Square-root bottleneckを超えるRIP行列と関連する組合せ論

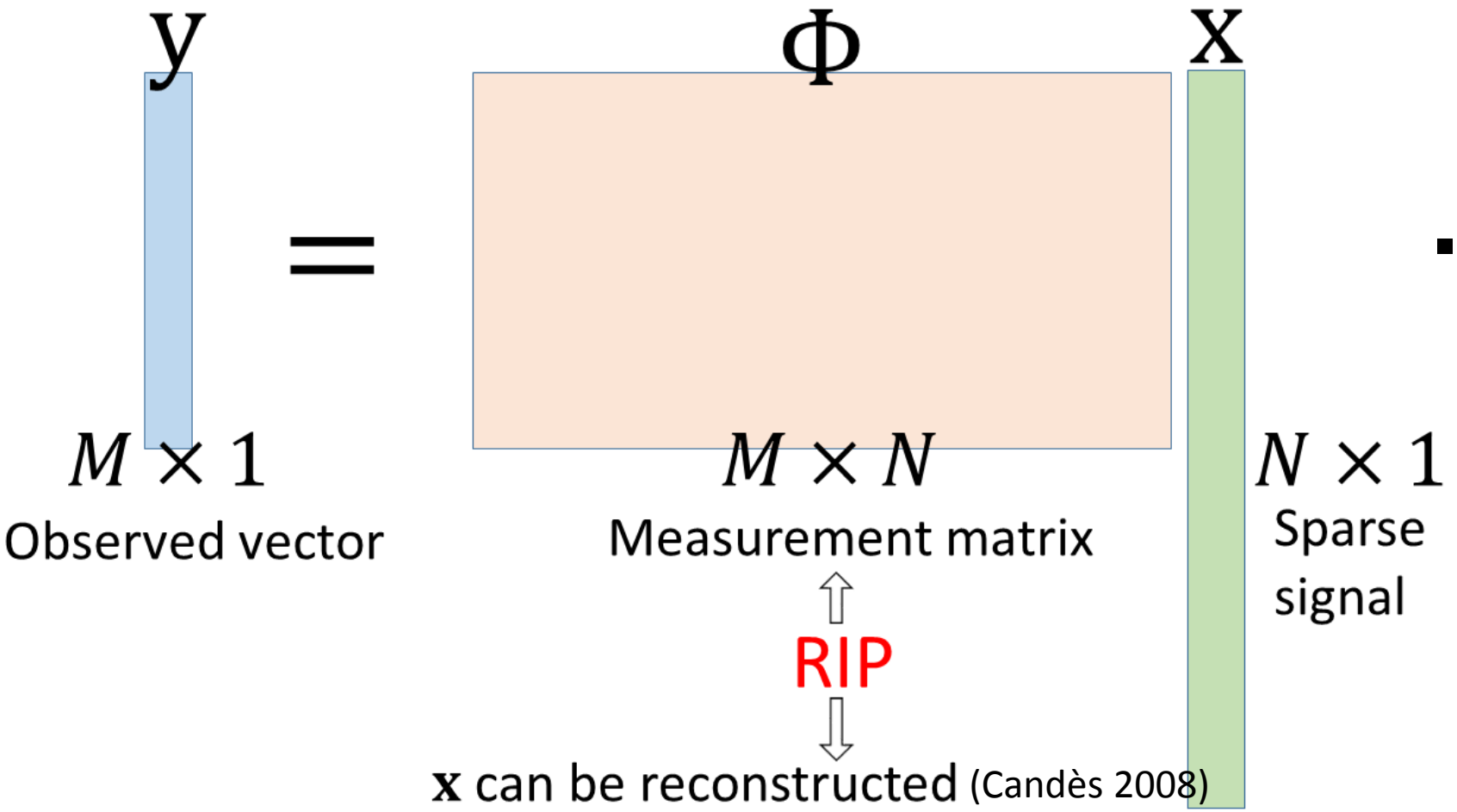
佐竹 翔平
熊本大学・日本学術振興会特別研究員PD

電子情報通信学会 7月情報理論研究会, 2021.07.08

1. Restricted Isometry Property(RIP)

Compressed sensing

- Reconstruction of sparse signals



$\cdot M \ll N$

RIP=**R**estricted **I**sometry **P**roperty

- Φ: $M \times N$ matrix ($M \leq N$),
- $K \leq M$,
- $\delta \in [0, 1)$.

$$\Phi \text{ has the } (K, \delta)\text{-RIP} \underset{\text{def}}{\Leftrightarrow} \begin{array}{l} \forall \mathbf{x}\text{: } K\text{-sparse (i.e. } |\mathrm{supp}(\mathbf{x})| \leq K), \\ (1-\delta)\|\mathbf{x}\|^2 \leq \|\Phi\mathbf{x}\|^2 \leq (1+\delta)\|\mathbf{x}\|^2. \end{array}$$

- $\delta_K = \delta_K(\Phi) := \min\{\delta \in [0, 1) \mid \Phi\text{: } (K, \delta)\text{- RIP}\}$.

