Positive spectrahedra:

Invariance principles and PRGs

Srinivasan Arunachalam (IBM Research)

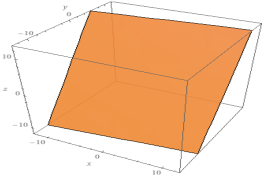
joint with Penghui Yao (Nanjing University)

Linear programs

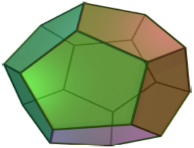
- Optimizing a linear function over a polytope
- A general LP has the form: $w^1, \dots, w^k, c \in \mathbb{R}^n$ and $\theta^i \in \mathbb{R}$

$$\mathrm{OPT} = \max_{x \in \mathbb{R}^n} \{c^T x : w^1 \cdot x \leq \theta^1, \dots, w^k \cdot x \leq \theta^k\}$$

- Efficiently solvable!



- Halfspace in $\mathbb{R}^n$ is a constraint that divides the space, i.e., $h_1 : \mathbb{R}^n \to \{0, 1\}$
- Let $w \in \mathbb{R}^n$ and $x \in \{-1, 1\}^n$, then a halfspace $h_1(x) = 1$ iff $w \cdot x \leq \theta$, or $h_1(x) = [w \cdot x \leq \theta]$



- **Polytope** is an intersection of halfspaces
- Let $w^i \in \mathbb{R}^n$, $\theta^i \in \mathbb{R}$, a k-facet polytope is

$$P = \{x : h_1(x) \wedge h_2(x) \wedge \dots \wedge h_k(x)\}$$

where $h_i = [w^i \cdot x \leq \theta^i]$

Applications: Optimization, combinatorics, geometry, computational complexity, ...

Semi-definite programs

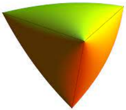
What is an SDP?

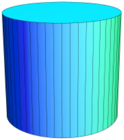
- Optimizing a linear function over a spectrahedron
- A general SDP has the form: $W^1, \dots, W^k, B \in \mathrm{Sym}_n$

$$\mathrm{OPT} = \max_{x \in \mathbb{R}^n} \{c^T x : x_1 W^1 + \dots + x_n W^n \preceq B\},$$

where $C \preceq D$ means $D - C$ is PSD (i.e., all eigenvalues are ≥ 0)

How does it look?

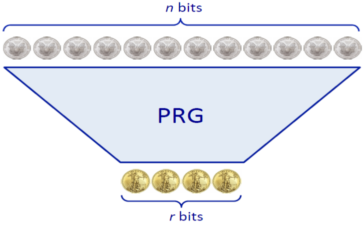




- Generalizes linear programs and still efficiently solvable!
- Unfortunately, spectrahedra are not very well understood!
- But SDPs have found applications in approximation theory, SoS heirarchy, quantum computing

Pseudorandom generators

A PRG is a function that "expands" randomness



PRGs for a class of functions

An ε-PRG for $\mathcal{C} \subseteq \{F : \{0,1\}^n \to \{0,1\}\}$ is a function $G : \{0,1\}^r \to \{0,1\}^n$ such that

$$\text{for every } F \in \mathcal{C}, \qquad \left| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mathcal{U}_r}[F(G(\boldsymbol{x}))] - \mathop{\mathbb{E}}_{\boldsymbol{u}\sim\mathcal{U}_n}[F(\boldsymbol{u})] \right| \leq \varepsilon.$$

The seed length of G is r. **Goal** is to have $r = \text{polylog}(\cdot)$ in all relevant parameters

Holy grail. Can we design a PRG against the class of polynomial sized circuits unconditionally? If so, would imply BPP $=$ P

PRGs for geometric objects. Constructing PRGs using geometric properties has been a *rich* area of study this work.

