the Gel'fand width problems.

limitations of RIP matrices

Theorem (Candès - Tao, 2005)

For all RIP matrices Φ, $k = O\left(\frac{n}{\log(N/n)}\right)$.

The proof uses the lower bound for the Gel'fand width problem due to Garnaev and Gluskin (1984):

$$d^n(U(\ell_1^N), \ell_2) \gg \sqrt{\frac{\log(N/n)}{n}},$$

where, $U(\ell_1^N)$ is the unit ℓ_1-ball in $\mathbb{R}^N$, and for a set K,

$$d^n(K, \ell_2) := \inf_{\substack{\text{subspace} Y \text{ of } \mathbb{R}^N \\ \text{codim}(Y) \leqslant n}} \sup\{\|x\|_2 : x \in K \cap Y\}.$$

Coherence

Definition

The coherence μ *of unit vectors* $\mathbf{u}_1, \dots, \mathbf{u}_N \in \mathbb{C}^n$ *is*

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

Sets of vectors with small coherence are spherical codes

Proposition

Suppose that $\mathbf{u}_1, \dots, \mathbf{u}_N$ *are the columns of* Φ *with coherence* μ.
For all k, Φ *satisfies RIP of order* k *with constant* $\delta = k\mu$.
Cor: Φ *satisfies RIP of order* $k = 1/(3\mu)$ *and* $\delta = \frac{1}{3}$.

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

$$\left| \|\Phi \mathbf{x}\|_2^2 - \|\mathbf{x}\|_2^2 \right| = \sum_{r \neq s} |x_r x_s \langle \mathbf{u}_r, \mathbf{u}_s \rangle| \leqslant \mu \left(\sum |x_r| \right)^2 \leqslant k\mu \|\mathbf{x}\|_2^2.$$

Explicit constructions of RIP matrices: coherence

Many explicit contructions of vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$ satisfying

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

e.g. Kashin (1975), Alon-Goldreich-Håstad-Peralta (1992), DeVore (2007), Andersson (2008), and Nelson-Temlyakov (2010). All based on the arithmetic in finite fields.

Corollary: Such Φ with columns $\mathbf{u}_j$ satisfies RIP with $\delta = \frac{1}{3}$ and all $k = \frac{c\sqrt{n}\log n}{\log N}$.
Limitation: (Levenshtein, 1983) For all $\mathbf{u}_1, \ldots, \mathbf{u}_N$,

$$\mu \geqslant c\left(\frac{\log N}{n\log(n/\log N)}\right)^{1/2} \geqslant \frac{c}{\sqrt{n}},$$

With coherence, we cannot deduce RIP of order larger than $\sqrt{n}$.

Explicit constructions: Kashin

Kashin (1977): prime p, $n = p$, $r \geqslant 1$,

$$A \subseteq \{(a_1, \dots, a_r) : 0 \leqslant a_1 < \cdots < a_r < p\},\ N = |A| \leqslant \binom{p}{r}.$$

For $\mathbf{a} \in A$, let

$$\mathbf{u}_\mathbf{a} = \frac{1}{\sqrt{p-r}} \left(\left(\frac{(j+a_1)\cdots(j+a_r)}{p} \right) : j \in \mathbb{F}_p \right)^T.$$

Here
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has no solution.} \end{cases}$$

Coherence: By Weil's bound, for $\mathbf{a} \neq \mathbf{a}'$,

$$|\langle \mathbf{u}_\mathbf{a}, \mathbf{u}_{\mathbf{a}'} \rangle| = \frac{1}{p-r} \left| \sum_{j=0}^{p-1} \left(\frac{(j+a_1)\cdots(j+a'_r)}{p} \right) \right|$$
$$\leqslant \frac{2r\sqrt{p}}{p-r} \asymp \frac{r}{\sqrt{p}} \asymp \frac{\log N}{\sqrt{n}\log n}.$$

Explicit constructions: DeVore

DeVore (2007): prime p, $n = p^2$, $r \geqslant 1$

P_r = a rich subset of the polynomials over $\mathbb{F}_p$ of degree $\leqslant r$, $N = |P_r| \leqslant p^{r+1}$. Say $P_r = \{f_1, \dots, f_N\}$.