Remark:

- It suffices to certify RIP for some $\delta < \sqrt{2} - 1$ (Candès 2008).
- If the (j, k)-element$= b + ci$ ($b, c \in \mathbb{R}$), construct a $2M \times 2N$ real matrix by replacing it by $\begin{bmatrix} b & c \\ -c & b \end{bmatrix}$.

Then Φ has the (K, δ)-RIP $\Rightarrow$ Φ' also has the (K, δ)-RIP.

Constructing RIP matrix

■ $M \times N$ random matrix:

- Each entry $\sim$ Bernoulli distribution $\Rightarrow$ (K, δ)-RIP with $K = \Theta\left(\delta \frac{M}{\log\left(\frac{2N}{M}\right)}\right)$ w.h.p.
- Certifying RIP for a given matrix is NP-hard (Bandeira-Dobriban-Mixon-Sawin 2013).

■ Deterministic construction:

(e.g. T. Tao's weblog: "Open question: deterministic UUP matrices")

- DeVore (2007) - algebraic curves over finite fields,
- Li-Ge (2014): - orthogonal vector systems (e.g. ETF, MUB…),
- S.-Gu (2020) -algebraic expander graphs…

Coherence, RIP & Main problem

- $\Phi = (\boldsymbol{c}_1 \ \boldsymbol{c}_2 \ \cdots \ \boldsymbol{c}_N) \ (\boldsymbol{c}_i \in \mathbb{C}^M, \ \|\boldsymbol{c}_i\| = 1.)$

  Coherence of Φ: $\mu(\Phi) \coloneqq \max_{1 \le i \ne j \le N} |\langle \boldsymbol{c}_i, \boldsymbol{c}_j \rangle|$.

- $\mu(\Phi) = \mu \ \Rightarrow$ For each $K \le M$, Φ has the $\big(K, \mu(K-1)\big)$-RIP.

  $\Rightarrow \mu(K-1) < 1$ i.e. $K < \mu^{-1} + 1$.

  Remark: $\delta_K \le (K-1)\mu$.

- $\mu(\Phi) \ge \sqrt{\frac{N-M}{M(N-1)}}$ (Welch bound) $\Rightarrow$ this certifies RIP only for $K = O\big(\sqrt{M}\big)$.

  Square-root bottleneck

Problem	Give deterministic constructions of $M \times N$ matrices satisfying the (K, δ)-RIP with $K = \Omega(M^\gamma)$ $(\gamma > \frac{1}{2})$, $\delta \in \big[0, \sqrt{2} - 1\big)$.

Known (unconditional) constructions

	M	N	K	Comments
Bourgain-Dilworth-Ford-Konyagin-Kutzarova (2011)	$M \gg 0$	$N \leq M^{\gamma_1}$	$\lfloor M^{\frac{1}{2}+\gamma_1'} \rfloor$	$\gamma_1 \fallingdotseq 5.5169 \times 10^{-28}$, $\forall \gamma'_1 < \gamma_1$
Mixon (2015)	$p \gg 0$: prime	$\Omega(p^{1+\eta})$	$\Omega\left(p^{1/2+\gamma_2'}\right)$	Some $\eta > 0$, $\gamma_2 \fallingdotseq 4.4466 \times 10^{-24}$, $\forall \gamma'_2 < \gamma_2$

Remark:

$M \times N$ random matrices have (K, δ)-RIP with $K = \Theta\left(\delta \frac{M}{\log\left(\frac{2N}{M}\right)}\right)$ w.h.p.

2. RIP matrix from quadratic residues
- Renes-Zauner ETF -

Renes-Zauner ETF (Zauner 1999, Renes 2007)

- p: odd prime,
- $r = 0\ (1)$ if $p \equiv 1\ (3) \bmod 4$,
- $\mathbb{Z}/p\mathbb{Z} = \{a_1, \dots, a_p\}$,
- $b_1, \dots, b_{\frac{p-1}{2}}$: quadratic residues ($\underset{\text{def}}{\Leftrightarrow} \exists x \neq 0$ s.t. $x^2 \equiv b_j \bmod p$).

