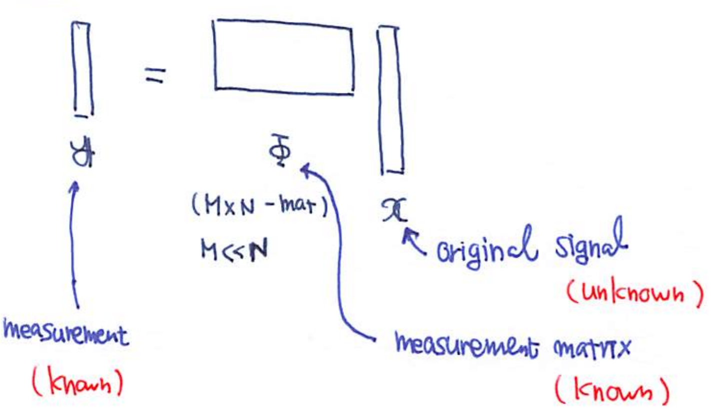
「RIP matrices, Ramsey graphs and randomness extractors」 佐竹さん

§1 RIP matrices ⟵ "Compressed Sensing"

§2 Ramsey graphs

§3 Randomness extractors

§1



想定としては $K<N$ である.

- x : K-sparce ($\overset{def}{\iff} |\mathrm{Supp}(x)| \leq K$)
- Φ : (K,δ)-RIP ($\delta \in (0, \sqrt{2}-1)$)

$\Longrightarrow$ x can be uniquely recovered by y, Φ (Candés '08)

Definition

- $K \leq M \ll N$: positive integers
- $\delta \in (0,1)$

$\Phi \in \mathrm{Mat}(M,N,\mathbb{C})$ が (K,δ)-$\underline{\underline{\mathrm{RIP}}}$ $\overset{def}{\iff}$, $\forall x \in \mathbb{C}^N$: K-sparse,

(ristricted isometry property)

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

where $\|\cdot\|_2$: l_2-Norm

Problem

Construct matrices having (K,δ)-RIP

- $K = O\left(\frac{M}{\log(\frac{N}{M})}\right)$ のとき, $\underbrace{\exists \Phi}_{\forall \delta \in (0,1),}$: $M\times N$-matrix (s.t.) (K,δ)-RIP (s.t.) $K = C_\delta \frac{M}{\log(\frac{N}{M})}$

- Random matrix.

$\Phi = (\phi_{ij})_{\substack{1\leq i \leq M \\ 1 \leq j \leq N}}$ (s.t.) $\phi_{ij} \sim N(0, \frac{1}{M})$

or

$$\phi_{ij} = \begin{cases} \frac{1}{\sqrt{M}} & \text{w./ prob} = \frac{1}{2} \\ -\frac{1}{\sqrt{M}} & \text{w./ prob} = \frac{1}{2} \end{cases}$$

$\rightsquigarrow$ Φ has the (K, δ)-RIP w/ $K = C_\delta \dfrac{M}{\log\left(\frac{N}{M}\right)}$ for any δ w.h.p.

Issue (theorical)

- Checking RIP for a given matrix is NP-hard (worst/average)
- Random watnices spend large space complexi.

$\rightsquigarrow$ Open problem

Construct determistic RIP matrices

§2

- $n, q \geq 2$: integers
- K_n : complere graph with n-vertices.
- Clique : complete subgraph

An edge-colored K_n by q_n-colors is $(m:q)$-Ramsey

$\overset{\text{def}}{\Longleftrightarrow}$ for any color, the corresponding monochromatic clique has size at most m

Example

$\exists (3,2)$-Ramsey graph $\leftarrow$ Paley graphs

- For $q \geq 2$, random coloring of K_n yields $(\underbrace{O(\log n)}_{\text{best possible}}, q)$-Ramsey graphs w.h.p.

- ~~Checking Ramsey~~ Finding clique is NP-complete

Open problem

How to construct nice determistic Ramsey graphs

(m, q)-Ramsey s.t. $m = O(\text{poly} \log(n))$

State of the art : $\forall c > 1$, $\exists (O(\log^c n); 2)$ - Ramsey graph (Li, '20)
($q=2$)

Theorem [Gamarnik '19]

A certain RIP matrix yields nice Ramsey graphs for $q = 3$
$m = O(\mathrm{poly}\log n)$ # colors

- Φ : $M \times N$ matrix (real)
- ϕ_j : j-th column of Φ, $\|\phi_j\| = 1$
- G_Φ : edged - colored K_n (s.t.) $\begin{cases} \cdot \text{ vertex set } = \{1, 2, \cdots, n\} \\ \cdot \; i < j \\ \quad \begin{cases} \{i, j\} : \text{green} & \text{if } |\langle \phi_i, \phi_j \rangle| \le \frac{1}{2\sqrt{M}} \\ \{i, j\} : \text{red} & \text{if } \langle \phi_i, \phi_j \rangle > \frac{1}{2\sqrt{M}} \\ \{i, j\} : \text{blue} & \text{otherwise} \end{cases} \end{cases}$

