Two Algorithmic Hardness Results in Random Combinatorial Structures

David Gamarnik

MIT

Spin Glasses and Related Topics. Banff 2018

September, 2018

Two algorithmic challenges

Two algorithmic challenges

- Computing *exactly* the partition function of the **Sherrington-Kirkpatrick (SK)** spin glass model with Gaussian couplings. The algorithmic hardness result.

Two algorithmic challenges

- Computing *exactly* the partition function of the **Sherrington-Kirkpatrick (SK)** spin glass model with Gaussian couplings. The algorithmic hardness result.
- Explicit construction of matrices satisfying the **Restricted Isometry Property (RIP)** is "**Ramsey**"-hard.

PART I: Computing the partition function of the SK model

- Input: $\mathbf{J} = (J_{ij}, 1 \le i < j \le n)$, $\beta \in \mathbb{R}$. $J_{ij} \stackrel{d}{=} N(0,1)$, i.i.d.

- Input: $\mathbf{J} = (J_{ij}, 1 \le i < j \le n)$, $\beta \in \mathbb{R}$. $J_{ij} \overset{d}{=} N(0,1)$, i.i.d.
- Computational goal: construct an algorithm $\mathcal{A}$ for computing the partition function

$$Z(\mathbf{J}) \triangleq \sum_{\sigma \in \{-1,1\}^n} \exp\left(\frac{\beta}{\sqrt{n}} \sum_{i<j} J_{ij}\sigma_i\sigma_j \right).$$

Computing the partition function of the SK model

Computing the partition function of the SK model

- The problem of computing $Z(\mathbf{J})$ for *arbitrary* $\mathbf{J}$ is known to be #P-hard, Valiant [80s].

Computing the partition function of the SK model

- The problem of computing $Z(\mathbf{J})$ for *arbitrary* $\mathbf{J}$ is known to be #P-hard, Valiant [80s].
- Requirement:

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{J}) = Z(\mathbf{J})\right) = 1 - o(1).$$

The probability is with respect to randomness of $\mathbf{J}$.

Computing the partition function of the SK model

- The problem of computing $Z(\mathbf{J})$ for *arbitrary* $\mathbf{J}$ is known to be #P-hard, Valiant [80s].
- Requirement:

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{J}) = Z(\mathbf{J})\right) = 1 - o(1).$$

  The probability is with respect to randomness of $\mathbf{J}$.
- Thus our goal is *average* case hardness.

Computing the partition function of the SK model

- The problem of computing $Z(\mathbf{J})$ for *arbitrary* $\mathbf{J}$ is known to be #P-hard, Valiant [80s].
- Requirement:

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{J}) = Z(\mathbf{J})\right) = 1 - o(1).$$

  The probability is with respect to randomness of $\mathbf{J}$.
- Thus our goal is *average* case hardness.
- Average case hardness if of interest in Cryptography and TCS in general.
- Examples of average case hard problems: Permanent, Shortest Lattice Vector

Reformulation in terms of cuts

Let $H(\sigma) = \sum_{i<j:\sigma_i \neq \sigma_j} J_{ij}$. Then

$$\sum_{i<j} J_{ij}\sigma_i\sigma_j + 2H(\sigma) = \sum_{ij} J_{ij}.$$

Thus we focus on computing

$$Z(\mathbf{J}) = \sum_{\sigma} \exp(\beta n^{-\frac{1}{2}} H(\sigma)).$$

Finite precision version of the problem

Finite precision version of the problem

The problem is not algorithmically sound since the input J_{ij} is irrational (unless Blum-Shub-Smale model of computation is used).

Finite precision version of the problem

The problem is not algorithmically sound since the input J_{ij} is irrational (unless Blum-Shub-Smale model of computation is used).
Finite precision version:

Finite precision version of the problem

The problem is not algorithmically sound since the input J_{ij} is irrational (unless Blum-Shub-Smale model of computation is used).
Finite precision version:

- Let $X_{ij} = \exp(\beta n^{-\frac{1}{2}} J_{ij})$, so that $Z(\mathbf{J}) = \sum_{\sigma} \prod_{\sigma_i \neq \sigma_j} X_{ij}$