$$\Phi_p := \underbrace{\begin{pmatrix} \frac{1}{\sqrt{p}} & \cdots & \frac{1}{\sqrt{p}} & i^r \\ \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_1 a_1\right) & \cdots & \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_1 a_p\right) & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_{\frac{p-1}{2}} a_1\right) & \cdots & \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_{\frac{p-1}{2}} a_p\right) & 0 \end{pmatrix}}_{p+1 \text{ columns}} \Bigg\} \frac{p+1}{2} \text{ rows}$$

Renes-Zauner ETF (Zauner 1999, Renes 2007)

- p: odd prime,
- $r = 0\ (1)$ if $p \equiv 1\ (3) \bmod 4$,
- $\mathbb{Z}/p\mathbb{Z} = \{a_1, \dots, a_p\}$,
- $b_1, \dots, b_{\frac{p-1}{2}}$: quadratic residues ($\underset{\text{def}}{\Leftrightarrow} \exists x \neq 0$ s.t. $x^2 \equiv b_j \bmod p$).

$$\Phi_p := \underbrace{\begin{pmatrix} \frac{1}{\sqrt{p}} & \cdots & \frac{1}{\sqrt{p}} & i^r \\ \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_1 a_1\right) & \cdots & \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_1 a_p\right) & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_{\frac{p-1}{2}} a_1\right) & \cdots & \sqrt{\frac{2}{p}} \exp\left(\frac{2\pi i}{p} b_{\frac{p-1}{2}} a_p\right) & 0 \end{pmatrix}}_{p+1 \text{ columns}} \Bigg\} \frac{p+1}{2} \text{ rows}$$

Conjecture (Bandeira-Fickus-Mixon-Wong 2013)

For every sufficiently large p, Φ_p has the $\left(\Theta\left(\frac{p}{\log^{\alpha} p}\right), \delta\right)$-RIP for some $\alpha > 0$ and $\delta < \sqrt{2} - 1$.

Main result 1

Notation: $\left(\frac{x}{p}\right) := \begin{cases} 0 & x = 0; \\ 1 & x: \text{QR}; \\ -1 & x: \text{otherwise.} \end{cases}$

Theorem (Bandeira-Mixon-Moreira 2017)

For sufficiently large $p \equiv 1 \bmod 4$, 一 $\Rightarrow$ 二 holds.

一. $\forall \alpha \in \left(0, \frac{1}{2}\right), \exists \beta_1 = \beta_1(\alpha) > 0$ s.t.

$\forall S \subset \mathbb{Z}/p\mathbb{Z}$ with $|S| > p^{\alpha}$,

$$\left| \sum_{s_1, s_2 \in S} \left(\frac{s_1 - s_2}{p}\right) \right| \leq |S|^{2-\beta_1}.$$

Conjecture (Chung 1994)

Remark: $p \equiv 3 \bmod 4 \Rightarrow \forall S, \sum_{s_1, s_2 \in S} \left(\frac{s_1 - s_2}{p}\right) = 0$!

二. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.

Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

$K = p^{\gamma} \gg \sqrt{M}!$

Remark: Φ_p: $\left(\frac{p+1}{2}\right) \times (p+1)$ matrix.

Main result 1

Notation: $\left(\frac{x}{p}\right) := \begin{cases} 0 & x = 0; \\ 1 & x: \text{QR}; \\ -1 & x: \text{otherwise}. \end{cases}$

Theorem (Bandeira-Mixon-Moreira 2017)

For sufficiently large $p \equiv 1 \bmod 4$, 一 $\Rightarrow$ 二 holds.

一. $\forall \alpha \in \left(0, \frac{1}{2}\right), \exists \beta_1 = \beta_1(\alpha) > 0$ s.t.
$\forall S \subset \mathbb{Z}/p\mathbb{Z}$ with $|S| > p^{\alpha}$,

$$\left| \sum_{s_1, s_2 \in S} \left(\frac{s_1 - s_2}{p}\right) \right| \leq |S|^{2-\beta_1}.$$

Conjecture (Chung 1994)

Remark: $p \equiv 3 \bmod 4 \Rightarrow \forall S, \sum_{s_1, s_2 \in S} \left(\frac{s_1 - s_2}{p}\right) = 0$!

二. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.
Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

Theorem (S. 2020+)

For sufficiently large p, 1 $\Rightarrow$ 2 holds.

1. $\forall \alpha \in \left(0, \frac{1}{2}\right), \exists \beta = \beta(\alpha) > 0$ s.t.
$\forall S, T \subset \mathbb{Z}/p\mathbb{Z}$ with $|S|, |T| > p^{\alpha}$,

$$\left| \sum_{s \in S,\, t \in T} \left(\frac{s - t}{p}\right) \right| \leq p^{-\beta} |S||T|.$$

The Paley graph conjecture

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.
Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

$K = p^{\gamma} \gg \sqrt{M}!$

Remark: Φ_p: $\left(\frac{p+1}{2}\right) \times (p+1)$ matrix.

