Spectral pseudorandomness and the clique number of the Paley graph

Tim Kunisky

Yale University

MIT Stochastics and Statistics Seminar
March 3, 2023

I. Introduction

Paley Graph

Paley Graph

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ = finite field on p elements for $p \equiv 1 \bmod 4$.

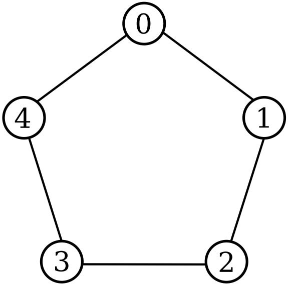
G_p a graph on vertices $\mathbb{F}_p$ with $i \sim j$ iff $j - i$ is a **square** mod p (for some $x \neq 0$, $j - i = x^2$).

Paley Graph

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ = finite field on p elements for $p \equiv 1 \bmod 4$.

G_p a graph on vertices $\mathbb{F}_p$ with $i \sim j$ iff $j - i$ is a **square** mod p (for some $x \neq 0$, $j - i = x^2$).

Example: $p = 5 \rightsquigarrow$ squares are $\{1, 4 \equiv -1\}$.



Paley Graph

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ = finite field on p elements for $p \equiv 1 \bmod 4$.

G_p a graph on vertices $\mathbb{F}_p$ with $i \sim j$ iff $j - i$ is a **square** mod p (for some $x \neq 0$, $j - i = x^2$).

Heuristic: Addition and multiplication are independent.

Paley Graph

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ = finite field on p elements for $p \equiv 1 \bmod 4$.

G_p a graph on vertices $\mathbb{F}_p$ with $i \sim j$ iff $j - i$ is a **square** mod p (for some $x \neq 0$, $j - i = x^2$).

Heuristic: Addition and multiplication are independent.

$\Longrightarrow$ adjacencies in G_p look independent.

$\Longrightarrow$ G_p is **pseudorandom**, behaving like Erdős-Rényi graph with edge probability $\frac{1}{2}$ (since $\deg(x) = \frac{p-1}{2} \sim \frac{1}{2}p$).

Paley Graph

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ = finite field on p elements for $p \equiv 1 \bmod 4$.

G_p a graph on vertices $\mathbb{F}_p$ with $i \sim j$ iff $j - i$ is a **square** mod p (for some $x \neq 0$, $j - i = x^2$).

Heuristic: Addition and multiplication are independent.

$\implies$ adjacencies in G_p look independent.

$\implies$ G_p is **pseudorandom**, behaving like Erdős-Rényi graph with edge probability $\frac{1}{2}$ (since $\deg(x) = \frac{p-1}{2} \sim \frac{1}{2}p$).

Example: As $p \to \infty$,

$$\begin{aligned}\#\text{ triangles in } G_p &\sim \mathbb{E}\left[\#\text{ triangles in ER}\right] \\ &= \binom{p}{3}\left(\frac{1}{2}\right)^3 \sim \frac{1}{48}p^3.\end{aligned}$$

Paley Graphs: The Clique Number

Question: How about extremal questions (large subgraphs)?

Example: $\omega(G) :=$ **largest clique** in G.

Paley Graphs: The Clique Number

Question: How about extremal questions (large subgraphs)?

Example: $\omega(G) :=$ **largest clique** in G. Easy calculations $\Longrightarrow$

$$\mathbb{E}[\omega(\mathsf{ER})] \sim 2 \log_2 p$$

Paley Graphs: The Clique Number

Question: How about extremal questions (large subgraphs)?

Example: $\omega(G)$:= **largest clique** in G. Easy calculations $\Longrightarrow$

$$\mathbb{E}[\omega(\mathsf{ER})] \sim 2 \log_2 p$$

Same for $\omega(G_p)$? Not quite...

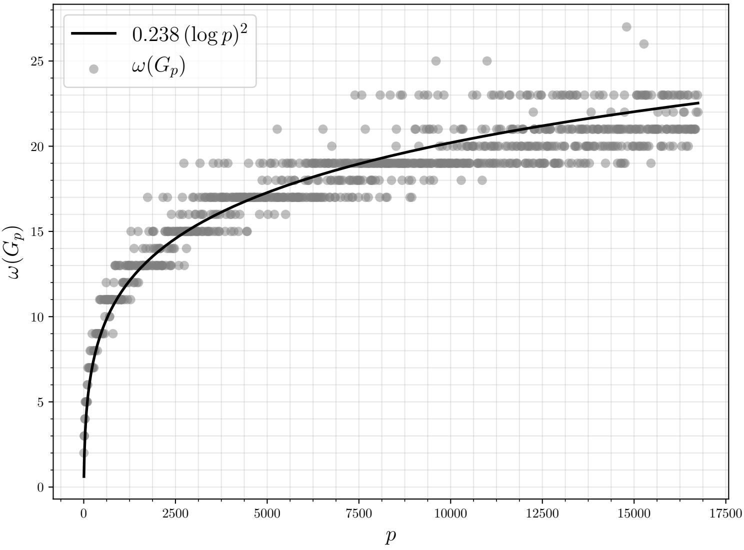
$$\omega(G_{p_i}) \geq \log p_i \log\log\log p_i \qquad \text{[Graham, Ringrose '90]}$$

$$\omega(G_p) \overset{?}{\sim} (\log p)^2 \qquad \text{(numerics)}$$

And, in any case, the best **upper bounds** we have are

$$\omega(G_p) \leq \sqrt{p} \qquad \text{(spectral/Hoffman/trivial bound)}$$

$$\omega(G_p) \leq \sqrt{p/2} + 1 \qquad \text{[Hanson, Petridis '21]}$$



$0.238\,(\log p)^2$
$\omega(G_p)$
$\omega(G_p)$
p
0
5
10
15
20
25
0
2500
5000
7500
10000
12500
15000
17500

Big **number theory** question:

What proof technique can break the "square root barrier" and prove

$$\omega(G_p) = O(p^{1/2-\varepsilon}) \ ?$$

II. Sum-of-Squares Relaxations

(joint work with with Xifan Yu)

A degree 4 sum-of-squares lower bound for the clique number of the Paley graph [arXiv:2211.02713]

Sum-of-Squares (SOS) Relaxations

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max \left\{ \sum_{i \in V} y_i \;:\; y_i^2 - y_i = 0, \quad y_i y_j = 0 \text{ if } \{i, j\} \notin E \right\}$$

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max\left\{\sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E\right\}$$

Semidefinite programming upper bound recipe:

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max\left\{\sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E\right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d^\top}$

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max \left\{ \sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E \right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \le d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \le d} \boldsymbol{y}^{\otimes \le d^\top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max\left\{\sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E\right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d^\top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:
    - $\boldsymbol{X} \succeq \boldsymbol{0}$