Finite precision version of the problem

The problem is not algorithmically sound since the input J_{ij} is irrational (unless Blum-Shub-Smale model of computation is used).
Finite precision version:

- Let $X_{ij} = \exp(\beta n^{-\frac{1}{2}} J_{ij})$, so that $Z(\mathbf{J}) = \sum_\sigma \prod_{\sigma_i \neq \sigma_j} X_{ij}$
- Fix $N \in \mathbb{Z}$ and let $X_{ij}^{[N]} = 2^{-N} \lfloor 2^N X_{ij} \rfloor \in \mathbb{Q}$. Let

$$Z(\mathbf{X}^{[N]}) = \sum_\sigma \prod_{\sigma_i \neq \sigma_j} X_{ij}^{[N]}$$

Finite precision version of the problem

The problem is not algorithmically sound since the input J_{ij} is irrational (unless Blum-Shub-Smale model of computation is used).
Finite precision version:

- Let $X_{ij} = \exp(\beta n^{-\frac{1}{2}} J_{ij})$, so that $Z(\mathbf{J}) = \sum_\sigma \prod_{\sigma_i \neq \sigma_j} X_{ij}$
- Fix $N \in \mathbb{Z}$ and let $X_{ij}^{[N]} = 2^{-N} \lfloor 2^N X_{ij} \rfloor \in \mathbb{Q}$. Let

$$Z(\mathbf{X}^{[N]}) = \sum_\sigma \prod_{\sigma_i \neq \sigma_j} X_{ij}^{[N]}$$

Note: $A_{ij} = 2^N X_{ij}^{[N]} = \lfloor 2^N X_{ij} \rfloor$ are integers. Let $I(\sigma)$ be the cardinality of the set $\{i < j : \sigma_i \neq \sigma_j\}$. Then

$$Z(\mathbf{A}) \triangleq \sum_\sigma 2^{N \frac{n(n-1)}{2} - NI(\sigma)} \prod_{i<j:\sigma_i \neq \sigma_j} A_{ij} \tag{1}$$

$$= 2^{N \frac{n(n-1)}{2}} Z(\mathbf{X}^{[N]}),$$

Finite precision version of the problem

Finite precision version of the problem

Goal: Compute

$$Z(\mathbf{A}) = \sum_{\sigma} 2^{N\frac{n(n-1)}{2} - NI(\sigma)} \prod_{\sigma_i \neq \sigma_j} A_{ij}$$

exactly.

Main result

Main result

Theorem

Suppose the precision value N satisfies $18 \log n \leq N \leq n^{\alpha}$*, for any constant* $\alpha > 0$*. Namely the number of bits in the precision is at least logarithmic and at most polynomial in n. If there exists a polynomial in n time algorithm* $\mathcal{A}$ *which on input* $\mathbf{A}$ *produces a value* $Z_{\mathcal{A}}(\mathbf{A})$ *satisfying*

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{A}) = Z(\mathbf{A})\right) \geq 1 - \frac{1}{3n^2},$$

for all sufficiently large n, then $P = \#P$*.*

Main result

Theorem

Suppose the precision value N satisfies $18 \log n \leq N \leq n^{\alpha}$*, for any constant* $\alpha > 0$*. Namely the number of bits in the precision is at least logarithmic and at most polynomial in n. If there exists a polynomial in n time algorithm* $\mathcal{A}$ *which on input* $\mathbf{A}$ *produces a value* $Z_{\mathcal{A}}(\mathbf{A})$ *satisfying*

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{A}) = Z(\mathbf{A})\right) \geq 1 - \frac{1}{3n^2},$$

for all sufficiently large n, then $P = \#P$*.*

Comments:

Main result

Theorem

Suppose the precision value N satisfies $18 \log n \leq N \leq n^{\alpha}$*, for any constant* $\alpha > 0$*. Namely the number of bits in the precision is at least logarithmic and at most polynomial in n. If there exists a polynomial in n time algorithm* $\mathcal{A}$ *which on input* $\mathbf{A}$ *produces a value* $Z_{\mathcal{A}}(\mathbf{A})$ *satisfying*

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{A}) = Z(\mathbf{A})\right) \geq 1 - \frac{1}{3n^2},$$

for all sufficiently large n, then $P = \#P$*.*

Comments:

- The proof uses Lipton's [91] mod prime computation in $\mathbb{Z}_p$ and hardness of computing the permanent of a matrix on average.