For $1 \leqslant j \leqslant N$, $a, b \in \{0, 1, \dots, p-1\}$, let

$$\mathbf{u}_j(ap + b) = \begin{cases} \frac{1}{\sqrt{p}} & (a, b) = (x, f_j(x)) \text{ for some } x \\ 0 & \text{else.} \end{cases}$$

Coherence: If $f \neq g$ and $N \approx p^{r+1}$, then

$$\begin{aligned} \langle \mathbf{u}_f, \mathbf{u}_g \rangle &= \frac{1}{p} \#\{x \in \mathbb{F}_p : f(x) = g(x)\} \\ &\leqslant \frac{r}{p} = \frac{r}{\sqrt{n}} \asymp \frac{\log N}{\sqrt{n} \log n}. \end{aligned}$$

Explicit constructions: Nelson-Temlyakov

Nelson-Temlyakov (2010):
P_r = a rich subset of the polynomials over $\mathbb{F}_p$ of degree $\leqslant r$,
$N = |P_r| \leqslant p^{r+1}$.

Same P_r, but now $n = p$ and

$$\mathbf{u}_f = \frac{1}{\sqrt{p}} \left(e^{2\pi i f(x)/p} : x \in \mathbb{F}_p \right).$$

By Weil's bounds again, for $f \neq g$,

$$|\langle \mathbf{u}_f, \mathbf{u}_g \rangle| = \frac{1}{p} \left| \sum_{x \in \mathbb{F}_p} e^{2\pi i (f(x) - g(x))/p} \right| \leqslant \frac{r-1}{\sqrt{p}} \asymp \frac{\log N}{\sqrt{n} \log n}.$$

Breaking the $\sqrt{n}$ barrier with explicit constructions

Theorem (BDFKK, 2010)

For some constants $\alpha > 0$ and $\beta > 0$, large N and $N^{1-\alpha} \leqslant n \leqslant N$, the $N \times n$ matrix below satisfies RIP of order $k = n^{1/2+\beta}$.

The construction: Take m a large integer, p a large prime,

- $\mathcal{A} = \left\{1, 2, \ldots, \lfloor p^{1/m} \rfloor\right\}$,
- $M = 2^{2m-1}$, $r = \left\lfloor \frac{\log p}{2m \log 2} \right\rfloor$,

  $$\mathcal{B} = \left\{ \sum_{j=0}^{r-1} x_j (2M)^j : 0 \leqslant x_j \leqslant M-1 \right\} \subset \{1, \ldots, p-1\}$$

- matrix columns $\mathbf{u}_{(a,b)} = \frac{1}{\sqrt{p}} \left(e^{2\pi i (ax^2+bx)/p} \right)_{1 \leqslant x \leqslant p}$;

  $a \in \mathcal{A}, b \in \mathcal{B}$.
- $N = |\mathcal{A}| \cdot |\mathcal{B}| \asymp p^{1+1/(2m)}$, $n = p$.

Some ideas of the proof

$$\mathcal{A} = \left\{1, 2, \ldots, \lfloor p^{1/m} \rfloor\right\}, \ \mathcal{B} = \left\{\sum_{j=0}^{r-1} x_j (2M)^j : 0 \leqslant x_j \leqslant M-1\right\}.$$

matrix columns $\mathbf{u}_{(a,b)} = p^{-1/2}\left(e^{2\pi i(ax^2+bx)/p}\right)_{x\in\mathbb{F}_p}$; $a \in \mathcal{A}, b \in \mathcal{B}$.

$|\mathcal{B}| \asymp p^{1-\frac{1}{2m}}$, $N = |\mathcal{A}| \cdot |\mathcal{B}|$, $n = p$.

---

(1) $\langle \mathbf{u}_{a,b}, \mathbf{u}_{a',b'} \rangle = 0$ if $a = a', b \neq b'$ and otherwise

$$\langle \mathbf{u}_{a,b}, \mathbf{u}_{a',b'} \rangle = \frac{\sigma_p}{\sqrt{p}} \left(\frac{a-a'}{p}\right) e^{-2\pi i (b-b')^2 [4(a-a')]^{-1}/p}$$

by Gauss' formula. Here c^{-1} means inverse in $\mathbb{F}_p$, $\sigma_p \in \{-1, 1\}$.

(2) The game is to capture cancellations among the exponentials. This is done using *additive combinatorics.* A key: adding elements of $\mathcal{B}$ involves no "carries" in base-$2M$.

Flat-RIP

Let $\mathbf{u}_1, \ldots, \mathbf{u}_N$ be the columns of an $n \times N$ matrix Φ, $\|\mathbf{u}_j\|_2 = 1$.

It is more convenient to work with 0-1 vectors $\mathbf{x}$ ("flat" vectors). If the RIP property holds when restricted to flat vectors, then it holds with all vectors with an increase in δ.