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max \left\{ \sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E \right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d^\top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:
   - $\boldsymbol{X} \succeq \boldsymbol{0}$
   - $X_{\boldsymbol{i},\boldsymbol{j}} = y_{i_1} \cdots y_{i_k} y_{j_1} \cdots y_{j_\ell}$

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max \left\{ \sum_{i \in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E \right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d^\top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:
    - $\boldsymbol{X} \succeq \boldsymbol{0}$
    - $X_{\boldsymbol{i},\boldsymbol{j}} = X(S)$ depends only on index set S in $\boldsymbol{i}, \boldsymbol{j}$

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max\left\{\sum_{i\in V} y_i \ : \ y_i^2 - y_i = 0, \ \ y_i y_j = 0 \text{ if } \{i, j\} \notin E\right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \ \ \boldsymbol{y} \ \ \boldsymbol{y}^{\otimes 2} \ \cdots \ \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d^\top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:
   - $\boldsymbol{X} \succeq \boldsymbol{0}$
   - $X_{\boldsymbol{i},\boldsymbol{j}} = X(S)$ depends only on index set S in $\boldsymbol{i}, \boldsymbol{j}$
   - $X(\varnothing) = 1$, $X(S) = 0$ for all S not a clique in G

Sum-of-Squares (SOS) Relaxations

For any graph $G = (V, E)$, have polynomial (Boolean) optimization formulation,

$$\omega(G) = \max \left\{ \sum_{i \in V} y_i \;:\; y_i^2 - y_i = 0, \quad y_i y_j = 0 \text{ if } \{i, j\} \notin E \right\}$$

Semidefinite programming upper bound recipe:

1. Write $\boldsymbol{y}^{\otimes \leq d} = [1 \;\; \boldsymbol{y} \;\; \boldsymbol{y}^{\otimes 2} \;\; \cdots \;\; \boldsymbol{y}^{\otimes d}]$ and $\boldsymbol{X} = \boldsymbol{y}^{\otimes \leq d} \boldsymbol{y}^{\otimes \leq d \top}$
2. Find some tractable constraints on $\boldsymbol{X}$ for feasible $\boldsymbol{y}$:
   - $\boldsymbol{X} \succeq \boldsymbol{0}$
   - $X_{\boldsymbol{i}, \boldsymbol{j}} = X(S)$ depends only on index set S in $\boldsymbol{i}, \boldsymbol{j}$
   - $X(\emptyset) = 1$, $X(S) = 0$ for all S not a clique in G
3. Optimize $\sum_{i \in V} X(\{i\})$ over that enlarged set

Degree 2 $=: \mathsf{SOS}_2(G)$ (Case $d = 1$)

Degree 2 =: $\mathsf{SOS}_2(G)$ (Case $d = 1$)

maximize $\sum_{i=1}^{p} X(\{i\})$ subject to

$$\boldsymbol{X} = \left[\begin{array}{c|cccc} 1 & X(\{1\}) & X(\{2\}) & \cdots & X(\{p\}) \\ \hline X(\{1\}) & X(\{1\}) & X(\{1,2\}) & \cdots & X(\{1,p\}) \\ X(\{2\}) & X(\{1,2\}) & X(\{2\}) & \cdots & X(\{2,p\}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X(\{p\}) & X(\{1,p\}) & X(\{2,p\}) & \cdots & X(\{p\}) \end{array}\right] \succeq \mathbf{0},$$

$X(\{i,j\}) = 0$ whenever $i \not\sim_G j$.

Degree 2 =: $\mathsf{SOS}_2(G)$ (Case $d = 1$)

maximize $\sum_{i=1}^{p} X(\{i\})$ subject to

$$\boldsymbol{X} = \left[\begin{array}{c|cccc} 1 & X(\{1\}) & X(\{2\}) & \cdots & X(\{p\}) \\ \hline X(\{1\}) & X(\{1\}) & X(\{1,2\}) & \cdots & X(\{1,p\}) \\ X(\{2\}) & X(\{1,2\}) & X(\{2\}) & \cdots & X(\{2,p\}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X(\{p\}) & X(\{1,p\}) & X(\{2,p\}) & \cdots & X(\{p\}) \end{array}\right] \succeq \mathbf{0},$$

$X(\{i,j\}) = 0$ whenever $i \not\sim_G j$.

This has been studied earlier as the **Lovász function** $\vartheta(\overline{G})$.

Degree 2 =: $\mathsf{SOS}_2(G)$ (Case $d = 1$)

maximize $\sum_{i=1}^{p} X(\{i\})$ subject to

$$\boldsymbol{X} = \left[\begin{array}{c|cccc} 1 & X(\{1\}) & X(\{2\}) & \cdots & X(\{p\}) \\ \hline X(\{1\}) & X(\{1\}) & X(\{1,2\}) & \cdots & X(\{1,p\}) \\ X(\{2\}) & X(\{1,2\}) & X(\{2\}) & \cdots & X(\{2,p\}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X(\{p\}) & X(\{1,p\}) & X(\{2,p\}) & \cdots & X(\{p\}) \end{array}\right] \succeq \mathbf{0},$$

$X(\{i,j\}) = 0$ whenever $i \not\sim_G j$.

This has been studied earlier as the **Lovász function** $\vartheta(\overline{G})$.

$d \geq 2 \rightsquigarrow \mathsf{SOS}_{2d}(G) \geq \omega(G)$, tighter bounds in time $p^{O(d)}$.

SOS Lower Bounds for Random Graphs

To study average-case difficulty of $\omega(\cdot)$, people wanted to understand how hard it is to compute $\omega(\mathsf{ER})$.

SOS Lower Bounds for Random Graphs

To study average-case difficulty of $\omega(\cdot)$, people wanted to understand how hard it is to compute $\omega(\mathsf{ER})$.

Theorem: [MW '13]...[BHKKMP '19] For any fixed d, as $p \to \infty$,

$$\mathbb{E}[\mathsf{SOS}_{2d}(\mathsf{ER})] = \Omega(p^{1/2-o(1)}) \gg O(\log p) = \mathbb{E}[\omega(\mathsf{ER})].$$

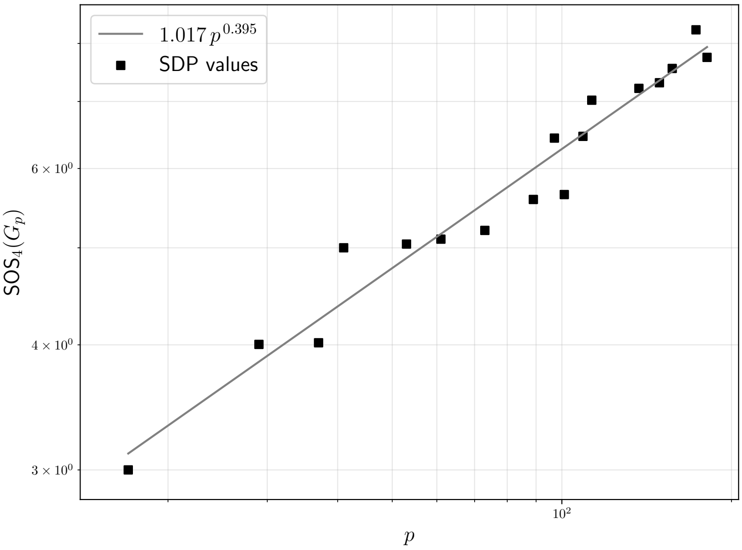
SOS Lower Bounds for Random Graphs

To study average-case difficulty of $\omega(\cdot)$, people wanted to understand how hard it is to compute $\omega(\mathsf{ER})$.