Main result

Theorem

Suppose the precision value N satisfies $18 \log n \leq N \leq n^{\alpha}$*, for any constant* $\alpha > 0$*. Namely the number of bits in the precision is at least logarithmic and at most polynomial in n. If there exists a polynomial in n time algorithm* $\mathcal{A}$ *which on input* $\mathbf{A}$ *produces a value* $Z_{\mathcal{A}}(\mathbf{A})$ *satisfying*

$$\mathbb{P}\left(Z_{\mathcal{A}}(\mathbf{A}) = Z(\mathbf{A})\right) \geq 1 - \frac{1}{3n^2},$$

for all sufficiently large n, then $P = \#P$*.*

Comments:

- The proof uses Lipton's [91] mod prime computation in $\mathbb{Z}_p$ and hardness of computing the permanent of a matrix on average.
- Some strengthening of $1 - n^{O(1)}$ assumption was obtained later by Feige & Lund [92] using the communication complexity theory.

Proof sketch. Step I

Proof sketch. Step I

- Fix a prime $n^2 < p_n = O(n^2 \log n)$ (possible using the density of primes property). Compute $Z(\mathbf{A}) \bmod (p_n)$ instead.

Proof sketch. Step I

- Fix a prime $n^2 < p_n = O(n^2 \log n)$ (possible using the density of primes property). Compute $Z(\mathbf{A})$ mod (p_n) instead.
- Suppose $\mathbf{U} = (U_{ij}, i < j)$ are generated uniformly at random from $[0, p_n - 1]$.

Proof sketch. Step I

- Fix a prime $n^2 < p_n = O(n^2 \log n)$ (possible using the density of primes property). Compute $Z(\mathbf{A}) \bmod (p_n)$ instead.
- Suppose $\mathbf{U} = (U_{ij}, i < j)$ are generated uniformly at random from $[0, p_n - 1]$.
- **Claim:** computing $Z(\mathbf{U})$ is hard on average by worst-case to average case reduction.

Proof sketch. Step I

- Fix a prime $n^2 < p_n = O(n^2 \log n)$ (possible using the density of primes property). Compute $Z(\mathbf{A}) \bmod (p_n)$ instead.
- Suppose $\mathbf{U} = (U_{ij}, i < j)$ are generated uniformly at random from $[0, p_n - 1]$.
- **Claim:** computing $Z(\mathbf{U})$ is hard on average by worst-case to average case reduction.
- **Key observation (Lipton's trick):** for every deterministic a_{ij}, $a_{ij} + tU_{ij} \bmod (p_n)$ is u.a.r. in $[0, p_n - 1]$ for all $1 \leq t \leq p_n - 1$.

Proof sketch. Step I

- Fix a prime $n^2 < p_n = O(n^2 \log n)$ (possible using the density of primes property). Compute $Z(\mathbf{A}) \bmod (p_n)$ instead.
- Suppose $\mathbf{U} = (U_{ij}, i < j)$ are generated uniformly at random from $[0, p_n - 1]$.
- **Claim:** computing $Z(\mathbf{U})$ is hard on average by worst-case to average case reduction.
- **Key observation (Lipton's trick):** for every deterministic a_{ij}, $a_{ij} + tU_{ij} \bmod (p_n)$ is u.a.r. in $[0, p_n - 1]$ for all $1 \le t \le p_n - 1$.
- $$P(t) \triangleq Z(\mathbf{a} + t\mathbf{U}) = \sum_{\sigma} 2^{N\frac{n(n-1)}{2} - NI(\sigma)} \prod_{\sigma_i \neq \sigma_j} (a_{ij} + tU_{ij})$$

  is a polynomial in t with degree $M = \max_i i(n-i) < n^2 < p_n$.

Proof sketch. Step I

Proof sketch. Step I

- If we can compute $Z(\mathbf{A})$ with probability at at least $1 - O(n^{-2})$ we can compute $P(t)$ for all $t = 1, 2, \ldots, M + 1$ with probability at least $1/2$.