Sketch of proof

Notation: $\left(\frac{x}{p}\right) \coloneqq \begin{cases} 0 & x = 0; \\ 1 & x\text{: QR}; \\ -1 & x\text{: otherwise.} \end{cases}$

Theorem (S. 2020+ reproduced)

For sufficiently large p, 1 ⇒ 2 holds.

1. $\forall \alpha \in \left(0, \frac{1}{2}\right), \exists \beta = \beta(\alpha) > 0$ s.t. $\forall S, T \subset \mathbb{Z}/p\mathbb{Z}$ with $|S|, |T| > p^{\alpha}$,

$$\left| \sum_{s \in S,\, t \in T} \left(\frac{s-t}{p}\right) \right| \leq p^{-\beta} |S||T|.$$

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t. Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

Definition (Flat RIP)

- ϕ_s: the s-th column of Φ_p

Φ_p has the $\left(p^{\gamma},\ p^{\tau-\frac{1}{2}}\right)$-flat RIP

$$\Updownarrow \text{def}$$

$\forall S, T \subset \{1, 2, \ldots, p+1\}$ s. t. $S \cap T = \emptyset,\ |S|, |T| \leq p^{\gamma}$,

$$\left| \sum_{s \in S,\, t \in T} \langle \phi_s, \phi_t \rangle \right| \leq p^{\tau - \frac{1}{2}} \sqrt{|S||T|}.$$

Lemma

$$\left| \sum_{s \in S, t \in T} \langle \phi_s, \phi_t \rangle \right| \leq \max \left\{ \frac{\left| \sum_{s \in S, t \in T} \left(\frac{s-t}{p}\right) \right|}{\sqrt{p}}, \frac{|T|}{\sqrt{p}} \right\}.$$

Lemma Condition 1.

$$\Downarrow$$

$\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.

Φ_p has the $\left(p^{\gamma},\ p^{\tau-\frac{1}{2}}\right)$-flat RIP.

Lemma (Bandeira et.al. 2013)

$\left(p^{\gamma}, p^{\tau-\frac{1}{2}}\right)$ –flat RIP

$$\Downarrow$$

$\left(p^{\gamma}, 150\, p^{\tau-\frac{1}{2}} \log(p^{\gamma})\right)$ –RIP.

$$\Downarrow$$

$\left(p^{\gamma},\ p^{\tau-\frac{1}{2}+o(1)}\right)$ -RIP.

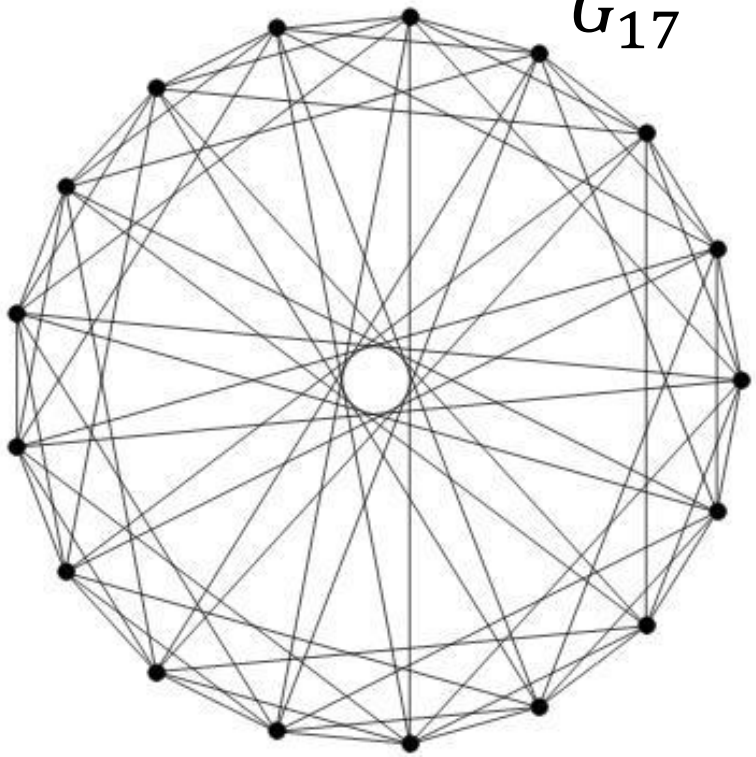
3. RIP $\Rightarrow$ Ramsey

Paley graph/tournament

G_p: the Paley graph with p vertices
($p \equiv 1 \bmod 4$: prime)

- Vertex set: $\mathbb{Z}/p\mathbb{Z}$,
- $x \sim y \underset{\text{def}}{\Leftrightarrow} \left(\frac{x-y}{p}\right) = 1.$