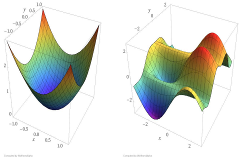
Some PRGs for geometric objects

Halfspaces

- Diakonikolas et al.'09
- Meka, Zuckerman'09
- Karnin, Rabani, Shpilka'11
- Kothari, Meka'15
- Gopalan, Kane, Meka'15

Polytopes

- Harsha, Klivans, Meka'13
- Gopalan et al.'13
- Servedio, Tan'17
- O'Donnell, Servedio, Tan'19



Polynomial Threshold function
$T(x) = \text{sign}(p(x_1, \ldots, x_n))$ where p is a polynomial

- Meka, Zuckerman'09
- Diakonikolas'10
- Kane'11, Kane'12, Kane'13
- Kane, Meka'14
- O'Donnell, Servedio, Tan'20

Spectrahedra: generalization of halfspaces, polytopes and PTFs in one framework

In this work: Can we construct PRGs for spectrahedra?

Results

Recall. Spectrahedron is the set $S = \left\{x \in \{-1,1\}^n : \sum_i x_i A^i \preceq B\right\}$.

1. Positive: $A^1, \ldots, A^n, B$ are $k \times k$ PSD matrices
2. Bounded width: $\mathbb{I} \preceq \sum_i (A^i)^2 \preceq M \cdot \mathbb{I}$
3. Regular: $(A^i) \preceq \tau \cdot \mathbb{I}$ for every i

Main Theorem

There exists a PRG $G : \{0,1\}^r \to \{-1,1\}^n$ with seed length

$$r = (\log n) \cdot \mathrm{poly}\left(\log k \cdot M \cdot 1/\delta\right),$$

that δ-fools the class of positive bounded width regular spectrahedron S, i.e.,

$$\left| \underset{\boldsymbol{x}\sim\mathcal{U}_r}{\mathbb{E}}[G(\boldsymbol{x}) \in S] - \underset{\boldsymbol{u}\sim\mathcal{U}_n}{\mathbb{E}}[\boldsymbol{u} \in S] \right| \leq \delta.$$

Main technical contributions: Rest of this talk

An invariance principle for *positive* regular spectrahedra

How to fool: Meka-Zuckerman Invariance principles

Punchline: Invariance principles give pseudorandom generators.

What is an invariance principle? Generalization of Berry-Esseen theorem

Standard central limit theorem states: suppose $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are random variables satisfying $\mathbb{E}[\boldsymbol{x}] = 0$ and $\mathrm{Var}[\boldsymbol{x}^2] = 1$, then

$$\frac{\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n}{\sqrt{n}} \longrightarrow \boldsymbol{g}(0,1),$$

where $\boldsymbol{g}(0,1)$ is a Gaussian

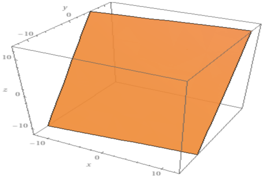
But what about convergence? Berry-Esseen states that for every $u \in \mathbb{R}$

$$\Pr\left[\frac{\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_n}{\sqrt{n}} \leq u\right] - \Pr\left[\boldsymbol{g}(0,1) \leq u\right] \leq \frac{C}{\sqrt{n}},$$

for "C-nice" $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. Proved using the Lindeberg method'22 (aka hybrid method)

Invariance principles: understanding in the Gaussian space is similar to Boolean space

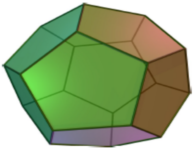
How was M-Z used so far?