⇝ **Theorem** [Gamarnik]

Φ has (K, δ) - RIP (s.t.) $K \ge 2\sqrt{M} + 1$, $\delta \in (0, 1)$

$\Rightarrow \begin{cases} \cdot \text{ green clique of } G_\Phi \text{ has size at most } 2M \longleftarrow \text{Levenstein bound} \\ \cdot \text{ red / blue clique of } G_\Phi \text{ has size at most } 2\sqrt{M} + 1 \longleftarrow \text{RIP} \end{cases}$

Corollary

$\Phi : (K, \delta)$ - RIP (s.t.) $K \ge 2\sqrt{M} + 1$, $\delta \in (0, 1)$, $M = \mathrm{poly}\log(n)$

$\Rightarrow$ G_Φ : nice Ramsey .

Proof

· green : $\forall \{\psi_1, \dots, \psi_{2M}\} \subseteq \mathbb{R}^M$ $(\|\psi_i\| = 1)$

$$\Rightarrow \max_{i \neq j} |\langle \psi_i, \psi_j \rangle| > \frac{1}{2\sqrt{M}} \quad \text{(Levenstein's bound)}.$$

· red : C: red clique $(C \subsetneq \{1, 2, \dots, n\})$

$\mathbb{1}_C \in \mathbb{R}^n$: indicator of C

$\hat{\mathbb{1}}_C := \frac{1}{\sqrt{|C|}} \mathbb{1}_C$

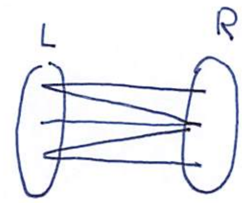
If $(K \geq)\ |C| > 2\sqrt{M} + 1$, $\hat{\mathbb{1}}_C$: K-sparse

$$\|\Phi \hat{\mathbb{1}}_C\|_2^2 - \|\hat{\mathbb{1}}_C\|_2^2 = \frac{1}{|C|} \sum_{\substack{i,j \in C \\ i \neq j}} \langle \phi_i, \phi_j \rangle = \frac{|C|-1}{2\sqrt{M}} > 1.$$

§3

Definition

$G = (L \sqcup R, E)$ を 2部グラフで $|L| = |R| = N$ とする.



G : (k, ε)-extractor

$\overset{\text{def}}{\Longleftrightarrow}$ $\forall S \subseteq L$, $\forall T \subseteq R$ (s.t.) $|S|, |T| > 2^k$

$$\left| \frac{e_G(S,T)}{|S||T|} - \boxed{\frac{1}{2}} \right| < \varepsilon.$$

$\mathbb{E}\left[\frac{e_H(S,T)}{|S||T|}\right]$, $H \sim G(L \sqcup R, \frac{1}{2})$

random bipartite graph each edge is chosen w/ prob $\frac{1}{2}$.

$e_G(S,T)$ = # of edges between S & T.

Problem

Find explicit extractors.

Definition

$p \equiv 1 \mod 4$, prime.

$G_p = (L \sqcup R, E)$: bipertite graph (s.t.)
$$\begin{cases} L, R = \mathbb{F}_p \\ E = \{(l, r) \in L \times R \mid \left(\frac{l-r}{p}\right) = 1\}, \\ \text{where } \left(\frac{\cdot}{p}\right) : \text{Legendre symbol.} \end{cases}$$

Conjecture [Cho-Goldreich '88]

$\forall d > 0$, G_p is a $(d \log_2 P, \varepsilon)$ extractor where ε is negligible (w.r.t. $\log_2 P$)

Theorem [S, ITW'24]

$\exists \Phi_p$: Paley matrix has $\left(\frac{P}{\mathrm{poly}\log P}, \delta\right)$-RIP $\Longrightarrow$ CG-conjecture is true

for some $C_\delta > 0$

Paley RIP conjecture

- Φ_p : $\left(\frac{p+1}{2}\right) \times (p+1)$-matrix is constructed as follows.

- $$\mathrm{DFT}_p = \frac{1}{\sqrt{p}} \begin{array}{c} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & & & w^{p-1} \\ 1 & w^2 & \ddots & & w^{2(p-1)} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & w^{p-1} & \cdots & & w^{(p-1)^2} \end{bmatrix} \end{array} \begin{array}{l} \text{0th} \\ \text{1st} \\ \text{2nd} \\ \vdots \\ \text{p-1st} \end{array} \qquad w := \exp\left(-\frac{2\pi\sqrt{-1}}{p}\right)$$

- Select j-th row of DFT_p (s.t.) $\left(\frac{j}{p}\right) = 0$

- Normalize each column