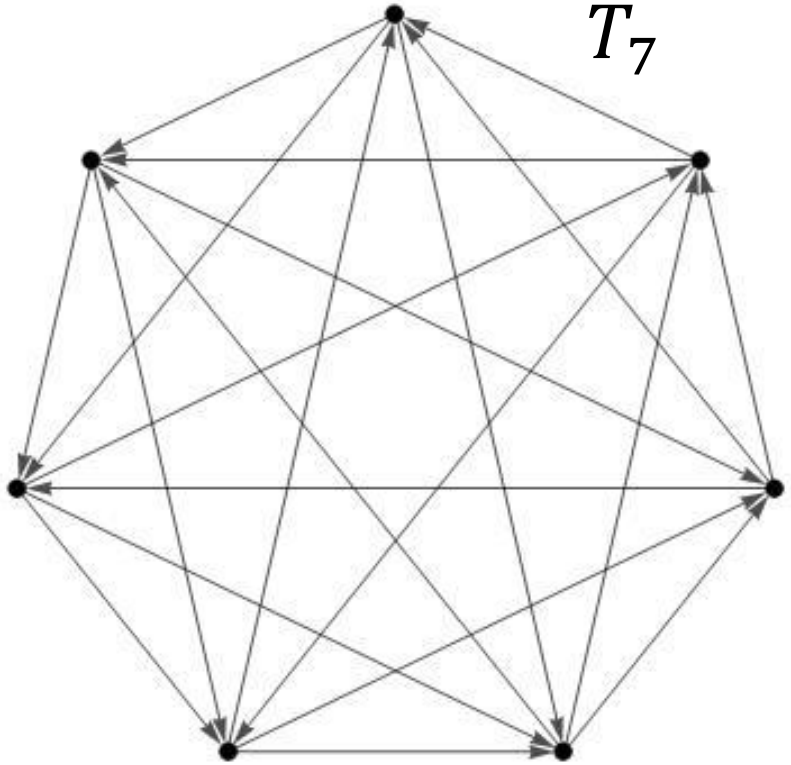
G_{17}



T_p: the Paley tournament with p vertices
($p \equiv 3 \bmod 4$: prime)

- Vertex set: $\mathbb{Z}/p\mathbb{Z}$,
- $x \longrightarrow y \underset{\text{def}}{\Leftrightarrow} \left(\frac{x-y}{p}\right) = 1.$

T_7



Paley graph/tournament

Remark: A transitive tournament is a tournament with no directed cycles.

G_p: the Paley graph with p vertices
($p \equiv 1 \bmod 4$: prime)

- Vertex set: $\mathbb{Z}/p\mathbb{Z}$,
- $x \sim y \underset{\text{def}}{\Leftrightarrow} \left(\frac{x-y}{p}\right) = 1.$

Conjecture (e.g. Croot-Lev 2007)
The maximal size of complete subgraphs (clique) in G_p is $o(\sqrt{p})$.

- $\leq \sqrt{p}$ (well-known)
- $\leq \sqrt{p} - 1$ (Bachoc-Ruzsa-Matolcsi 2013)
- $\leq \sqrt{\frac{p}{2}} + 1$ (Hanson-Petridis 2020)

T_p: the Paley tournament with p vertices
($p \equiv 3 \bmod 4$: prime)

- Vertex set: $\mathbb{Z}/p\mathbb{Z}$,
- $x \longrightarrow y \underset{\text{def}}{\Leftrightarrow} \left(\frac{x-y}{p}\right) = 1.$

Conjecture (e.g. Sanchez-Flores 1998)
The maximal size of transitive subtournaments in T_p is $o(\sqrt{p})$.

- $\leq \frac{-3+\sqrt{13+12p}}{2}$ (Tabib 1986)
- $\leq -2 + \left\lfloor \sqrt{3p+4} \right\rfloor$ for some p (Momihara-Suda 2017)
- $\leq 1 + \sqrt{2p-1}$ (S. 2020+)

Ramsey theory

Remark: A transitive tournament is a tournament with no directed cycles.

Ramsey number:

$R(k) := \max\{n \in \mathbb{N} \mid \exists G: \text{graph with } n \text{ vtx. s.t. the max. size of cliq./cocliq.} \leq k\}$.

- $\forall k \geq 1, R(k) < \infty$ (Ramsey 1930)
- Explicit construction of graphs providing good lower bounds on $R(k)$ (Ramsey graph)?

  i.e. Graphs without large cliq./cocliq.

Conjecture

Paley graphs are Ramsey graphs.

Oriented Ramsey number:

$\vec{R}(k) := \max\{n \in \mathbb{N} \mid \exists T: \text{tournament with } n \text{ vtx. s.t. the max. size of transitive subtournaments} \leq k\}$.