Proof sketch. Step I

- If we can compute $Z(\mathbf{A})$ with probability at at least $1 - O(n^{-2})$ we can compute $P(t)$ for all $t = 1, 2, \ldots, M + 1$ with probability at least $1/2$.
- Inverting, we can compute $P(0) = Z(\mathbf{a})$, which is #P-hard. $\square$

Proof sketch. Step II

Proof sketch. Step II

In the regime $18 \log n \leq N \leq n^{\alpha}$, the distribution of $A_{ij} = \lfloor 2^N \exp(\beta n^{-\frac{1}{2}} J_{ij}) \rfloor$ in $[0, p_n - 1]$ is $O(n^{-3})$ close to uniform. $\square$

Some comments

Some comments

- Some immediate generalizations

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.
  - Gaussianity of the couplings is non-essential. Well behaved distributions with sufficiently smooth density should be enough.

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.
  - Gaussianity of the couplings is non-essential. Well behaved distributions with sufficiently smooth density should be enough.
  - $n^{\frac{1}{2}}$ in $\exp(\beta n^{-\frac{1}{2}})$ is non-essential. Any constant power of n is ok.

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.
  - Gaussianity of the couplings is non-essential. Well behaved distributions with sufficiently smooth density should be enough.
  - $n^{\frac{1}{2}}$ in $\exp(\beta n^{-\frac{1}{2}})$ is non-essential. Any constant power of n is ok.
- Limitations

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.
  - Gaussianity of the couplings is non-essential. Well behaved distributions with sufficiently smooth density should be enough.
  - $n^{\frac{1}{2}}$ in $\exp(\beta n^{-\frac{1}{2}})$ is non-essential. Any constant power of n is ok.
- Limitations
  - The trick of $\mathrm{mod}(p_n)$ computation is too "fragile" to survive the approximate computation. It seems this method is hopeless to establish the approximation hardness of computing $Z(\mathbf{J})$.

Some comments

- Some immediate generalizations
  - 2-spin assumption of the SK is non-essential. The method extends to the p-spin models.
  - Gaussianity of the couplings is non-essential. Well behaved distributions with sufficiently smooth density should be enough.
  - $n^{\frac{1}{2}}$ in $\exp(\beta n^{-\frac{1}{2}})$ is non-essential. Any constant power of n is ok.
- Limitations
  - The trick of $\mathrm{mod}(p_n)$ computation is too "fragile" to survive the approximate computation. It seems this method is hopeless to establish the approximation hardness of computing $Z(\mathbf{J})$.
  - The problem of computing the ground state $\min_\sigma J_{ij}\sigma_i\sigma_j$ is "non-algebraic" so the trick of $\mathrm{mod}(p_n)$ computation again appears useless.

Part II

Explicit construction of RIP matrices

Explicit construction of RIP matrices

- A matrix $\Phi \in \mathbb{R}^{n\times p}$ satisfies the (δ, s) Restricted Isometry Property (RIP) for $\delta \in (0,1), s \leq p$ if for every s-sparse vector β ($\|\beta\|_0 \leq s$)

$$||\|\Phi\beta\|_2^2 - \|\beta\|_2| \leq \delta\|\beta\|_2^2.$$

Explicit construction of RIP matrices

- A matrix $\Phi \in \mathbb{R}^{n \times p}$ satisfies the (δ, s) Restricted Isometry Property (RIP) for $\delta \in (0, 1)$, $s \leq p$ if for every s-sparse vector β ($\|\beta\|_0 \leq s$)

$$||\|\Phi\beta\|_2^2 - \|\beta\|_2| \leq \delta\|\beta\|_2^2.$$

- Importance: compressive sensing: if Φ is $2s$-RIP with $\delta < 2/3$, then every s-sparse β^* is the unique solution of

$$\begin{aligned} &\min \|\beta\|_1 \\ &\text{Subject to } : \Phi\beta = \Phi\beta^*, \end{aligned}$$

  and thus can be uniquely recovered by solving this linear programming problem.

Random matrices are RIP

Random matrices are RIP

- If entries of Φ are i.i.d. zero mean sub-Gaussian with variance $1/n$, then Φ is RIP w.h.p. provided

$$n = \Omega\left(s \log(p/s)\right).$$

Random matrices are RIP

- If entries of Φ are i.i.d. zero mean sub-Gaussian with variance $1/n$, then Φ is RIP w.h.p. provided

$$n = \Omega\left(s \log(p/s)\right).$$

- For example, if $s = \log^{\alpha} p$, then $n = \Omega(\log^{\alpha+1} p)$ suffices.