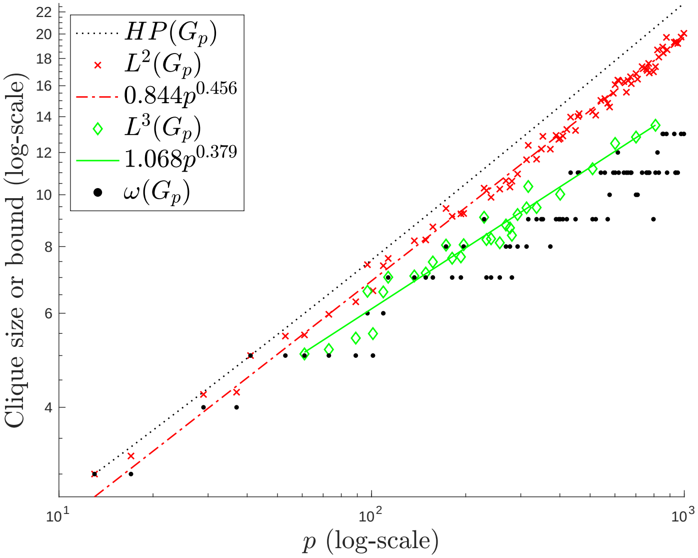
Theorem: [MW '13]...[BHKKMP '19] For any fixed d, as $p \to \infty$,

$$\mathbb{E}[\mathsf{SOS}_{2d}(\mathsf{ER})] = \Omega(p^{1/2-o(1)}) \gg O(\log p) = \mathbb{E}[\omega(\mathsf{ER})].$$

Question: Does this transfer to Paley graphs, showing that low-degree SOS cannot break the $\sqrt{p}$ barrier?



$1.017\,p^{0.395}$
SDP values
6×10^0
4×10^0
3×10^0
$\mathsf{SOS}_4(G_p)$
10^2
p



[Gvozdenović, Laurent, Vallentin ’09; Kobzar, Mody ’23 (forthcoming)]

Our Results

Main message: Degree 4 SOS might improve on the $\omega(G_p) \lesssim \sqrt{p}$ bound, but subject to limitations.

Our Results

Main message: Degree 4 SOS might improve on the $\omega(G_p) \lesssim \sqrt{p}$ bound, but subject to limitations.

Easy to show: $\mathsf{SOS}_2(G_p) = p^{1/2}$.

Our Results

Main message: Degree 4 SOS might improve on the $\omega(G_p) \lesssim \sqrt{p}$ bound, but subject to limitations.

Easy to show: $\mathsf{SOS}_2(G_p) = p^{1/2}$.

Main theorem: [KY '22] $\mathsf{SOS}_4(G_p) = \Omega(p^{1/3})$.

Our Results

Main message: Degree 4 SOS might improve on the $\omega(G_p) \lesssim \sqrt{p}$ bound, but subject to limitations.

Easy to show: $\mathsf{SOS}_2(G_p) = p^{1/2}$.

Main theorem: [KY '22] $\mathsf{SOS}_4(G_p) = \Omega(p^{1/3})$.

Remarks:

1. Derandomizes an early result on the random graph case: [DM '15] showed $\mathbb{E}[\mathsf{SOS}_4(\mathsf{ER})] = \widetilde{\Omega}(p^{1/3})$.

Our Results

Main message: Degree 4 SOS might improve on the $\omega(G_p) \lesssim \sqrt{p}$ bound, but subject to limitations.

Easy to show: $\mathsf{SOS}_2(G_p) = p^{1/2}$.

Main theorem: [KY '22] $\mathsf{SOS}_4(G_p) = \Omega(p^{1/3})$.

Remarks:

1. Derandomizes an early result on the random graph case: [DM '15] showed $\mathbb{E}[\mathsf{SOS}_4(\mathsf{ER})] = \widetilde{\Omega}(p^{1/3})$.
2. Compatible with numerics: maybe $\mathsf{SOS}_4(G_p) \sim p^{0.4}$.

Ancillary Results I: Lower Bound of $\Omega(p^{0.4})$?

Ancillary Results I: Lower Bound of $\Omega(p^{0.4})$?

We use a simple $\boldsymbol{X}$, first used by [FK '03], later by [MW '13], but ultimately found to be insufficient by [BHKKMP '19]:

$$X(S) := f(|S|) \cdot \mathbb{1}\{S \text{ is a clique in } G\}.$$

Ancillary Results I: Lower Bound of $\Omega(p^{0.4})$?

We use a simple $\boldsymbol{X}$, first used by [FK '03], later by [MW '13], but ultimately found to be insufficient by [BHKKMP '19]:

$$X(S) := f(|S|) \cdot \mathbb{1}\{S \text{ is a clique in } G\}.$$

Theorem: [Kelner '15] For ER graphs, such proves only

$$\mathbb{E}[\mathsf{SOS}_{2d}(\mathsf{ER})] = \widetilde{\Omega}(p^{1/(d+1)}).$$

Ancillary Results I: Lower Bound of $\Omega(p^{0.4})$?

We use a simple $\boldsymbol{X}$, first used by [FK '03], later by [MW '13], but ultimately found to be insufficient by [BHKKMP '19]:

$$X(S) := f(|S|) \cdot \mathbb{1}\{S \text{ is a clique in } G\}.$$

Theorem: [Kelner '15] For ER graphs, such proves only

$$\mathbb{E}[\mathsf{SOS}_{2d}(\mathsf{ER})] = \widetilde{\Omega}(p^{1/(d+1)}).$$

Theorem: [KY '22] For Paley graphs, such proves only

$$\mathsf{SOS}_4(G_p) = \Omega(p^{1/3}),$$

i.e., our main result cannot be improved without a fancier choice of $\boldsymbol{X}$ $\rightsquigarrow$ probably significantly harder to analyze.

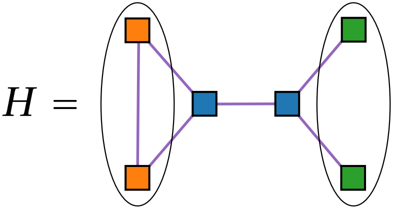
Ancillary Results II: Breaking the $\sqrt{p}$ Barrier?