- $\forall k \geq 1, \vec{R}(k) < \infty$ (Erdős-Moser 1964)
- Explicit construction of tournaments providing good lower bounds on $\vec{R}(k)$ (Ramsey tournament)?

  i.e. Tournaments without large transitive subtournaments.

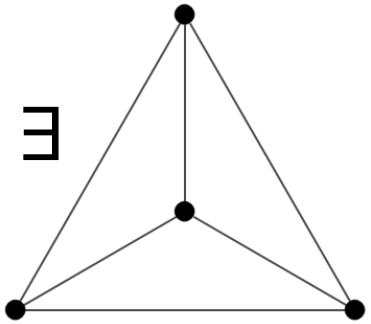
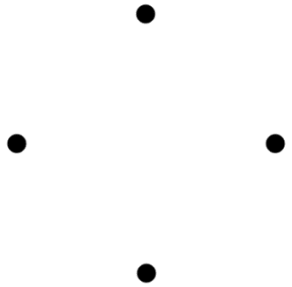
Conjecture

Paley tournaments are Ramsey tournaments.

Ramsey theory

Graphs

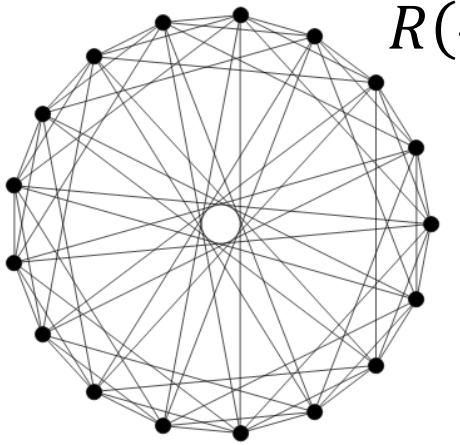
vertices

∃  or 

$R(4) = 18$

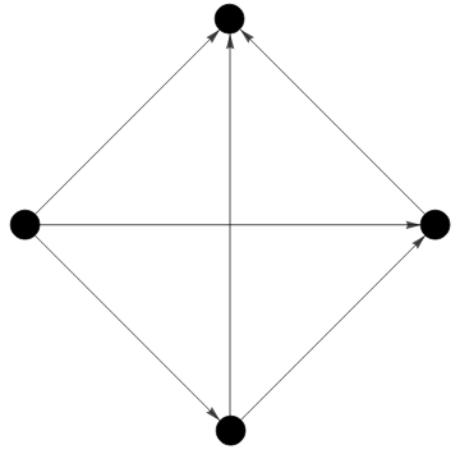
Paley graph with 17 vtx.

$R(4) > 17$



Tournaments

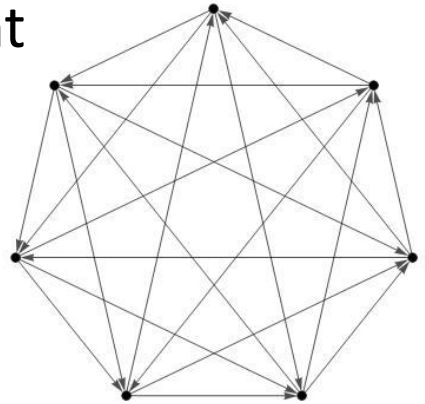
vertices

∃ 

$\vec{R}(4) = 8$

Paley tournament with 7 vtx.

$\vec{R}(4) > 7$



Main result 2

Theorem (Bandeira-Mixon-Moreira 2017)

For sufficiently large $p \equiv 1 \bmod 4$, 二 $\Rightarrow$ 三 holds.

二. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.

Φ_p has the $\left(p^{\gamma},\ p^{\tau-\frac{1}{2}+o(1)}\right)$-RIP.

三. The maximal size of cliques in G_p is $o\left(\sqrt{p}\right)$

Main result 2

Theorem (Bandeira-Mixon-Moreira 2017)

For sufficiently large $p \equiv 1 \bmod 4$, 二 ⇒ 三 holds.

二. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.

Φ_p has the $\left(p^{\gamma},\ p^{\tau-\frac{1}{2}+o(1)}\right)$-RIP.

三. The maximal size of cliques in G_p is $o\left(\sqrt{p}\right)$

Theorem (S. 2020+)

For sufficiently large $p \equiv 3 \bmod 4$, 2 ⇒ 3 holds.

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t.

Φ_p has the $\left(p^{\gamma},\ p^{\tau-\frac{1}{2}+o(1)}\right)$-RIP.