Lemma (BDFKK, 2010)

Let $k \geqslant 2^{10}$ and s be a positive integer. Suppose that the coherence of vectos $\mathbf{u}_j$ is $\leqslant 1/k$ and, for any disjoint $J_1, J_2 \subset \{1, \ldots, N\}$ with $|J_1| \leqslant k, |J_2| \leqslant k$, we have

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

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

We show this "flat-RIP" property in the lemma with $k = \sqrt{p} = \sqrt{n}$ and $\delta = p^{-\varepsilon}$ for some fixed $\varepsilon > 0$. Then take $m \approx p^{\varepsilon/3}$.

Further issues

Matrix columns $\mathbf{u}_{(a,b)} = p^{-1/2}\left(e^{2\pi i(ax^2+bx)/p}\right)_{x\in\mathbb{F}_p}$; $a \in \mathcal{A}, b \in \mathcal{B}$.

$|\mathcal{B}| \asymp p^{1-\frac{1}{2m}}$, $N = |\mathcal{A}| \cdot |\mathcal{B}|$, $n = p$.

---

1. Our Φ have complex entries. However, for any RIP matrix Φ, replacing each entry $a + ib$ with the 2×2 matrix $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ yields a $2n \times 2N$ real matrix having identical RIP parameters.
2. We are able to prove the RIP property for these matrices provided m is very large (approximately 10^8). This comes from the use of some results in additive combinatorics which are believed to be sub-optimal. Consequently, $n > N^{1-\beta}$ for some very small $\beta > 0$ is required for our proofs to work. It is likely that our matrices satisfy RIP for much smaller m.
3. Can we generalize our construction, using cubic or higher degree polynomials in place of quadratics (as in the constructions of DeVore and Nelson-Temlyakov)? **Problem:** there is no analog of Gauss' formula. Such matrices *may* still satisfy RIP (and would allow us to take smaller n).

Preview of talk # 2

We give a brief introduction to the field of additive combinatorics, and describe some results that are needed in our argument: these include

1. Bounds for sumsets with subsets of $\mathcal{B}$
2. A version of the Balog-Szemeredi-Gowers lemma
3. Bounds for the number of solutions of equations of the formula
$$\frac{1}{a_1} + \cdots + \frac{1}{a_k} = \frac{1}{b_1} + \cdots + \frac{1}{b_k},$$
with $a_1, \ldots, b_k \in \mathcal{C}$, where $\mathcal{C}$ is an arbitrary set of positive integers, and equations
$$a_1 + a_2 b = a_3 + a_4 b,$$
where $a_i \in \mathcal{A}$, $b \in \mathcal{B}$ and $\mathcal{A}$ and $\mathcal{B}$ are arbitrary sets of integers.

Preview of talk # 3

We describe in some detail how additive combinatorics are used to prove that our matrices satisfy RIP with $k \geqslant n^{1/2+\beta}$.

By the flat-RIP lemma, it suffices to prove the following:

Lemma

Let m be sufficiently large and p sufficiently large. Then for any disjoint sets $\Omega_1, \Omega_2 \subset \mathcal{A} \times \mathcal{B}$ such that $|\Omega_1| \leqslant \sqrt{p}$, $|\Omega_2| \leqslant \sqrt{p}$,

$$\left| \sum_{\omega_1 \in \Omega_1} \sum_{\omega_2 \in \Omega_2} \langle \mathbf{u}_{\omega_1}, \mathbf{u}_{\omega_2} \rangle \right| \leqslant p^{1/2-\varepsilon},$$

where $\varepsilon > 0$ is fixed (depends only on m).

The inequality with $\varepsilon = 0$ is trivial (from Gauss' formula, $|\langle \mathbf{u}_{\omega_1}, \mathbf{u}_{\omega_2} \rangle| \leqslant 1/\sqrt{p}$ for all ω_1, ω_2).

New explicit constructions of RIP matrices

Lecture # 2 : Additive Combinatorics

Standard references:

1. H. Halberastam and K. F. Roth, *Sequences*, 1966.
2. M. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, 1996.
3. T. Tao and V. Vu, *Additive Combinatorics*, 2006.

Set addition basics

Let G be an additive group. For $A, B \subset G$, define the sumset

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

Important cases: $G = \mathbb{Z}$, $G = \mathbb{Z}^d$, $G = \mathbb{Z}/m\mathbb{Z}$, $G = (\mathbb{Z}/m\mathbb{Z})^d$.
Example: $\{1, 2, 4\} + \{0, 3, 6\} = \{1, 2, 4, 5, 7, 8, 10\}$.

Generic problem. Given information about A, bound $|A + A|$.

Inverse problem. Given that $|A + A|$ is small (resp. large), deduce some structural information about A.