Theoretical evidence: [BHKKMP '19] proof depends on norm bounds for **graph matrices** formed from the $\{\pm 1\}$ adjacency matrix $\boldsymbol{A}$.

Ancillary Results II: Breaking the $\sqrt{p}$ Barrier?

Theoretical evidence: [BHKKMP '19] proof depends on norm bounds for **graph matrices** formed from the $\{\pm 1\}$ adjacency matrix $\boldsymbol{A}$.

Example: For a graph with sets of "left" and "right" vertices



we get a matrix

$$M^H(G)_{(a,b),(c,d)} = \sum_{i \neq j \notin \{a,b,c,d\}} A_{a,b} A_{a,i} A_{b,i} A_{i,j} A_{j,c} A_{j,d}.$$

Ancillary Results II: Breaking the $\sqrt{p}$ Barrier?

Theoretical evidence: [BHKKMP '19] proof depends on norm bounds for **graph matrices** formed from the $\{\pm 1\}$ adjacency matrix $\boldsymbol{A}$.

Theorem: [KY '22] There are some H for which

$$\|\boldsymbol{M}^H(G_p)\| \gg \mathbb{E}\left[\|\boldsymbol{M}^H(\mathsf{ER})\|\right],$$

i.e., the key technical tool does not derandomize **in general** (but it does **for small** H to get our lower bound).

Ancillary Results II: Breaking the $\sqrt{p}$ Barrier?

Theoretical evidence: [BHKKMP '19] proof depends on norm bounds for **graph matrices** formed from the $\{\pm 1\}$ adjacency matrix $\boldsymbol{A}$.

Theorem: [KY '22] There are some H for which

$$\|\boldsymbol{M}^H(G_p)\| \gg \mathbb{E}\left[\|\boldsymbol{M}^H(\mathsf{ER})\|\right],$$

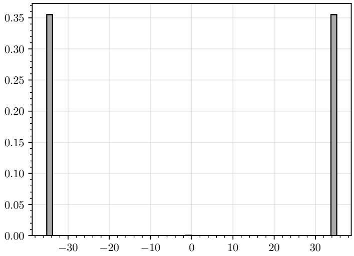
i.e., the key technical tool does not derandomize **in general** (but it does **for small** H to get our lower bound).

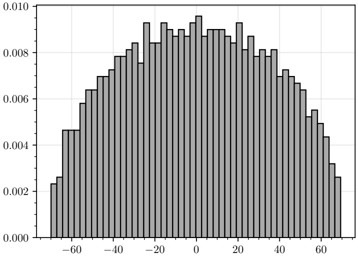
Basically, can build these by taking advantage of the discrepancy between

$$\boldsymbol{A}_{G_p}^2 = p\boldsymbol{I} - \boldsymbol{1}\boldsymbol{1}^\top,$$
$$\boldsymbol{A}_{\mathsf{ER}}^2 = p\boldsymbol{I} + \sqrt{p} \cdot (\text{random matrix}).$$

Our intuition: If SOS breaks the square root barrier, it is thanks to a spectral failure of pseudorandomness:

$$\lambda(G_p) \qquad \not\approx \qquad \lambda(\mathsf{ER})$$





Proof Idea

Also boils down to bounding $\|\boldsymbol{M}^H(G_p)\|$ for various H using $\operatorname{Tr} \boldsymbol{M}^H(G)^k$, but with different tools.

[AMP '16], [BHKKMP '19]: **combinatorics** from $\mathbb{E}[\operatorname{Tr} \boldsymbol{M}^H(\mathsf{ER})^k]$

[KY '22]: **character sums** from $\operatorname{Tr} \boldsymbol{M}^H(G_p)^k$

Proof Idea

Also boils down to bounding $\|\boldsymbol{M}^H(G_p)\|$ for various H using $\operatorname{Tr} \boldsymbol{M}^H(G)^k$, but with different tools.

[AMP '16], [BHKKMP '19]: **combinatorics** from $\mathbb{E}[\operatorname{Tr} \boldsymbol{M}^H(\mathsf{ER})^k]$

[KY '22]: **character sums** from $\operatorname{Tr} \boldsymbol{M}^H(G_p)^k$

For $\chi : \mathbb{F}_p \to \mathbb{C}$ the **Legendre symbol** character,

$$(\boldsymbol{A}_{G_p})_{i,j} = \left\{ \begin{array}{ll} +1 & \text{if } i \sim j \\ -1 & \text{if } i \not\sim j \end{array} \right\} = \chi(i - j),$$

so polynomials in χ appear in entries of $\boldsymbol{M}^H$. Not many good tools for handling $\operatorname{Tr} \boldsymbol{M}^H(G_p)^k$ character sums, but we can use other case-by-case tricks to mostly avoid these.

Character Sum Estimates

Typical, more classical, univariate example:

Theorem: (Weil) If $f \in \mathbb{F}_p[x]$ is not a multiple of a perfect square, then

$$\left| \sum_{a \in \mathbb{F}_p} \chi(f(a)) \right| \leq \deg f \cdot \sqrt{p}.$$

Character Sum Estimates

Typical, more classical, univariate example:

Theorem: (Weil) If $f \in \mathbb{F}_p[x]$ is not a multiple of a perfect square, then

$$\left| \sum_{a \in \mathbb{F}_p} \chi(f(a)) \right| \leq \deg f \cdot \sqrt{p}.$$

Describes square root cancellations: as though sum were of weakly correlated ± 1 signs.

Character Sum Estimates

Typical, more classical, univariate example:

Theorem: (Weil) If $f \in \mathbb{F}_p[x]$ is not a multiple of a perfect square, then

$$\left| \sum_{a \in \mathbb{F}_p} \chi(f(a)) \right| \leq \deg f \cdot \sqrt{p}.$$

Describes square root cancellations: as though sum were of weakly correlated ± 1 signs.

But we need the **much harder** multivariate case:

$$\left| \sum_{a_1, \ldots, a_k \in \mathbb{F}_p} \chi(f(a_1, \ldots, a_k)) \right| \overset{?}{\lesssim} \sqrt{p^k}.$$

III. Spectral Pseudorandomness

Generic MANOVA limit theorems for products of projections
[arXiv:2301.09543]

Next: How (spectrally) pseudorandom is G_p, if at all? Can we use this to prove clique number bounds?

The Localization Approach: Formulas [MMP '19]

The Localization Approach: Formulas [MMP '19]

G_p is **vertex transitive**, so there is a maximum clique that contains $0 \in \mathbb{F}_p$.

Defining $G_{p,\{0\}}$:= induced subgraph on $\{i : i \sim 0 \text{ in } G_p\}$,

$$\omega(G_p) = 1 + \omega(G_{p,\{0\}}).$$

The Localization Approach: Formulas [MMP ’19]

G_p is **vertex transitive**, so there is a maximum clique that contains $0 \in \mathbb{F}_p$.