Random matrices are RIP

- If entries of Φ are i.i.d. zero mean sub-Gaussian with variance $1/n$, then Φ is RIP w.h.p. provided

$$n = \Omega\left(s \log(p/s)\right).$$

- For example, if $s = \log^\alpha p$, then $n = \Omega(\log^{\alpha+1} p)$ suffices.
- Thus one obtains a simple randomized algorithm for constructing RIP matrices.

Random matrices are RIP

- If entries of Φ are i.i.d. zero mean sub-Gaussian with variance $1/n$, then Φ is RIP w.h.p. provided

$$n = \Omega\left(s \log(p/s)\right).$$

- For example, if $s = \log^{\alpha} p$, then $n = \Omega(\log^{\alpha+1} p)$ suffices.
- Thus one obtains a simple randomized algorithm for constructing RIP matrices.
- ... But certifying RIP is hard in the worst-case Bandeira, Dobriban, Mixon & Sawin [13] and on average Koiran & Zouzias [14].

Random matrices are RIP

- If entries of Φ are i.i.d. zero mean sub-Gaussian with variance $1/n$, then Φ is RIP w.h.p. provided

$$n = \Omega\left(s \log(p/s)\right).$$

- For example, if $s = \log^\alpha p$, then $n = \Omega(\log^{\alpha+1} p)$ suffices.
- Thus one obtains a simple randomized algorithm for constructing RIP matrices.
- ... But certifying RIP is hard in the worst-case Bandeira, Dobriban, Mixon & Sawin [13] and on average Koiran & Zouzias [14].
- **Challenge:** explicit (deterministic) construction.

Square Root bottleneck for explicit constructions

- Many explicit constructions were known but all were hitting the barrier $s = O(\sqrt{n})$. Bandeira, Fickus, Mixon & Wong [13]

Square Root bottleneck for explicit constructions

- Many explicit constructions were known but all were hitting the barrier $s = O(\sqrt{n})$. Bandeira, Fickus, Mixon & Wong [13]
- Beating the "Square Root" barrier became a major challenge, popularized in Terry Tao's blog in [07], and Joel Moreira's blog in [13].

Square Root bottleneck for explicit constructions

- Many explicit constructions were known but all were hitting the barrier $s = O(\sqrt{n})$. Bandeira, Fickus, Mixon & Wong [13]
- Beating the "Square Root" barrier became a major challenge, popularized in Terry Tao's blog in [07], and Joel Moreira's blog in [13].
- Breakthrough: Bourgain, Dilworth, Ford, Konyagin & Kutzarova [11]. $n = s^{\frac{1}{2}+\epsilon}$ for small constant ϵ in the regime $n = p^{O(1)}$.

Square Root bottleneck for explicit constructions

- Many explicit constructions were known but all were hitting the barrier $s = O(\sqrt{n})$. Bandeira, Fickus, Mixon & Wong [13]
- Beating the "Square Root" barrier became a major challenge, popularized in Terry Tao's blog in [07], and Joel Moreira's blog in [13].
- Breakthrough: Bourgain, Dilworth, Ford, Konyagin & Kutzarova [11]. $n = s^{\frac{1}{2}+\epsilon}$ for small constant ϵ in the regime $n = p^{O(1)}$.
- No improvements since then.

Explicit construction of Ramsey graphs

Explicit construction of Ramsey graphs

- Given m, a complete graph on p nodes with edges colored by $1, \ldots, q$ is called $R(m; q)$-Ramsey if the largest monochromatic clique has size at most m.

Explicit construction of Ramsey graphs

- Given m, a complete graph on p nodes with edges colored by $1, \ldots, q$ is called $R(m; q)$-Ramsey if the largest monochromatic clique has size at most m.
- Random q-coloring of a p-node complete graph gives $m = O(\log p)$, Erdös, [1947].