Halfspace (Meka-Zuckerman'09)

- Halfspace is $\left\{x \in \{-1,1\}^n : \sum_i w_i x_i \leq \theta\right\}$
- For smooth $w \in \mathbb{R}^n$

$$\sum_i w_i \boldsymbol{x}_i \to \boldsymbol{g}(0,1)$$



Polytope (Harsha-Klivans-Meka'13)

- Polytope is

$$\left\{x \in \{-1,1\}^n : w^1 \cdot x \leq \theta_1, \ldots, w^k \cdot x \leq \theta_k\right\}$$

- Let $w^1, \ldots, w^k \in \mathbb{R}^n$ all be smooth, then

$$\begin{bmatrix} — & w^1 & — \\ — & w^2 & — \\ & \vdots & \\ — & w^k & — \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_n \end{bmatrix} \to \begin{bmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_k \end{bmatrix}$$

- Recently OST'19 removed regularity

Establishing the invariance principle

Recall: Polytope $F(x) = \left[w^1 \cdot x \leq \theta_1 \wedge \cdots \wedge w^k \cdot x \leq \theta_k\right]$ or $W \cdot x \leq \vec{\theta}$

Main result of HKM'13 Invariance principle for τ-regular polytopes (i.e., $\|w^i\| \leq \tau$)

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x} \sim \mathcal{U}_n}[W\boldsymbol{x} \leq \vec{\theta}] - \mathop{\mathbb{E}}_{\boldsymbol{g} \sim \mathcal{G}^n}[W\boldsymbol{g} \leq \vec{\theta}] \right| \leq \tau \operatorname{polylog} k \tag{1}$$

How to prove this?

1. Smooth invariance. Establish (1) for smooth functions $\mathcal{O} : \mathbb{R}^k \to \mathbb{R}$, i.e.,

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x} \sim \mathcal{U}_n}[\mathcal{O}(W\boldsymbol{x})] - \mathop{\mathbb{E}}_{\boldsymbol{g} \sim \mathcal{G}^n}[\mathcal{O}(W\boldsymbol{g})] \right| \leq \tau \log k \cdot \|\mathcal{O}^{(3)}\|_1$$

- Lindeberg method: Write out Taylor series for $\mathcal{O} : \mathbb{R}^k \to \mathbb{R}$, since $\mathcal{U}_n$ and $\mathcal{G}^n$ have matching first and second moments, we get 3rd derivatives, hence $\|\mathcal{O}^{(3)}\|_1$
- Since O is smooth, all derivatives are "small" so $\|O^{(3)}\|_1$ is also "small"

Establishing the invariance principle

Main result of HKM'13 Invariance principle for τ-regular polytopes

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mathcal{U}_n}[W\boldsymbol{x} \le \vec{\theta}] - \mathop{\mathbb{E}}_{\boldsymbol{g}\sim\mathcal{G}^n}[W\boldsymbol{g} \le \vec{\theta}] \right| \le \tau \,\mathrm{polylog}\, k \qquad (2)$$

How to prove this?

1. Smooth invariance. Establish (2) for smooth mollifiers $\mathcal{O} : \mathbb{R}^n \to \mathbb{R}$, i.e.,

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mathcal{U}_n}[\mathcal{O}(W\boldsymbol{x})] - \mathop{\mathbb{E}}_{\boldsymbol{g}\sim\mathcal{G}^n}[\mathcal{O}(W\boldsymbol{g})] \right| \le \tau \log k \cdot \|\mathcal{O}^{(3)}\|_1 \qquad (3)$$

2. Bentkus mollifier. Care about $[W\boldsymbol{x} \le \theta]$ **not** $\mathcal{O}(W\boldsymbol{x})$. Bentkus'90 established a mollifier $\mathcal{B} : \mathbb{R}^k \to \mathbb{R}$ that approximates the orthant function, i.e.,

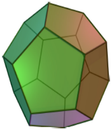
$$\mathcal{B}(z_1, \ldots, z_k) \approx \left[\max_i z_i \le \theta \right] \quad \text{and } \|\mathcal{B}^{\ell}\|_1 \le \log^{\ell/2} k$$

3. Anti-concentration. From above $\mathcal{B}$ "approximately agrees" with $\mathcal{O}$.

- Around the "boundary" of the polytope is where $\mathcal{B}$ and $\mathcal{O}$ disagree
- If probability of $x \in \mathcal{G}^n$ lying in boundary is "small", maybe it is ok? YES
- Gaussian surface area! Nazarov'03 showed GSA of k-facet polytopes is $\sqrt{\log k}$

Putting everything together. All dependence are logarithmic factors, so (3) $\implies$ (2).