Defining $G_{p,\{0\}}$:= induced subgraph on $\{i : i \sim 0 \text{ in } G_p\}$,

$$\omega(G_p) = 1 + \omega(G_{p,\{0\}}).$$

Why stop there? G_p is also **edge transitive**, so

$$\omega(G_p) = 2 + \omega(G_{p,\{0,1\}}).$$

The Localization Approach: Formulas [MMP '19]

G_p is **vertex transitive**, so there is a maximum clique that contains $0 \in \mathbb{F}_p$.

Defining $G_{p,\{0\}}$:= induced subgraph on $\{i : i \sim 0 \text{ in } G_p\}$,

$$\omega(G_p) = 1 + \omega(G_{p,\{0\}}).$$

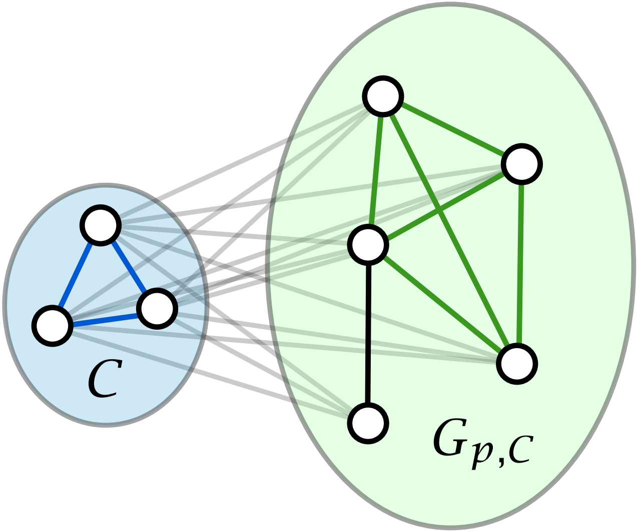
Why stop there? G_p is also **edge transitive**, so

$$\omega(G_p) = 2 + \omega(G_{p,\{0,1\}}).$$

Why stop there? We don't need transitivity; for any k,

$$\omega(G_p) = k + \max_{C \text{ a } k\text{-clique in } G_p} \omega(G_{p,C}).$$

Local Graphs



The Localization Approach: Bounds [MMP '19]

Now, can plug in our favorite clique number bounds and try to control those. [MMP '19] found empirically

$$\omega(G_p) \leq 1 + \mathsf{SOS}_2(G_{p,\{0\}}) \approx \sqrt{\frac{p}{2}} \quad \text{(state of the art!)}$$

The Localization Approach: Bounds [MMP '19]

Now, can plug in our favorite clique number bounds and try to control those. [MMP '19] found empirically

$$\omega(G_p) \le 1 + \mathsf{SOS}_2(G_{p,\{0\}}) \approx \sqrt{\frac{p}{2}} \quad \text{(state of the art!)}$$

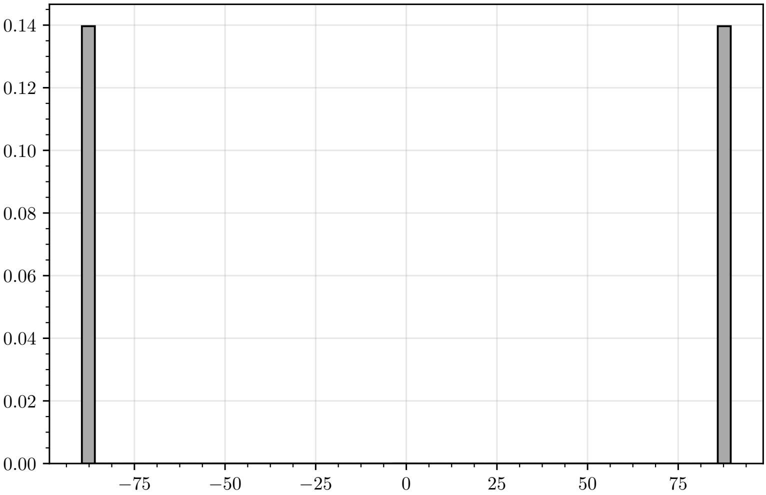
Even simpler is **spectral bound** (Haemers' variation on Hoffman's):

$$\omega(G_p) \le k + \max_{C \text{ a } k\text{-clique in } G_p} f(G_{p,C}),$$

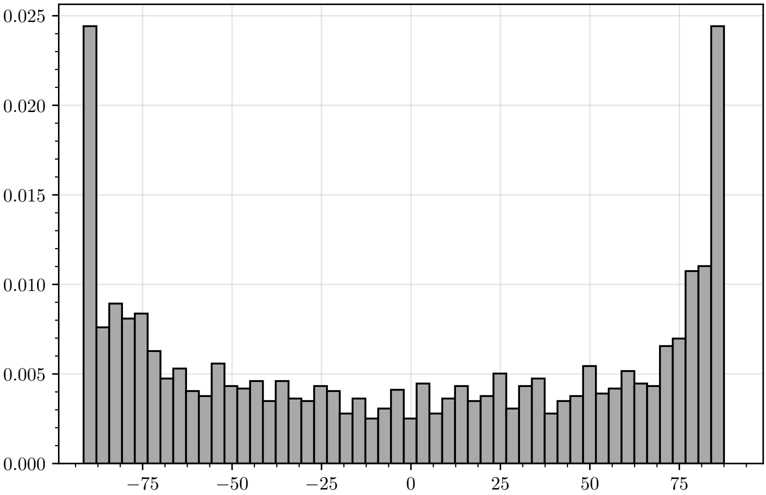
$$f(G) := |V(G)| \left(\frac{\min \deg(\overline{G})^2}{\max \deg(\overline{G}) \cdot |\lambda_{\min}(\overline{G})|} - 1 \right)^{-1}.$$

Main point: Enough to understand **spectrum** of the $G_{p,C}$.