Remark: Similar theory for $A - A = \{a - a' : a, a' \in A\}$, since

$$a_1 + a_2 = a_3 + a_4 \iff a_1 - a_3 = a_4 - a_2.$$

Sumsets: some basic examples

Example. $G = \mathbb{Z}$, $|A| = N$. Then

$$2N - 1 \leqslant |A + A| \leqslant N^2.$$

Proof: WLOG $\min A = 0$. if $A = \{a_1 = 0, \ldots, a_N\}$, $0 < a_2 < \cdots < a_N$, then $A + A$ contains

$$S = \{a_1, a_2, \ldots, a_N, a_2 + a_N, a_3 + a_N, \ldots, a_N + a_N\}.$$

Theorem: $|A + A| = 2N - 1$ if and only if A is an *arithmetic progression*: $A = \{a, a + d, \ldots, a + (N - 1)d\}$ for some $a, d \in \mathbb{Z}$.
Proof. (i) WLOG $\min A = 0$. If $A = \{0, d, \ldots, d(N - 1)\}$, then $A + A = \{0, d, \ldots, d(2N - 2)\}$.
(ii) if $|A| = N$ and $|A + A| = 2N - 1$, then $A + A = S$. In particular, $a_2 + a_i \in S$ for all $i < N$. But $a_2 + a_i < a_2 + a_N$, so $a_2 + a_i \in A$ for $i < N$. Easy to see $a_2 + a_i = a_{i+1}$ for $i < N$, so A is an arithmetic progression.

Sets with small doubling

A set of the form

$$B = \{a + k_1 d_1 + \cdot + k_r d_r : 0 \leqslant k_i \leqslant m_i - 1 (1 \leqslant i \leqslant r)\}$$

is called an *r-dimensional arithmetic progression*. If r is small, these sets have small doubling, i.e. $|B + B| \leqslant 2^r |B|$.

Theorem (G. Freiman, 1960s)

If A is a finite set of integers and $|A + A| < KN$, then A is a subset of an r-dimensional arithmetic progression with r and $m_1 \cdots m_r / |A|$ bounded in terms of K. We say A has "additive structure".

Very active area today to find good bounds on r and $m_1 \cdots m_r / |A|$ as functions of K.

Sumset estimates in product sets, I

Recall $\mathcal{B} = \left\{ \sum_{j=0}^{r-1} x_j (2M)^j : 0 \leqslant x_j \leqslant M-1 \right\}$.

- Addition in $\mathcal{B}$ involves no "carries" in base-$2M$. In an additive sense, $\mathcal{B}$ behaves like $\mathcal{C}_{M,r} = \{0, \dots, M-1\}^r$. Let

  $$\phi\left(x_{r-1}(2M)^{r-1} + \cdots + x_1(2M) + x_0\right) = (x_0, \dots, x_{r-1}).$$

  Then ϕ is a "Freiman isomorphism": for $b_1, \dots, b_4 \in \mathcal{B}$,

  $$b_1 + b_2 = b_3 + b_4 \iff \phi(b_1) + \phi(b_2) = \phi(b_3) + \phi(b_4).$$

  In particular, for $D, E \subset \mathcal{B}$, $|D + E| = |\phi(D) + \phi(E)|$.

- $\mathcal{C}_{M,r}$ does not possess long arithmetic progressions (M is fixed, r is very large). Hence, we expect that $D + E$ cannot be too small, if $D, E \subset \mathcal{B}$.

Sumset estimates in product sets, II

Recall $\mathcal{B} = \left\{ \sum_{j=0}^{r-1} x_j (2M)^j : 0 \leqslant x_j \leqslant M-1 \right\}$.

For nonempty $D \subset \mathcal{B}$, it is trivial that

$$|D+D| \geqslant |D|.$$

Theorem B1 (BDFKK, 2010)

Let $r, M \in \mathbb{N}, M \geqslant 2$ and let $\tau = \tau_M$ be the solution of the equation $M^{-2\tau} + (1-1/M)^\tau = 1$. Then $\tau > \frac{1}{2}$ and for any $D \subset \mathcal{C}_{M,r}$ we have

$$|D+D| \geqslant |D|^{2\tau}.$$

Approximately, $\tau_M \approx \frac{1}{2} + \frac{\log 2}{2 \log M} \approx \frac{1}{2} + \frac{1}{4m}$. We conjecture that the extremal case is $D = \mathcal{C}_{M,r}$ and that τ may be improved to

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

This is true for $M = 2$ (Woodall, 1977).

Additive properties of integer reciprocals

Recall $\mathcal{A} = \{1, 2, 3, \dots, \lfloor p^{1/s} \rfloor\}$.