A halfspace $F(x) = \left[\sum_i w_i x_i \leq \theta\right]$. Spectrahedron is $F(x) = \left[x_1 A^1 + \cdots + x_n A^n \preceq B\right]$



1. Hybrid method?

1. Spectrahedron naturally deals with eigenvalues of matrices
2. Unknown if Lindeberg-type argument works for spectral mollifiers (i.e., smooth functions acting on the eigenspectrum of matrices)

An invariance principle for the Bentkus mollifier of *arbitrary* regular spectrahedra

2. Anti-concentration? Even if GSA of spectrahedra are small, they are "funky" geometric objects, not clear how to go from mollifier-closeness to CDF closeness

Prove a Littlewood-Offord theorem for positive regular spectrahedra

Invariance principle: two new definitions

1. Spectral function $f : \mathbb{R}^{n\times n} \to \mathbb{R}$ acts on the eigenvalues of matrices:

$$f(M) = g \circ \lambda(M) = g\big(\lambda_1(M), \ldots, \lambda_n(M)\big)$$

for some $g : \mathbb{R}^n \to \mathbb{R}$. Examples include determinants, trace, matrix norms

2. Derivatives of matrix-valued functions $f : \mathbb{R}^{n\times n} \to \mathbb{R}^{m\times m}$.
Taylor series. Let $h : \mathbb{R} \to \mathbb{R}$, then Taylor series of h is

$$h(x) = h(a) + \frac{h'(a)}{1!}(x-a) + \frac{h''(a)}{2!}(x-a)^2 + \frac{h'''(a)}{3!}(x-a)^3 + \cdots,$$

where

$$h'(a) = \lim_{s\to 0} \frac{1}{s} \cdot \big(h(a+s) - h(a)\big)$$

Fréchet derivatives. Derivatives in Banach spaces. "Similar" to standard calculus. For $A, B \in \mathbb{R}^{n\times n}$, we have

$$Df(A)[B] = \lim_{s\to 0} \frac{1}{s} \cdot \big(f(A+sB) - f(A)\big),$$

$$D^t f(A)[B] = \lim_{s\to 0} \frac{1}{s} \cdot \big(D^{t-1} f(A+sB)[B] - D^{t-1} f(A)[B]\big)$$

Fréchet derivatives are hard to compute. Poorly understood: basic properties as continuity, Lipschitz continuity, differentiability proven in last 2 decades.

Invariance principle: Part I

Goal: Invariance principle for Bentkus mollifier $\mathcal{B}$

$$\left| \Pr_{\boldsymbol{x}\sim\mathcal{U}_n}[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B)] - \Pr_{\boldsymbol{g}\sim\mathcal{G}^n}[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{g}_i A^i - B)] \right| \leq \tau \operatorname{polylog} k$$

1. **Hybrid method.** Hash the sum over $[n]$ into t blocks: let $Q_{\boldsymbol{x}} = \sum_{i=1}^{n/t} \boldsymbol{x}_i A^i$,

$$\left| \mathbb{E}_{\boldsymbol{x},\boldsymbol{g}}[(\mathcal{B}\circ\lambda)\big(Q_{\boldsymbol{x}} + P_{\boldsymbol{x},\boldsymbol{g}}\big)] - \mathbb{E}_{\boldsymbol{x},\boldsymbol{g}}[(\mathcal{B}\circ\lambda)\big(Q_{\boldsymbol{g}} + P_{\boldsymbol{x},\boldsymbol{g}}\big)] \right| \tag{4}$$

2. **Taylor expansion.** Write out Fréchet series for both these terms.