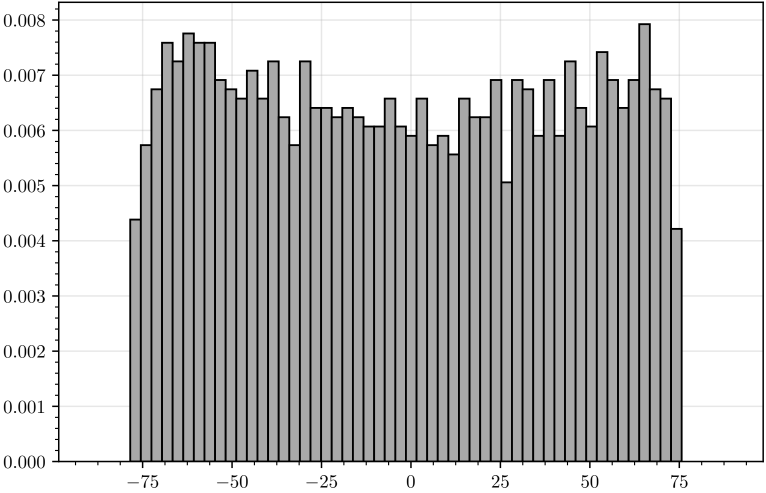
Experiments: $\lambda(G_p)$ ($p \approx 8000$)



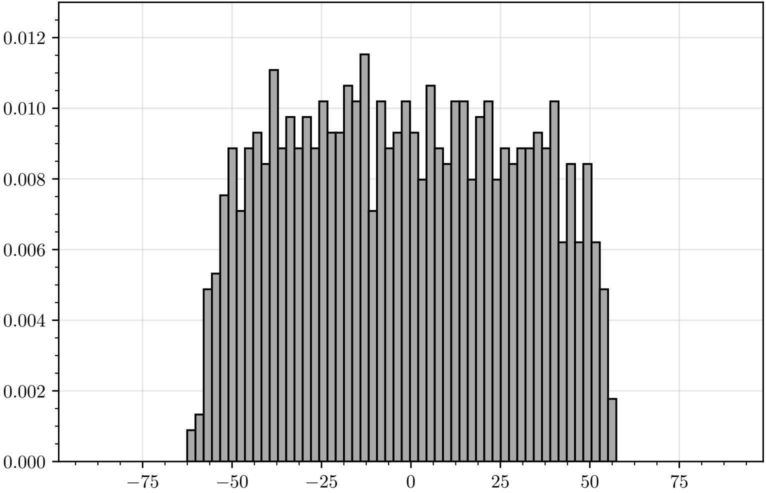
Experiments: $\lambda(G_{p,\{0\}})$



Experiments: $\lambda(G_{p,\{0,1\}})$



Experiments: $\lambda(G_{p,\{0,1,x\}})$



A Probabilist's Old Friend

Definition: The **Kesten-McKay law** with parameter $d \geq 2$ is

$$d\mu_{\mathsf{KM}(d)}(x) = \frac{d\sqrt{4(d-1)-x^2}}{2\pi(d^2-x^2)} \mathbb{1}\left\{|x| \leq 2\sqrt{d-1}\right\} dx$$

Also extends to $1 \leq d < 2$ by adding two atoms:

$$d\mu_{\mathsf{KM}(d)}(x) = (\cdots) + \frac{2-d}{2}\delta_{-d}(x) + +\frac{2-d}{2}\delta_d(x).$$

A Probabilist's Old Friend

Definition: The **Kesten-McKay law** with parameter $d \geq 2$ is

$$d\mu_{\mathsf{KM}(d)}(x) = \frac{d\sqrt{4(d-1) - x^2}}{2\pi(d^2 - x^2)} \mathbb{1}\left\{|x| \leq 2\sqrt{d-1}\right\} dx$$

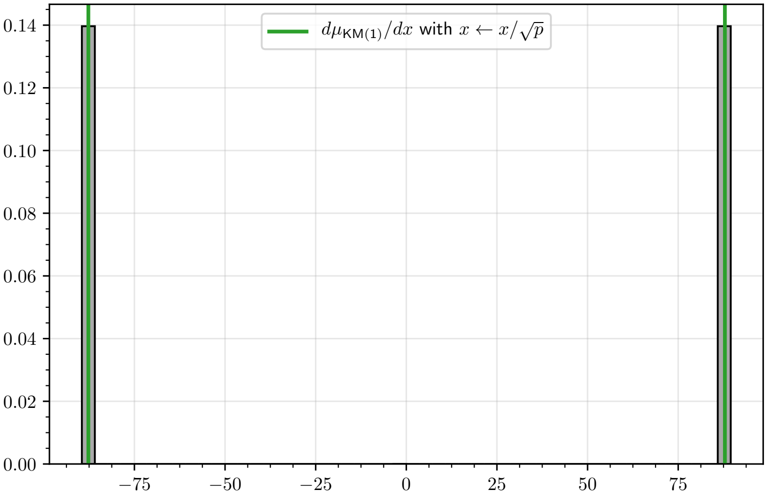
Also extends to $1 \leq d < 2$ by adding two atoms:

$$d\mu_{\mathsf{KM}(d)}(x) = (\cdots) + \frac{2-d}{2}\delta_{-d}(x) + + \frac{2-d}{2}\delta_{d}(x).$$

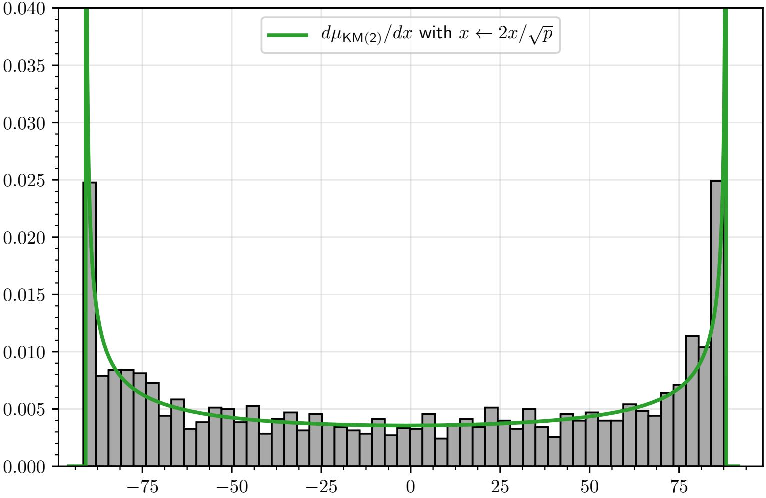
Observation: Up to rescaling and suitable shifting, empirical spectral distribution of $G_{p,C}$ looks like $\mu_{\mathsf{KM}(2^{|C|})}$.

Let's look...