Theorem A (BDFKK, 2010)

Suppose $m \geqslant 1$, $\mathcal{N}$ is a set of positive integers in $[1, N]$. For every $\varepsilon > 0$, the number of solutions of

$$\frac{1}{n_1} + \cdots + \frac{1}{n_m} = \frac{1}{n_{m+1}} + \cdots + \frac{1}{n_{2m}} \qquad (n_i \in \mathcal{N}, 1 \leqslant i \leqslant 2m)$$

is $\leqslant C(m, \varepsilon) |\mathcal{N}|^m N^{\varepsilon}$, for some constant $C(m, \varepsilon)$.

Remark: There are $\geqslant |\mathcal{N}|^m$ trivial solutions $(n_{m+i} = n_i,\ i \leqslant m)$

Idea (from a paper of Karatsuba): Clearing denominators leads to divisibility conditions $n_i | \prod_{j \neq i} n_j$. So every prime dividing one of the n_i must divide another. Key inequality:

$$\forall \varepsilon > 0, \exists c(\varepsilon) \text{ such that } \#\{d : d|n\} \leqslant c(\varepsilon) n^{\varepsilon}.$$

Additive energy, I

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

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

Special case: $A = B$, $G = \mathbb{Z}$.

- Trivially, $E(A,A) \leqslant |A|^3$.
- If A is an arithmetic progression, $E(A,A) \sim \frac{2}{3}|A|^3$.
- If $E(A,A) \geqslant |A|^3/K$ with small K, must A be "structured" (like an arithmetic progression of small dimension) ?
- **No!** If A contains a long arithmetic progression, say of length $\delta|A|$, then $E(A,A) > \frac{2}{3}\delta^3|A|^3$, even if the other $(1-\delta)|A|$ elements of A are unstructured (look like a random set).
- However, if $E(A,A)$ is close to $|A|^3$ then A must have a large structured subset.

Additive energy, II

Theorem E (BDFKK, 2010)

If A is a finite set of integers and $E(A,A) \geqslant |A|^3/K$, then there exists $A' \subset A$ such that $|A'| \geqslant |A|/(20K)$ and

$$|A' + A'| \leqslant 10^{17} K^{20} |A'|.$$

The proof is a relatively simple consequence of a variant of the fundamental Balog-Szemeredi-Gowers Lemma:

Theorem (Bourgain-Garaev, 2009)

If $F \subset A \times A$, $|F| \geqslant |A|^2/L$ and

$$\#\{a_1 + a_2 : (a_1, a_2) \in F\} \leqslant L|A|.$$

Then there exists $A' \subset A$ such that $|A'| \geqslant |A|/(10L)$ and $|A' - A'| \leqslant 10^4 L^9 |A|$.

The proof uses "elementary" graph-theory (Tao-Vu §2.5, 6.4).

Additive energy, III. Theorems B1 and E

Theorem B1 (BDFKK, 2010)

For some $\tau > \frac{1}{2}$ and for any $D \subset \mathcal{B}$ we have $|D + D| \geqslant |D|^{2\tau}$.

Theorem E (BDFKK, 2010)

If A is a finite set of integers and $E(A, A) \geqslant |A|^3/K$, then there exists $A' \subset A$ such that $|A'| \geqslant |A|/(20K)$ and

$$|A' + A'| \leqslant 10^{17} K^{20} |A'|.$$

Corollary: Suppose $A \subset \mathcal{B}$. Take $K = c|A'|^{(2\tau-1)/20}$ (A' from Theorem E) and deduce

Theorem B2 (BDFKK, 2010)

For any $A \subset \mathcal{B}$,

$$E(A, A) = O\left(|A|^{3-\gamma}\right), \qquad \gamma = \frac{2\tau - 1}{20 + 2\tau - 1}.$$

Twisted energy averages

Theorem (Bourgain, 2009 (GAFA))

Suppose $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p \setminus \{0\}$*. For some* $c > 0$,

$$\sum_{b \in B} E(A, b \cdot A) := \#\{a_1 + ba_2 = a_3 + ba_4 : a_i \in A, b \in B\}$$

$$\ll (\min(p/|A|, |A|, |B|))^{-c} |A|^3 |B|.$$

Remarks. An explicit version of the theorem, with $c = \frac{1}{10430}$, given by Bourgain-Glibuchuk (2011). Open: Is the statement true with any $c < 1$?

Idea (over $\mathbb{Z}$): Say $A = \{0, 1, \dots, N-1\}$. So $E(A, A)$ is very large. However,if $b \geqslant 1$, we have $a_1 - a_3 = b(a_4 - a_2)$, which forces $|a_4 - a_2| < (N-1)/b$ and hence $E(A, b \cdot A) \leqslant 2N^3/b$.