$$\mathcal{B}_\lambda\big(Q_{\boldsymbol{x}} + P_{\boldsymbol{x},\boldsymbol{g}}\big) = \mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}}) + D\mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}] + \frac{1}{2}D^2\mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}] + \frac{1}{6}D^3\mathcal{B}_\lambda(P'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}]$$

$$\mathcal{B}_\lambda\big(Q_{\boldsymbol{g}} + P_{\boldsymbol{x},\boldsymbol{g}}\big) = \mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}}) + D\mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}] + \frac{1}{2}D^2\mathcal{B}_\lambda(P_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}] + \frac{1}{6}D^3\mathcal{B}_\lambda(R'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}]$$

Same colour terms are equal in expectation

So bounding Eq (4) amounts to proving. **Goal**: upper bound

$$\left| \mathbb{E}_{\boldsymbol{x},\boldsymbol{g}}\left[D^3\mathcal{B}_\lambda(P'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}] - D^3\mathcal{B}_\lambda(R'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}]\right] \right| \leq \tau \operatorname{polylog} k$$

3. **Sendov to the rescue.** For us, Sendov provided a tensorial representation of Fréchet series for spectral functions

Invariance principle: Part II

Recall: Goal is to upper bound

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x},\boldsymbol{g}} \left[D^3\mathcal{B}_\lambda(P'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}] - D^3\mathcal{B}_\lambda(R'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}] \right] \right|$$

Hope: use Sendov's tensor-result. BUT, if you write it out, we get:

$H = VQV^T$. Then $D^3F(P)[Q,Q,Q]$ *is the summation of the following terms.*

1. $\sum_{i_1} \nabla^3_{i_1,i_1,i_1} f(x) H^3_{i_1,i_1}$
2. $\sum_{i_1 \neq i_2} \nabla^3_{i_1,i_2,i_1} f(x) H^2_{i_1,i_1} H_{i_2,i_2}$
3. $\sum_{i_1 \neq i_2 \neq i_3} (\nabla^3_{i_1,i_2,i_2} f(x)) \cdot H_{i_1,i_1} H_{i_2,i_2} H_{i_3,i_3}$

DIAGONAL ELEMENTS

4. $\sum_{i_1 \neq i_2} \left(\frac{\nabla^2_{i_2,i_2} - \nabla^2_{i_1,i_2}}{x_{i_2} - x_{i_1}} - \frac{\nabla_{i_2} - \nabla_{i_1}}{(x_{i_2} - x_{i_1})^2} \right) f(x) H_{i_2,i_2} H^2_{i_2,i_1}$
5. $\sum_{i_1 \neq i_2 \neq i_3} \frac{\nabla^2_{i_2,i_3} - \nabla^2_{i_1,i_3}}{x_{i_2} - x_{i_1}} f(x) H^2_{i_1,i_2} H_{i_3,i_3}$
6. $\sum_{i_1 \neq i_2 \neq i_3} \left(\frac{\nabla_{i_3} - \nabla_{i_1}}{(x_{i_3} - x_{i_2})(x_{i_3} - x_{i_1})} - \frac{\nabla_{i_2} - \nabla_{i_1}}{(x_{i_3} - x_{i_2})(x_{i_2} - x_{i_1})} \right) f(x) H_{i_1,i_2} H_{i_2,i_3} H_{i_3,i_1}$
7. $\sum_{i_1 \neq i_2 \neq i_3} \left(\frac{\nabla_{i_2} - \nabla_{i_3}}{(x_{i_3} - x_{i_1})(x_{i_2} - x_{i_3})} - \frac{\nabla_{i_2} - \nabla_{i_1}}{(x_{i_3} - x_{i_1})(x_{i_2} - x_{i_1})} \right) f(x) H_{i_1,i_3} H_{i_2,i_1} H_{i_3,i_2},$

Invariance principle: Part II

Recall: Goal is to upper bound

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x},\boldsymbol{g}} \left[D^3\mathcal{B}_\lambda(P'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}, Q_{\boldsymbol{x}}] - D^3\mathcal{B}_\lambda(R'_{\boldsymbol{x},\boldsymbol{g}})[Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}, Q_{\boldsymbol{g}}] \right] \right|$$

Technical contribution.

