Explicit constructions of RIP matrices and related problems

Jean Bourgain\textsuperscript{1} Steven J. Dilworth\textsuperscript{2} Kevin Ford\textsuperscript{3} Sergei Konyagin\textsuperscript{4} Denka Kutzarova\textsuperscript{5}

\textsuperscript{1}Institute For Advanced Study
\textsuperscript{2}University of South Carolina
\textsuperscript{3}University of Illinois
\textsuperscript{4}Steklov Mathematical Institute
\textsuperscript{5}Bulgarian Academy of Sciences

August 2, 2010
RIP matrices

**Definition**

An $N \times n$ matrix (with $n < N$) $\Phi$ has the Restricted Isometry Property (RIP) of order $k$ with constant $\delta$ if, for all $k$-sparse vectors $x$, we have

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

**Application:** sparse signal recovery

- $x \in \mathbb{C}^N$ is a signal with at most $k$ nonzero components
- $\Phi x \in \mathbb{C}^n$ is a lower dimensional linear measurement
- Candès, Romberg and Tao (2006) showed that given $\Phi x$, one can effectively recover $x$;
- It suffices, for sparse signal recovery, that $\Phi$ 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 \( \Phi \) with maximal \( k \) (Alternatively, minimize \( n \) given \( N, k \)).
Fundamental Problem

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

**Theorem (Kashin (1977); Candèes, Romberg, Tao (2006))**

Suppose $n \leq N/2$. Choose entries of $\Phi$ as independent $\pm n^{-1/2}$ Bernouilli random variables. With positive probability, $\Phi$ will satisfy RIP of order $k$, for all $k \leq \frac{cn}{\log(N/n)}$.

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

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

**Theorem (Kashin (1977); Candès, Romberg, Tao (2006))**

Suppose $n \leq N/2$. Choose entries of $\Phi$ as independent $\pm n^{-1/2}$ Bernouilli random variables. With positive probability, $\Phi$ will satisfy RIP of order $k$, for all $k \leq \frac{cn}{\log(N/n)}$.


**Theorem (Nelson and Temlyakov, 2010)**

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

Explicit RIP matrices
Coherence

Definition

The coherence $\mu$ of unit vectors $u_1, \ldots, u_N \in \mathbb{C}^n$ is

$$\mu := \max_{r \neq s} |\langle u_r, u_s \rangle|.$$
The coherence $\mu$ of unit vectors $u_1, \ldots, u_N \in \mathbb{C}^n$ is

$$\mu := \max_{r \neq s} |\langle u_r, u_s \rangle|.$$ 

Sets of vectors with small coherence are spherical codes.
**Coherence**

**Definition**

The **coherence** $\mu$ of unit vectors $u_1, \ldots, u_N \in \mathbb{C}^n$ is

$$\mu := \max_{r \neq s} |\langle u_r, u_s \rangle|.$$ 

Sets of vectors with small coherence are **spherical codes**

**Proposition**

Suppose that $u_1, \ldots, u_N$ are the columns of $\Phi$ with coherence $\mu$. For all $k$, $\Phi$ satisfies RIP of order $k$ with constant $\delta = k\mu$.

**Cor:** $\Phi$ satisfies RIP of order $k = \lceil 1/(3\mu) \rceil$ and $\delta = \frac{1}{3}$.

**Proof:** For a $k$-sparse vector $x$,

$$||\Phi x||^2_2 - ||x||^2_2 = \sum_{r,s} |x_r x_s \langle u_r, u_s \rangle| \leq \mu \left( \sum |x_r| \right)^2 \leq k\mu ||x||^2_2.$$
Many explicit constructions of vectors $u_1, \ldots, u_N$ satisfying

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

Explicit constructions of RIP matrices

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

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


**Corollary:** $\Phi$ with columns $\mathbf{u}_j$ satisfies RIP with $\delta = \frac{1}{3}$ and all

$$
k \leq \frac{c \sqrt{n \log n}}{\log N}.
$$
Explicit constructions of RIP matrices

Many explicit constructions of vectors $u_1, \ldots, u_N$ satisfying

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


**Corollary:** $\Phi$ with columns $u_j$ satisfies RIP with $\delta = \frac{1}{3}$ and all $k \leq \frac{c \sqrt{n \log n}}{\log N}$.