Fourier analysis and sumsets

For a set $A \subset \mathbb{Z}$, let

$$T_A(\theta) = \sum_{a \in A} e^{2\pi i \theta a}$$

be the trigonometric sum associated with A. Clearly,

$$T_A(\theta)^2 = \sum_{c \in A+A} r(c) e^{2\pi i \theta c}, \quad r(c) = \#\{(a, a') \in A^2 : a + a' = c\}.$$

Also,

$$r(c) = \int_0^1 T_A(\theta)^2 e^{-2\pi i \theta c}\, d\theta.$$

If A is an arithmetic progression $\{a, a+d, \ldots, a+(N-1)d\}$, then $T_A(\theta)$ is a geometric sum - concentrated mass (large only for θ near points k/d, $k \in \mathbb{Z}$).

Conversely, if the mass of $T_A(\theta)$ is very concentrated, then A has "arithmetic progression - like behavior", i.e. $A + A$ is small.

Fourier analysis in finite fields

For a set $A \subset \mathbb{F}_p$, let

$$T_A(\theta) = \sum_{a \in A} e^{2\pi i \theta a}.$$

Then

$$r(c) = \#\{(a, a') \in A^2 : a + a' = c\} = \frac{1}{p} \sum_{a \in \mathbb{F}_p} T_A^2(a/p) e^{-2\pi i a c/p}.$$

Exponential sums and additive energy

Recall (Gauss sum formula)

$$\langle \mathbf{u}_{a,b}, \mathbf{u}_{a',b'} \rangle = \frac{\sigma(a,a',p)}{\sqrt{p}} e^{-2\pi i (b-b')^2 \lambda(a,a')/p},$$

where $|\sigma(a,a',p)| = 1$ and $\lambda(a,a') = (4(a-a'))^{-1} \mod p$.

Lemma

For any $\theta \in \mathbb{F}_p \backslash \{0\}$, $B_1 \subset \mathbb{F}_p$, $B_2 \subset \mathbb{F}_p$ we have

$$\left| \sum_{b_1 \in B_1, b_2 \in B_2} e^{2\pi i \theta (b_1 - b_2)^2 / p} \right| \leqslant |B_1|^{\frac{1}{2}} E(B_1, B_1)^{\frac{1}{8}} |B_2|^{\frac{1}{2}} E(B_2, B_2)^{\frac{1}{8}} p^{\frac{1}{8}}.$$

Proof sketch. Three successive applications of Cauchy-Schwarz. Observe that

$$E(B,B) = \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{b \in B} e^{2\pi i ab/p} \right|^4$$

New explicit constructions of RIP matrices

Lecture # 3 : Sketch of the proof of our theorem
Plus Turán's power sums

Goal

Theorem

Let m be a sufficiently large, fixed constant and p sufficiently large. There is a fixed $\varepsilon > 0$ (depending only on m), so that for any disjoint sets $\Omega_1, \Omega_2 \subset \mathcal{A} \times \mathcal{B}$ such that $|\Omega_1| \leqslant \sqrt{p}$, $|\Omega_2| \leqslant \sqrt{p}$,

$$S := \left| \sum_{\omega_1 \in \Omega_1} \sum_{\omega_2 \in \Omega_2} \langle \mathbf{u}_{\omega_1}, \mathbf{u}_{\omega_2} \rangle \right| \leqslant p^{1/2-\varepsilon},$$

Def. $A_i = \{a_i : (a_i, b_i) \in \Omega_i\} \qquad (i = 1, 2).$

Def. $\Omega_i(a_i) = \{b_i : (a_i, b_i) \in \Omega_i\} \qquad (i = 1, 2).$

Small A_i

(i) Suppose $|A_i| \leqslant p^{\gamma/3}$ for $i = 1, 2$. Recall

Lemma

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

$$\Big| \sum_{b_1 \in B_1, b_2 \in B_2} e^{2\pi i \theta (b_1 - b_2)^2 / p} \Big| \leqslant |B_1|^{\frac{1}{2}} E(B_1, B_1)^{\frac{1}{8}} |B_2|^{\frac{1}{2}} E(B_2, B_2)^{\frac{1}{8}} p^{\frac{1}{8}}.$$