Explicit construction of Ramsey graphs

- Given m, a complete graph on p nodes with edges colored by $1, \ldots, q$ is called $R(m; q)$-Ramsey if the largest monochromatic clique has size at most m.
- Random q-coloring of a p-node complete graph gives $m = O(\log p)$, Erdös, [1947].
- **Challenge:** explicit construction of Ramsey graphs. Construct explicitly a graph on p nodes with $m = O(\log p)$. Applications in cryptography.

Explicit construction of Ramsey graphs

- Given m, a complete graph on p nodes with edges colored by $1, \ldots, q$ is called $R(m; q)$-Ramsey if the largest monochromatic clique has size at most m.
- Random q-coloring of a p-node complete graph gives $m = O(\log p)$, Erdös, [1947].
- **Challenge:** explicit construction of Ramsey graphs. Construct explicitly a graph on p nodes with $m = O(\log p)$. Applications in cryptography.
- Huge literature and gradual improvements from $p^{O(1)}$, to

$$(\log p)^{\log\log\log^{O(1)} p}, \qquad q = 2,$$

Cohen [17]. Survey by Conlon, Fox & Sudakov [15]. There are results for general q, but weaker than the above.

Constructing RIP matrices is Ramsey-hard

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n \times p}$, suppose it is RIP with $s \geq 2\sqrt{n} + 1$ and $s = O(\log p)$. Then one can construct a $R(m; 3)$ graph with $m = O(\log^2 p)$.

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n \times p}$*, suppose it is RIP with* $s \geq 2\sqrt{n} + 1$ *and* $s = O(\log p)$*. Then one can construct a* $R(m; 3)$ *graph with* $m = O(\log^2 p)$*.*

Proof

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n\times p}$, suppose it is RIP with $s \geq 2\sqrt{n}+1$ and $s = O(\log p)$. Then one can construct a $R(m;3)$ graph with $m = O(\log^2 p)$.

Proof

Construction. Given $\Phi = [u_1, \ldots, u_p]$, color (i, j)

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n\times p}$, suppose it is RIP with $s \geq 2\sqrt{n}+1$ and $s = O(\log p)$. Then one can construct a $R(m;3)$ graph with $m = O(\log^2 p)$.

Proof

Construction. Given $\Phi = [u_1, \ldots, u_p]$, color (i, j)

- red if $|\langle u_i, u_j\rangle| \leq \frac{1}{2\sqrt{n}}$;

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n \times p}$*, suppose it is RIP with* $s \geq 2\sqrt{n} + 1$ *and* $s = O(\log p)$*. Then one can construct a* $R(m; 3)$ *graph with* $m = O(\log^2 p)$*.*

Proof

Construction. Given $\Phi = [u_1, \ldots, u_p]$, color (i, j)

- red if $|\langle u_i, u_j \rangle| \leq \frac{1}{2\sqrt{n}}$;
- blue if $\langle u_i, u_j \rangle > \frac{1}{2\sqrt{n}}$

Constructing RIP matrices is Ramsey-hard

Theorem

Given a matrix $\Phi \in \mathbb{R}^{n \times p}$, suppose it is RIP with $s \geq 2\sqrt{n} + 1$ and $s = O(\log p)$. Then one can construct a $R(m; 3)$ graph with $m = O(\log^2 p)$.

Proof

Construction. Given $\Phi = [u_1, \ldots, u_p]$, color (i, j)

- red if $|\langle u_i, u_j \rangle| \leq \frac{1}{2\sqrt{n}}$;
- blue if $\langle u_i, u_j \rangle > \frac{1}{2\sqrt{n}}$
- green if $\langle u_i, u_j \rangle < -\frac{1}{2\sqrt{n}}$

Proof

Proof

- **Claim:** If Φ is s-RIP, then the largest monochromatic clique in this graph is at most $2n$.

Proof

- **Claim:** If Φ is s-RIP, then the largest monochromatic clique in this graph is at most $2n$.
- Assume claim holds. Take RIP matrix with $s = O(\log p)$.

Proof

- **Claim:** If Φ is s-RIP, then the largest monochromatic clique in this graph is at most $2n$.
- Assume claim holds. Take RIP matrix with $s = O(\log p)$.
- From $s \geq 2\sqrt{n} + 1$, the Ramsey value of this graph is $n \leq ((s-1)/2)^2 = O(\log^2 p)$. $\square$

Proof of claim

Proof of claim

Proposition

For any set of unit norm vectors $u_1, \ldots, u_{2n} \in \mathbb{R}^n$*,*
$\max_{1 \le i \ne j \le 2n} |\langle u_i, u_j \rangle| > \frac{1}{2\sqrt{n}}$.