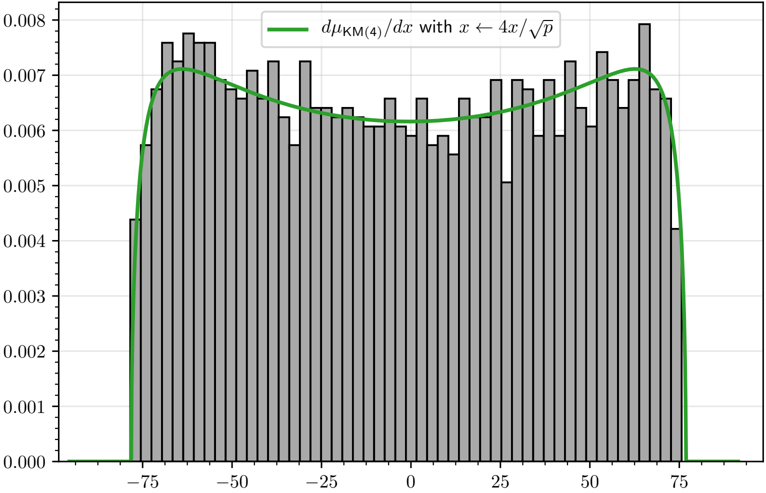
Experiments: $\lambda(G_p)$



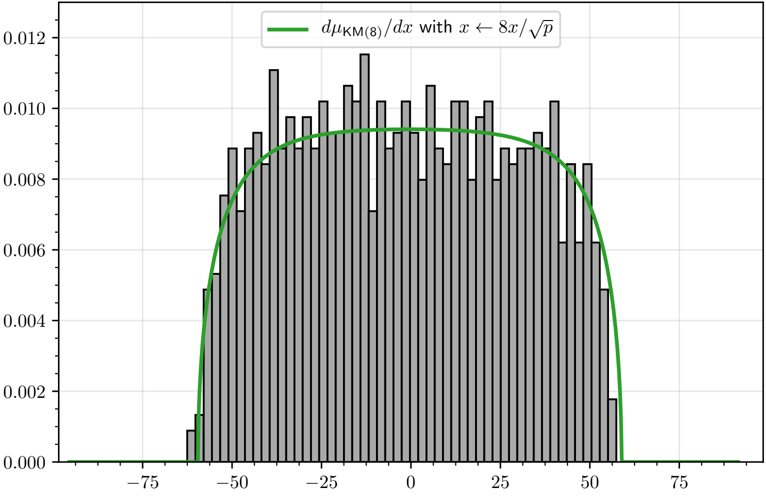
Experiments: $\lambda(G_{p,\{0\}})$



Experiments: $\lambda(G_{p,\{0,1\}})$



Experiments: $\lambda(G_{p,\{0,1,x\}})$



Why Does Kesten-McKay Appear?

Why Does Kesten-McKay Appear?

Related to its role in **free probability**:

Theorem: [Voiculescu ’90s] $\boldsymbol{D} \in \mathbb{R}^{N \times N}$ diagonal with $D_{ii} \overset{\mathsf{iid}}{\sim} \mathsf{Unif}(\{\pm 1\})$, $\boldsymbol{U} \sim \mathsf{Haar}(\mathcal{U}(N))$, and $\boldsymbol{M}$ a principal submatrix of $\boldsymbol{UDU}^*$ with each row/column included with probability $\alpha \in (0, 1]$. Then,

$$\text{rescaled empirical spectral distribution of } \boldsymbol{M} \Rightarrow \mu_{\mathsf{KM}(1/\alpha)}.$$

Why Does Kesten-McKay Appear?

Related to its role in **free probability**:

Theorem: [Voiculescu '90s] $\boldsymbol{D} \in \mathbb{R}^{N \times N}$ diagonal with $D_{ii} \stackrel{\text{iid}}{\sim} \mathsf{Unif}(\{\pm 1\})$, $\boldsymbol{U} \sim \mathsf{Haar}(\mathcal{U}(N))$, and $\boldsymbol{M}$ a principal submatrix of $\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^*$ with each row/column included with probability $\alpha \in (0, 1]$. Then,

$$\text{rescaled empirical spectral distribution of } \boldsymbol{M} \Rightarrow \mu_{\mathsf{KM}(1/\alpha)}.$$

$\boldsymbol{P}$ diagonal with $P_{ii} \stackrel{\text{iid}}{\sim} \mathsf{Ber}(\alpha) \rightsquigarrow \boldsymbol{M} = \boldsymbol{P}\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^*\boldsymbol{P}$.

Why Does Kesten-McKay Appear?

Related to its role in **free probability**:

Theorem: [Voiculescu '90s] $\boldsymbol{D} \in \mathbb{R}^{N \times N}$ diagonal with $D_{ii} \overset{\text{iid}}{\sim} \mathsf{Unif}(\{\pm 1\})$, $\boldsymbol{U} \sim \mathsf{Haar}(\mathcal{U}(N))$, and $\boldsymbol{M}$ a principal submatrix of $\boldsymbol{UDU}^*$ with each row/column included with probability $\alpha \in (0, 1]$. Then,

rescaled empirical spectral distribution of $\boldsymbol{M} \Rightarrow \mu_{\mathsf{KM}(1/\alpha)}$.

$\boldsymbol{P}$ diagonal with $P_{ii} \overset{\text{iid}}{\sim} \mathsf{Ber}(\alpha) \rightsquigarrow \boldsymbol{M} = \boldsymbol{PUDU}^*\boldsymbol{P}$.

$\boldsymbol{P}$ and $\boldsymbol{UDU}^*$ are **asymptotically free** $\Longrightarrow$ Theorem.

Why Does Kesten-McKay Appear?

Related to its role in **free probability**:

Theorem: [Voiculescu '90s] $\boldsymbol{D} \in \mathbb{R}^{N \times N}$ diagonal with $D_{ii} \overset{\text{iid}}{\sim} \mathsf{Unif}(\{\pm 1\})$, $\boldsymbol{U} \sim \mathsf{Haar}(\mathcal{U}(N))$, and $\boldsymbol{M}$ a principal submatrix of $\boldsymbol{UDU}^*$ with each row/column included with probability $\alpha \in (0, 1]$. Then,

$$\text{rescaled empirical spectral distribution of } \boldsymbol{M} \Rightarrow \mu_{\mathsf{KM}(1/\alpha)}.$$

$\boldsymbol{P}$ diagonal with $P_{ii} \overset{\text{iid}}{\sim} \mathsf{Ber}(\alpha) \rightsquigarrow \boldsymbol{M} = \boldsymbol{PUDU}^*\boldsymbol{P}$.

$\boldsymbol{P}$ and $\boldsymbol{UDU}^*$ are **asymptotically free** $\Longrightarrow$ Theorem.

Idea: **derandomize** this model (in $\boldsymbol{U}, \boldsymbol{D}, \boldsymbol{P}$).

Spectral Pseudorandomness for Local Graphs

Observe that

$$\boldsymbol{A}_{G_{p,C}} = \boldsymbol{P}_{G_{p,C}} \boldsymbol{A}_{G_p} \boldsymbol{P}_{G_{p,C}}.$$

Spectral Pseudorandomness for Local Graphs

Observe that

$$\boldsymbol{A}_{G_{p,C}} = \boldsymbol{P}_{G_{p,C}} \boldsymbol{A}_{G_p} \boldsymbol{P}_{G_{p,C}}.$$

Intuition: $G_{p,C}$ is a pseudorandom induced subgraph, like vertices were chosen independently with probability $\alpha = 1/2^{|C|}$ ($|C|$ "independent" adjacency relations).