By this lemma, Lemma B2 (that $E(B, B) \ll |B|^{3-\gamma}$ for $B \subset \mathcal{B}$), and Hölder:

$$\begin{aligned} S &\leqslant p^{-1/2} \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} |\Omega_1(a_1)|^{\frac{7-\gamma}{8}} |\Omega_2(a_2)|^{\frac{7-\gamma}{8}} p^{\frac{1}{8}} \\ &\leqslant p^{-\frac{1}{2}+\frac{1}{8}} |A_1|^{\frac{1+\gamma}{8}} \Big(\sum_{a_1} |\Omega_1(a_1)| \Big)^{\frac{7-\gamma}{8}} |A_2|^{\frac{1+\gamma}{8}} \Big(\sum_{a_2} |\Omega_2(a_2)| \Big)^{\frac{7-\gamma}{8}} \\ &\leqslant p^{\frac{1}{2} - \frac{\gamma}{8} + \frac{\gamma^2+\gamma}{12}} \leqslant p^{\frac{1}{2} - \varepsilon}, \qquad \text{if } \varepsilon \leqslant \frac{\gamma}{24} - \frac{\gamma^2}{12}. \end{aligned}$$

Small $E(\Omega_i(a_i), \Omega_1(a_i))$

(ii) Suppose $E(\Omega_i(a_i), \Omega_i(a_i)) \leqslant |\Omega_1(a_i)|^3 p^{-2/m}$ for some i (say $i = 1$). By the same lemma and Hölder's inequality, the sum of $\langle \mathbf{u}_{(a_1,a_2)}, \mathbf{u}_{(a_2,b_2)} \rangle$ over quadruples with such a_1 is

$$\leqslant p^{-\frac{1}{2}+\frac{1}{8}} \sum_{a_1,a_2} |\Omega_1(a_1)|^{\frac{7}{8}} p^{-\frac{2}{8m}} |\Omega_2(a_2)|^{\frac{7-\gamma}{8}}$$

$$\leqslant p^{-\frac{3}{8}-\frac{2}{8m}} |A_1|^{\frac{1}{8}} |A_2|^{\frac{1+\gamma}{8}} \Big(\sum_{a_1} |\Omega_1(a_1)| \Big)^{\frac{7}{8}} \Big(\sum_{a_2} |\Omega_2(a_2)| \Big)^{\frac{7-\gamma}{8}}$$

$$\leqslant p^{\frac{1}{2}-\frac{\gamma}{16}+\frac{\gamma}{8m}} \leqslant p^{\frac{1}{2}-2\varepsilon}, \qquad \varepsilon \leqslant \frac{\gamma}{32} - \frac{\gamma}{16m}.$$

Remaining case

(iii) We now consider the case $\max|A_i| > p^{\gamma/3}$ (WLOG $|A_2| > p^{\gamma/3}$), and $E(B,B) > |B|^3 p^{-2/m}$, $B = \Omega_1(a_1)$.

Using Theorem E, we can reduce to consideration of the case where $|B-B| \leqslant p^{30/m}|B|$ and $|B+B| \leqslant p^{60/m}|B|$. With a_1 fixed, we show that

$$\Big| \sum_{\substack{b_1 \in B \\ a_2 \in A_2, b_2 \in \Omega_2(a_2)}} \left(\frac{a_1 - a_2}{p}\right) e_p\left((b_1 - b_2)^2 [4(a_1 - a_2]^{-1}\right) \Big| \ll |B| p^{1/2-\varepsilon}.$$

where $e_p(x) = e^{2\pi i x/p}$. Denote by $T(a_1)$ the above sum.

Subdivide into cases according to the size of $\Omega_2(a_2)$: say

$$M_2 < |\Omega_2(a_2)| \leqslant 2M_2, \qquad M_2 = 2^j.$$

Further details

Say m is even. Cauchy-Schwartz + Hölder:

$$|T(a_1)|^2 \leqslant \sqrt{p}|B|^{2-2/m} \left(\sum_{b_1, b \in B} |F(b, b_1)|^m \right)^{\frac{1}{m}},$$

where

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

Also,

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

$$\leqslant M_2^m \sum_{y \in B-B} \sum_{\substack{a^{(i)} \in A_2 \\ 1 \leqslant i \leqslant m}} \left| \sum_{x \in B+B} e_p \left(\frac{xy}{4} \sum_{i=1}^{m/2} \left[\frac{1}{a_1 - a^{(i)}} - \frac{1}{a_1 - a^{(i+m/2)}} \right] \right) \right|.$$

Further details, II

For some complex numbers $\varepsilon_{y,\xi}$ of modulus $\leqslant 1$,

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

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

By Theorem A, since $A_2 \subset [1, p^{1/m}]$, for any $\nu > 0$,

$$\lambda(0) \ll_\nu |A_2|^{m/2} p^\nu.$$

Therefore,

$$\sum_{b_1,b\in B} |F(b,b_1)|^m \ll_\nu M_2^m |A_2|^{m/2} p^\nu |B-B||B+B| + \sum_{y\in B-B} \sum_{\xi\in\mathbb{F}_p^*} \lambda(\xi)\varepsilon_{y,\xi} \sum_{x\in B+B} e_p(xy\xi/4).$$

