Explicit constructions of RIP matrices and related problems

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

August 2, 2010

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 k-sparse vectors $\mathbf{x}$, 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
- $\Phi\mathbf{x} \in \mathbb{C}^n$ is a lower dimensional linear measurement
- Candès, Romberg and Tao (2006) showed that given $\Phi\mathbf{x}$, one can effectively recover $\mathbf{x}$;
- 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).

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); Candès, Romberg, Tao (2006))

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

Remarks: Baraniuk, Davenport, DeVore and Wakin (2008) gave a proof using the Johnson-Lindenstrauss lemma.
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 Φ with maximal k (Alternatively, minimize n given N, k).

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

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

Remarks: Baraniuk, Davenport, DeVore and Wakin (2008) gave a proof using the Johnson-Lindenstrauss lemma.
Other random constructions given by Rudelson/Vershinin (2008), Mendelson, Pajor and Tomczak-Jaegermann (2007).

Theorem (Nelson and Temlyakov, 2010)

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

Coherence

Definition

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

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

Coherence

Definition

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

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

Sets of vectors with small coherence are spherical codes

Coherence

Definition

The *coherence* μ *of unit vectors* $\mathbf{u}_1, \ldots, \mathbf{u}_N \in \mathbb{C}^n$ *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 $\mathbf{u}_1, \ldots, \mathbf{u}_N$ *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* $k = \lfloor 1/(3\mu) \rfloor$ *and* $\delta = \frac{1}{3}$.

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

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

Explicit constructions of RIP matrices

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 (1977), Alon-Goldreich-Håstad-Peralta (1992), DeVore (2007), Andersson (2008), and Nelson-Temlyakov (2010).

Explicit constructions of RIP matrices

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

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

e.g. Kashin (1977), Alon-Goldreich-Håstad-Peralta (1992), DeVore (2007), Andersson (2008), and Nelson-Temlyakov (2010).

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

$$k \leqslant \frac{c\sqrt{n}\log n}{\log N}.$$

Explicit constructions of RIP matrices

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

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

e.g. Kashin (1977), Alon-Goldreich-Håstad-Peralta (1992), DeVore (2007), Andersson (2008), and Nelson-Temlyakov (2010).

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

$$k \leqslant \frac{c\sqrt{n} \log n}{\log N}.$$

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 $\sqrt{n}$.

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

Theorem (BDFKK, 2010)

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

The construction: Take s a large integer, p a large prime,
$\mathcal{A} = \left\{1, 2, \dots, \lfloor p^{1/s} \rfloor\right\}$,

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

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

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

Some ideas of the proof

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

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

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

---

(1) No "carries" when adding elements of $\mathcal{B}$, thought of as base-$2M$ numbers.

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

(3) results from additive combinatorics for subsets of $\mathcal{B}$.

Turán's power sums

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

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

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

Turán's power sums

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

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

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

Proposition

For unit complex numbers $z_1, \dots, z_n$, the vectors $\mathbf{u}_m = n^{-1/2}(z_1^{m-1}, \dots, z_n^{m-1})^T, 1 \leqslant m \leqslant N$, have coherence

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

Explicit constructions for Turán's power sums

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

Explicit constructions for Turán's power sums

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

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 $n \lesssim (\log N)^4$.

Explicit constructions for Turán's power sums

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

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 $n \lesssim (\log N)^4$.

Corollary. Explicit constructions of vectors $\mathbf{u}_1, \dots, \mathbf{u}_N$ 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

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

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

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