**Limitation:** (Levenshtein, 1983) For all $u_1, \ldots, u_N$,

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

With coherence, we cannot deduce RIP of order larger than $\sqrt{n}.$
Theorem (BDFKK, 2010)

For an effective constant $\alpha > 0$, large $n$ and $N^{1-\alpha} \leq n \leq N$, we give an explicit $n \times N$ RIP matrix of order $k = \lceil n^{1/2} + \alpha \rceil$ and constant $\delta = \frac{1}{3}$.
Breaking the $\sqrt{n}$ barrier with explicit constructions

Theorem (BDFKK, 2010)

For an effective constant $\alpha > 0$, large $n$ and $N^{1-\alpha} \leq n \leq N$, we give an explicit $n \times N$ RIP matrix of order $k = \lfloor n^{1/2} + \alpha \rfloor$ and constant $\delta = \frac{1}{3}$.

The construction: Take $s$ a large integer, $p$ a large prime, $\mathcal{A} = \{ 1, 2, \ldots, \lfloor p^{1/s} \rfloor \}$, $M = 2^{2s-1}$, $r = \left\lfloor \frac{\log p}{2s \log 2} \right\rfloor$, $\mathcal{B} = \left\{ \sum_{j=0}^{r-1} x_j (2M)^j : 0 \leq x_j \leq M - 1 \right\}$.

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

$N = |\mathcal{A}| \cdot |\mathcal{B}|$, $n = p$. 

Bourgain, Dilworth, Ford, Konyagin, Kutzarova

Explicit RIP matrices
Some ideas of the proof

Take $s$ a large integer, $p$ a large prime, 
$A = \{1, 2, \ldots, \lfloor p^{1/s} \rfloor \}$, 

$M = 2^{2s-1}$, $r = \left\lfloor \frac{\log p}{2s \log 2} \right\rfloor$, $B = \left\{ \sum_{j=0}^{r-1} x_j (2M)^j : 0 \leq x_j \leq M - 1 \right\}$.

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

$N = |A| \cdot |B|$, $n = p$.

(1) No “carries” when adding elements of $B$, thought of as base-$2M$ numbers.

(2) use Gauss sum formula to compute exactly $\langle u_{a,b}, u_{a',b'} \rangle$.

(3) results from additive combinatorics for subsets of $B$. 

Bourgain, Dilworth, Ford, Konyagin, Kutzarova
Turán’s power sums

For unit complex numbers $z_1, \ldots, z_n$, let

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

General problem: find $z$ to minimize $M_N(z)$. 
Turán’s power sums

For unit complex numbers $z_1, \ldots, z_n$, let

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

General problem: find $z$ to minimize $M_N(z)$.

Proposition

For unit complex numbers $z_1, \ldots, z_n$, the vectors

$$u_m = n^{-1/2}(z_1^{m-1}, \ldots, z_n^{m-1})^T, 1 \leq m \leq N,$$

have coherence

$$\mu = \frac{M_{N-1}(z)}{n}.$$
Explicit constructions for Turán’s power sums

**Andersson (2008).** Explicit $z$ with $M_N(z) = O\left(n^{1/2} \frac{\log N}{\log n}\right)$.
Andersson (2008). Explicit $z$ with $M_N(z) = O \left( n^{1/2} \frac{\log N}{\log n} \right)$.

**Theorem (BDFKK, 2010)**

We give explicit constructions of $z$ such that

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

**Remark.** Our constructions are better than Andersson’s constructions for $n \lesssim (\log N)^4$. 

Corollary. Explicit constructions of vectors $u_1, \ldots, u_N$ with

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

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

Explicit constructions for Turán’s power sums
Andersson (2008). Explicit $z$ with $M_N(z) = O \left( n^{1/2} \frac{\log N}{\log n} \right)$.

**Theorem (BDFKK, 2010)**

We give explicit constructions of $z$ such that

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

**Remark.** Our constructions are better than Andersson’s constructions for $n \lesssim (\log N)^4$.

**Corollary.** Explicit constructions of vectors $u_1, \ldots, u_N$ with

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

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 Szemeredi (1990). They were interested in constructing sets $T \subseteq \{1, \ldots, N\}$ such that all the Fourier coefficients

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

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

The analysis uses only very basic (undergraduate-level) number theory.