3. The maximal size of transitive subtournaments in T_p is $o\left(\sqrt{p}\right)$.

Sketch of proof

Theorem (S. 2020+ reproduced)

For sufficiently large $p \equiv 3 \bmod 4$, 2 ⇒ 3 holds.

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t. Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

3. The maximal size of transitive subtournaments in T_p is $o\left(\sqrt{p}\right)$.

Lemma

- U: vertex set of a transitive subtournament in T_p,
- ϕ_s: the s-th column of Φ_p,
- $\Phi_U := (\phi_u)_{u \in U}$: $\frac{p+1}{2} \times |U|$ matrix.

$$\left(\Phi_U^T \overline{\Phi_U}\right)_{u_1, u_2 \in U} = \begin{cases} \frac{i}{\sqrt{p}} \cdot \left(\frac{u_1 - u_2}{p}\right) & u_1 \neq u_2; \\ 1 & u_1 = u_2. \end{cases}$$

Thus $\Phi_U^T \overline{\Phi_U} = \frac{1}{\sqrt{p}} \begin{bmatrix} 1 & & i \\ & \ddots & \\ -i & & 1 \end{bmatrix}$.

Remark: Hermitian ⇒ all eigenvalues are real.

Lemma

- $\left(\text{largest eigenvalue of } \Phi_U^T \overline{\Phi_U}\right) \geq 1 + \sqrt{\frac{|U|^2 - 1}{3p}}$,
- $\left(\text{smallest eigenvalue of } \Phi_U^T \overline{\Phi_U}\right) \leq 1 - \sqrt{\frac{|U|^2 - 1}{3p}}$.

Lemma

Condition 2. ⇒ $\forall \lambda$: eigenvalue of $\Phi_U^T \overline{\Phi_U}$, $1 - \delta \leq \lambda \leq 1 + \delta$.

$(\delta = p^{\tau - \frac{1}{2} + o(1)})$

Remark: $|U| = O\left(\sqrt{p}\right) \ll K$.

cf. Tabib (1986)

⇨ $|U| \leq \delta \sqrt{3p} + 1$.

4. RIP ⇒ Pseudo-randomness

Pseudo-randomness of quadratic residues

Conjecture (cf. Mrazović 2016)

For every pair of $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with $|X|, |Y| \geq \log^C p$ for some $C > 0$,

$$\left| \#\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : x - y \text{ is a QR}\} - \frac{1}{2}|X||Y| \right| = o(|X||Y|) \quad \cdots \quad (*)$$

Pseudo-randomness of quadratic residues

Conjecture (cf. Mrazović 2016)

For every pair of $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with $|X|, |Y| \geq \log^C p$ for some $C > 0$,

$$\left| \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : x - y \text{ is a QR}\} - \frac{1}{2}|X||Y| \right| = o(|X||Y|) \quad \cdots \quad (*)$$

Remark:

- This conjecture implies that a function $f\colon (\mathbb{Z}/p\mathbb{Z})^2 \to \{0,1\}$ with $f(x,y) = \begin{cases} 1 & x-y \text{ is a QR;} \\ 0 & \text{otherwise,} \end{cases}$ is a good *randomness extractor* (Chor-Goldreich 1988).

- But the current technique can prove $(*)$ only for the case that $|X||Y| > p$.

Pseudo-randomness of quadratic residues

Conjecture (cf. Mrazović 2016)

For every pair of $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with $|X|, |Y| \geq \log^C p$ for some $C > 0$,

$$\left| \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : x - y \text{ is a QR}\} - \frac{1}{2}|X||Y| \right| = o(|X||Y|) \quad \cdots \quad (*)$$

Remark:

- This conjecture implies that a function $f\colon (\mathbb{Z}/p\mathbb{Z})^2 \to \{0,1\}$ with $f(x,y) = \begin{cases} 1 & x-y \text{ is a QR;} \\ 0 & \text{otherwise,} \end{cases}$ is a good *randomness extractor* (Chor-Goldreich 1988).

- But the current technique can prove $(*)$ only for the case that $|X||Y| > p$.

Theorem (S. 2021+)

Suppose $p \equiv 1 \bmod 4$. Then 2. (in main result 1) ⇒ 3. holds.

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t. Φ_p has the $\left(p^\gamma,\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

3. We have $(*)$ for any pair of disjoint $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with
   - $|Y| = \Omega\left(p^{\tau + o(1)}\right)$;
   - $\Omega\left(\sqrt{|Y|} \cdot p^{\frac{\tau}{2} + o(1)}\right) = |X| \leq |Y|$.