Spectral Pseudorandomness for Local Graphs

Observe that

$$\boldsymbol{A}_{G_{p,C}} = \boldsymbol{P}_{G_{p,C}} \boldsymbol{A}_{G_p} \boldsymbol{P}_{G_{p,C}}.$$

Intuition: $G_{p,C}$ is a pseudorandom induced subgraph, like vertices were chosen independently with probability $\alpha = 1/2^{|C|}$ ($|C|$ "independent" adjacency relations).

Gradual derandomization of asymptotic freeness result:

Reference	Matrix	Intuition
[V '90s]	$\boldsymbol{PUDU^*P}$	
[MMP '19]	$\boldsymbol{P}\boldsymbol{A}_{G_p}\boldsymbol{P}$	pseudorandom eigenspaces
[K '23]	$\boldsymbol{P}_{G_{p,C}}\boldsymbol{A}_{G_p}\boldsymbol{P}_{G_{p,C}}$	pseudorandom vertex set

Precise Statement

Theorem: [K '23] Conditional on a family of natural Legendre symbol character sum estimates, for any sequence $C_p \subset V(G_p)$ of cliques with $|C_p| = k$,

$$\text{rescaled e.s.d. of } \pm 1 \text{ adjacency matrix of } G_{p,C_p} \Rightarrow \mu_{\mathsf{KM}(2^k)}.$$

Can prove estimates for $k = 1$, and make progress for $k = 2$.

Pseudorandomness at the Edges

Pseudorandomness at the Edges

Conjecture: For any $C_p \subset V(G_p)$ cliques with $|C_p| = k$,

rescaled $\lambda_{\mathsf{min}}(\pm 1 \text{ adj. matrix of } G_{p,C_p})$
$\geq$ left edge of $\mu_{\mathsf{KM}(2^k)} - o(1)$,

rescaled $\lambda_{\mathsf{max}}(\pm 1 \text{ adj. matrix of } G_{p,C_p})$
$\leq$ right edge of $\mu_{\mathsf{KM}(2^k)} + o(1)$.

Pseudorandomness at the Edges

Conjecture: For any $C_p \subset V(G_p)$ cliques with $|C_p| = k$,

rescaled $\lambda_{\mathsf{min}}(\pm 1$ adj. matrix of $G_{p,C_p})$
$\geq$ left edge of $\mu_{\mathsf{KM}(2^k)} - o(1)$,

rescaled $\lambda_{\mathsf{max}}(\pm 1$ adj. matrix of $G_{p,C_p})$
$\leq$ right edge of $\mu_{\mathsf{KM}(2^k)} + o(1)$.

Would imply, for any given constant k,

$$\omega(G_p) \leq k + \frac{\sqrt{2^k - 1}}{2^{k-1}}\sqrt{p} + o(\sqrt{p}) \approx 2^{-k/2}\sqrt{p}.$$

Already $k = 3$ would beat state of the art! And arbitrary k would show $\omega(G_p) = o(\sqrt{p})$, "denting" the $\sqrt{p}$ barrier.

Starting to Analyze the Edges

Edge behavior even for the classical free probability model only established using **fragile** “integrable” tools.

Starting to Analyze the Edges

Edge behavior even for the classical free probability model only established using **fragile** "integrable" tools.

Theorem: [K '23] In Voiculescu's model, $\boldsymbol{M}$ = random submatrix of $\boldsymbol{UDU}^*$ with inclusion probability α,

$$\begin{aligned} \lambda_{\mathsf{max}}(\boldsymbol{M}) &\to \text{ right edge of } \mu_{\mathsf{KM}(1/\alpha)}, \\ \lambda_{\mathsf{min}}(\boldsymbol{M}) &\to \text{ left edge of } \mu_{\mathsf{KM}(1/\alpha)}. \end{aligned}$$

Starting to Analyze the Edges

Edge behavior even for the classical free probability model only established using **fragile** “integrable” tools.

Theorem: [K ’23] In Voiculescu’s model, $\boldsymbol{M}$ = random submatrix of $\boldsymbol{UDU}^*$ with inclusion probability α,

$$\lambda_{\mathsf{max}}(\boldsymbol{M}) \;\to\; \text{right edge of } \mu_{\mathsf{KM}(1/\alpha)},$$
$$\lambda_{\mathsf{min}}(\boldsymbol{M}) \;\to\; \text{left edge of } \mu_{\mathsf{KM}(1/\alpha)}.$$

New proof combines **robust** trace method with recent tools [CM ’17]: entry moments of $\boldsymbol{U}$ given by Weingarten function; tools give non-asymptotic bounds.

Starting to Analyze the Edges

Edge behavior even for the classical free probability model only established using **fragile** “integrable” tools.

Theorem: [K ’23] In Voiculescu’s model, $\boldsymbol{M}$ = random submatrix of $\boldsymbol{UDU}^*$ with inclusion probability α,

$$\lambda_{\mathsf{max}}(\boldsymbol{M}) \;\to\; \text{right edge of } \mu_{\mathsf{KM}(1/\alpha)},$$
$$\lambda_{\mathsf{min}}(\boldsymbol{M}) \;\to\; \text{left edge of } \mu_{\mathsf{KM}(1/\alpha)}.$$

New proof combines **robust** trace method with recent tools [CM ’17]: entry moments of $\boldsymbol{U}$ given by Weingarten function; tools give non-asymptotic bounds.

$\rightsquigarrow$ long but plausible road to the case of deterministic $\boldsymbol{M}$.

Open Questions

1. If $\mathsf{SOS}_4(G_p) \lesssim p^{1/2-\varepsilon}$, how to extract formal proofs from SOS numerics or graph matrix computations?

Open Questions

1. If $\mathsf{SOS}_4(G_p) \lesssim p^{1/2-\varepsilon}$, how to extract formal proofs from SOS numerics or graph matrix computations?

2. Higher degrees of SOS relaxation?

Open Questions

1. If $\mathsf{SOS}_4(G_p) \lesssim p^{1/2-\varepsilon}$, how to extract formal proofs from SOS numerics or graph matrix computations?

2. Higher degrees of SOS relaxation?

---

3. Proof techniques to analyze **edge of spectrum** for matrix models with less and less randomness?

Open Questions

1. If $\mathsf{SOS}_4(G_p) \lesssim p^{1/2-\varepsilon}$, how to extract formal proofs from SOS numerics or graph matrix computations?

2. Higher degrees of SOS relaxation?

---

3. Proof techniques to analyze **convex relaxations** for matrix models with less and less randomness?

Open Questions

1. If $\mathsf{SOS}_4(G_p) \lesssim p^{1/2-\varepsilon}$, how to extract formal proofs from SOS numerics or graph matrix computations?

2. Higher degrees of SOS relaxation?

---

3. Proof techniques to analyze **convex relaxations** for matrix models with less and less randomness?

4. What other classical questions can be answered through **pseudorandomness (phenomenon)** leveraged via **convex relaxation (proof technique)**?

Thank you!