Proof of claim

Proposition

For any set of unit norm vectors $u_1, \ldots, u_{2n} \in \mathbb{R}^n$,
$\max_{1 \le i \ne j \le 2n} |\langle u_i, u_j \rangle| > \frac{1}{2\sqrt{n}}$.

Special case of Kabatyanski & Levenstein [78] bound, also discussed in Terry Tao's (different) blog in [13]

Proof (from this blog).

Consider the symmetric matrix $U = (\langle u_i, u_j \rangle, 1 \le i, j \le 2n) \in \mathbb{R}^{2n \times 2n}$ of inner products. This is a rank-n matrix in $\mathbb{R}^{2n \times 2n}$ and as such $\bar{U} \triangleq U - I_{2n \times 2n}$ has an eigenvalue -1 with multiplicity at least n. Thus the trace of $\bar{U}^2$ which is $\sum_{1 \le i \ne j \le 2n} (\langle u_i, u_j \rangle)^2$ is at least n, implying $\max_{i \ne j} |\langle u_i, u_j \rangle| \ge \frac{1}{\sqrt{2(2n-1)}}$. □

Proof of claim

Proof of claim

- Thus the largest red clique in our graph is at most $2n - 1$.

Proof of claim

- Thus the largest red clique in our graph is at most $2n - 1$.
- Suppose $C \subset [p]$ is a blue clique with $|C| = 2\sqrt{n} + 1$.

Proof of claim

- Thus the largest red clique in our graph is at most $2n - 1$.
- Suppose $C \subset [p]$ is a blue clique with $|C| = 2\sqrt{n} + 1$.
- Define $x \in \mathbb{R}^p$ by $x_i = 1/\sqrt{|C|}, i \in C$ and $x_i = 0$ otherwise. This vector is $|C| \leq s$-sparse.

Proof of claim

- Thus the largest red clique in our graph is at most $2n - 1$.
- Suppose $C \subset [p]$ is a blue clique with $|C| = 2\sqrt{n} + 1$.
- Define $x \in \mathbb{R}^p$ by $x_i = 1/\sqrt{|C|}, i \in C$ and $x_i = 0$ otherwise. This vector is $|C| \leq s$-sparse.
- But

$$\|\Phi x\|_2^2 - \|x\|_2^2 = \frac{1}{|C|} \sum_{i \neq j \in C} \langle u_i, u_j \rangle \geq \frac{|C| - 1}{2\sqrt{n}} = 1,$$

which contradicts RIP.

Proof of claim

- Thus the largest red clique in our graph is at most $2n - 1$.
- Suppose $C \subset [p]$ is a blue clique with $|C| = 2\sqrt{n} + 1$.
- Define $x \in \mathbb{R}^p$ by $x_i = 1/\sqrt{|C|}, i \in C$ and $x_i = 0$ otherwise. This vector is $|C| \leq s$-sparse.
- But

$$\|\Phi x\|_2^2 - \|x\|_2^2 = \frac{1}{|C|} \sum_{i \neq j \in C} \langle u_i, u_j \rangle \geq \frac{|C| - 1}{2\sqrt{n}} = 1,$$

  which contradicts RIP.
- Same proof for green cliques.
  Thus the largest monochromatic clique in this graph is $\max(2n, 2\sqrt{n}) = 2n$. $\square$

Comments

Comments

- If Φ consists of non-negative entries (as it is in many constructions), then our construction implies 2-Ramsey graph.

Comments

- If Φ consists of non-negative entries (as it is in many constructions), then our construction implies 2-Ramsey graph.
- The result does not contradict Bourgain et al [11] construction, which requires $n = p^{O(1)}$.

Comments

- If Φ consists of non-negative entries (as it is in many constructions), then our construction implies 2-Ramsey graph.
- The result does not contradict Bourgain et al [11] construction, which requires $n = p^{O(1)}$.
- **Question:** Can one use Ramsey graph to construct RIP matrices?

Thank you