Pseudo-randomness of quadratic residues

Conjecture (cf. Mrazović 2016)

For every pair of $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with $|X|, |Y| \geq \log^C p$ for some $C > 0$,

$$\left| \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : x - y \text{ is a QR}\} - \frac{1}{2}|X||Y| \right| = o(|X||Y|) \quad \cdots \quad (*)$$

Remark:

- This conjecture implies that a function $f\colon (\mathbb{Z}/p\mathbb{Z})^2 \to \{0,1\}$ with $f(x,y) = \begin{cases} 1 & x-y \text{ is a QR;} \\ 0 & \text{otherwise,} \end{cases}$ is a good *randomness extractor* (Chor-Goldreich 1988).

- But the current technique can prove $(*)$ only for the case that $|X||Y| > p$.

Theorem (S. 2021+)

Suppose $p \equiv 1 \bmod 4$. Then 2. (in main result 1) $\Rightarrow$ 3. holds.

2. $\exists \gamma > \frac{1}{2}$ $\exists \tau \in \left(0, \frac{1}{2}\right)$ s.t. Φ_p has the $\left(p^{\gamma},\ p^{\tau - \frac{1}{2} + o(1)}\right)$-RIP.

3. We have $(*)$ for any pair of disjoint $X, Y \subset \mathbb{Z}/p\mathbb{Z}$ with
   - $|Y| = \Omega\left(p^{\tau + o(1)}\right)$;
   - $\Omega\left(\sqrt{|Y|} \cdot p^{\frac{\tau}{2} + o(1)}\right) = |X| \leq |Y|$.

∗ Thm. works for $|X||Y| = o(p)$!

Summary & Future works

Problem Give deterministic constructions of $M \times N$ matrices satisfying the (K, δ)-RIP with $K = \Omega(M^{\gamma})$ ($\gamma > \frac{1}{2}$), $\delta \in \left[0, \sqrt{2} - 1\right)$.

Conditional constructions:

- Bandeira-Mixon-Moreira (2017)
- S. (2020 THIS TALK)

} RIP of Renes-Zauner ETF $\Rightarrow$ {

- Ramsey graphs/tournaments
- Pseudo-randomness / extractors

Summary & Future works

Problem Give deterministic constructions of $M \times N$ matrices satisfying the (K, δ)-RIP with $K = \Omega(M^{\gamma})$ ($\gamma > \frac{1}{2}$), $\delta \in \left[0, \sqrt{2} - 1\right)$.

Conditional constructions:

- Bandeira-Mixon-Moreira (2017)
- S. (2020 THIS TALK)

$\Rightarrow$ RIP of Renes-Zauner ETF $\Rightarrow$

- Ramsey graphs/tournaments
- Pseudo-randomness / extractors

Related work: S.-Gu (ITW2020): a generalization of Paley matrix.

Summary & Future works

Problem Give deterministic constructions of $M \times N$ matrices satisfying the (K, δ)-RIP with $K = \Omega(M^{\gamma})$ $(\gamma > \frac{1}{2})$, $\delta \in [0, \sqrt{2} - 1)$.

Conditional constructions:

- Bandeira-Mixon-Moreira (2017)
- S. (2020 THIS TALK)

$\Rightarrow$ RIP of Renes-Zauner ETF $\Rightarrow$

- Ramsey graphs/tournaments
- Pseudo-randomness / extractors

Related work: S.-Gu (ITW2020): a generalization of the Renes-Zauner ETF.

Future works:

- Confirm the following conjecture.

> Conjecture (Bandeira-Fickus-Mixon-Wong 2013, reproduced)
> For sufficiently large p, Φ_p has the $\left(\Theta\left(\frac{p}{\log^{\alpha} p}\right), \delta\right)$-RIP for some $\alpha > 0$ and $\delta < \sqrt{2} - 1$.

- Other implication to combinatorics and information theory?

References

- A. S. Bandeira, M. Fickus, D. G. Mixon, P. Wong, The road to deterministic matrices with the restricted isometry property, *J. Fourier Anal. Appl.* **19** (2013), 1123–1149.
- A. S. Bandeira, D. G. Mixon, J. Moreira, A conditional construction of restricted isometries, *Int. Math. Res. Not.* **2017** (2017), 372–381.
- J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit constructions of RIP matrices and related problems, *Duke Math. J.* **159** (2011), 145–185. (See also their paper in *STOC2011*).
- B. Chor, O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, *SIAM J. Comput.* **17** (1988), 230–261.
- R. Mrazović, Extractors in Paley graphs: a random model, *European J. Combin.* **54** (2016), 154–162.
- S. Satake, On the restricted isometry property of the Paley matrix, arXiv:2011.02907.
- S. Satake, Y. Gu, On compressed sensing matrices breaking the square-root bottleneck, Proceedings of IEEE Information Theory Workshop 2020 (ITW2020), arXiv:2010.11179.

✉ shohei-satake@kumamoto-u.ac.jp