Further details, III

Let

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

By Hölder and Parseval, we arrive at

$$\left| \sum_{y \in B-B} \sum_{\xi \in \mathbb{F}_p^*} \varepsilon'_{y,\xi} \sum_{x \in B+B} e_p(xy\xi/4) \right| \leqslant |B+B|^{3/4} \|\zeta * \zeta\|_2^{1/2} p^{1/4}.$$

Then

$$\|\zeta * \zeta\|_2 \leqslant \sum_{\xi, \xi' \in \mathbb{F}_p^*} \lambda(\xi)\lambda(\xi') \left| \{ y_1 - (\xi/\xi')y_2 = y_3 - (\xi/\xi')y_4 : y_i \in B-B \} \right|^{1/2}.$$

The RHS is estimated using a weighted version of Bourgain's theorem on $\sum_{d \in D} E(A, d \cdot A)$, with $A = B - B$.

Turán's power sums

Def: For $|z_j| = 1$, let

$$M_N(\mathbf{z}) = \max_{m=1,2,\ldots,N} \left| \sum_{j=1}^{n} z_j^m \right|.$$

Problem: find $\mathbf{z}$ to minimize $M_N(\mathbf{z})$.

Connection with coherence: The vectors

$$\mathbf{u}_m = \frac{1}{\sqrt{n}} \left(z_1^{m-1}, \ldots, z_n^{m-1} \right)^T, \quad 1 \leqslant m \leqslant N,$$

have coherence $\mu = \frac{1}{n} M_{N-1}(\mathbf{z})$.

Constructions for Turán's power sums

Erdős - Rényi (1957): If z_j chosen randomly on the unit circle for each j, then with overwhelming probability, $M_N(\mathbf{z}) \ll \sqrt{n \log N}$.

Montgomery (1978): p prime, $n = p - 1$, χ a Dirichlet character of order $p - 1$. Put

$$z_j = \chi(j) e^{2\pi i j/p}, \quad 1 \leqslant j \leqslant p - 1.$$

Then $M_N(\mathbf{z}) \leqslant \sqrt{p} = \sqrt{n+1}$ for $N < n(n+1)$.

Andersson (2008). p prime, $N = p^d - 1$, χ a generator of the group of characters of $F = \mathbb{F}_{p^d}$, $y \in F$ but in no proper subfield. Put

$$z_j = \chi(y + j - 1), \qquad 1 \leqslant j \leqslant p, \quad n = p.$$

By a character sum bound of N. Katz,

$$M_N(\mathbf{z}) \leqslant (d-1)\sqrt{p} \leqslant \sqrt{n} \frac{\log N}{\log n}.$$

Remark: the bound is nontrivial for $N < e^{\sqrt{n}}$.

New explicit construction

Theorem (BDFKK, 2010)

We give explicit constructions of $\mathbf{z}$ *such that*

$$M_N(\mathbf{z}) = O\left((\log N \log\log N)^{1/3} n^{2/3}\right).$$

Remark. Our constructions are better than Andersson's constructions for $N \geqslant \exp\{n^{1/4}\}$, nontrivial for $N < \exp\{cn/\log n\}$.

Corollary. Explicit constructions of vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$ with coherence

$$\mu = O\left(\left(\frac{\log N \log\log N}{n}\right)^{1/3}\right).$$

This matches, up to a power of $\log\log N$, the best known explicit constructions for codes when $n \lesssim (\log N)^4$.

Some ideas of the proof

Based on ideas in a paper of Ajtai, Iwaniec, Komlós, Pintz and Szemerédi (1990).
They were interested in constructing sets $T \subseteq \{1, \dots, N\}$ such that all the Fourier coefficients

$$\sum_{t \in T} e^{2\pi i m t/N}, \quad 1 \leqslant m \leqslant N-1,$$

are uniformly small, with $|T|$ taken a small as possible.

The construction: Parameters P_0, $P_1 > P_0$, $R \approx \log(P_0/\log P_1)$,

$$T_q = \text{ multiset } \{r + s/p : 1 \leqslant r \leqslant R, P_0 < p \leqslant 2P_0 \text{ prime}, |s| < p/2\}$$

of residues modulo q. Finally, let $\mathbf{z}$ be the multiset of numbers $e^{2\pi i t/q}$, $P_1 < q \leqslant 2P_1$ (q prime), $t \in T_q$.