- Bound each of the 7 terms by polylog k times norms of $Q_{\boldsymbol{g}}, Q_{\boldsymbol{x}}, P'_{\boldsymbol{x},\boldsymbol{g}}, R'_{\boldsymbol{x},\boldsymbol{g}}$.
- Completely open up the Bentkus mollifier (prior works used it as a blackbox)

4. Final step. Understand $\mathbb{E}_x[\|Q_{\boldsymbol{x}}\|_4^4]$ and similar quantities.

- We use matrix Rosenthal's inequality (proved "recently") gives good concentration for Schatten norms of $\|\sum_i \boldsymbol{x}_i A^i\|_p^p$
- Also matrix Rosenthal is true when $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ is p-wise independent

Putting everything together.

$$\left| \Pr_{\boldsymbol{x}\sim\mathcal{U}_n}[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B)] - \Pr_{\boldsymbol{g}\sim\mathcal{G}^n}[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{g}_i A^i - B)] \right| \leq \tau \cdot \text{polylog } k$$

Anticoncentration

Recall: positive spectrahedron $\mathcal{S} = \{x : x_1 A^1 + \cdots + x_n A^n \preceq B\}$ where $A^i, B \succeq 0$

So far.

$$\left| \underbrace{\Pr_{\boldsymbol{x}\sim\mathcal{U}_n}\left[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B)\right]}_{\approx\left[\sum_i \boldsymbol{x}_i A^i \preceq B\right]} - \underbrace{\Pr_{\boldsymbol{g}\sim\mathcal{G}^n}\left[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{g}_i A^i - B)\right]}_{\approx\left[\sum_i \boldsymbol{g}_i A^i \preceq B\right]} \right| \le \text{polylog}\, k \qquad (5)$$

But we care about CDF distance

$$\left| \Pr_{\boldsymbol{x}\sim\mathcal{U}_n}\left[\sum_i \boldsymbol{x}_i A^i \preceq B\right] - \Pr_{\boldsymbol{g}\sim\mathcal{G}^n}\left[\sum_i \boldsymbol{g}_i A^i \preceq B\right] \right| \le \text{polylog}\, k \qquad (6)$$

Intuition for this approximation: What $\approx$ means?

If $\lambda_1, \ldots, \lambda_k \in [-1/100, 1/100]$, then $(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B) \not\approx \left[\sum_i \boldsymbol{x}_i A^i \preceq B\right]$

Else $\lambda_1, \ldots, \lambda_k \notin [-1/100, 1/100]$, then $(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B) \approx \left[\sum_i \boldsymbol{x}_i A^i \preceq B\right]$

For uniform $\boldsymbol{x}$, $\lambda_{\max}\left(\sum_i \boldsymbol{x}_i A^i - B\right) \in [-\frac{1}{100}, \frac{1}{100}]$ with tiny probability

Recall: positive spectrahedron $\mathcal{S} = \{x : x_1 A^1 + \cdots + x_n A^n \preceq B\}$ where $A^i, B \succeq 0$

So far.

$$\left| \underbrace{\Pr_{\boldsymbol{x}\sim\mathcal{U}_n}\left[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{x}_i A^i - B) \right]}_{\approx\left[\sum_i \boldsymbol{x}_i A^i \preceq B\right]} - \underbrace{\Pr_{\boldsymbol{g}\sim\mathcal{G}^n}\left[(\mathcal{B}\circ\lambda)(\sum_i \boldsymbol{g}_i A^i - B) \right]}_{\approx\left[\sum_i \boldsymbol{g}_i A^i \preceq B\right]} \right| \leq \text{polylog } k \qquad (7)$$

But we care about CDF distance

$$\left| \Pr_{\boldsymbol{x}\sim\mathcal{U}_n}\left[\sum_i \boldsymbol{x}_i A^i \preceq B \right] - \Pr_{\boldsymbol{g}\sim\mathcal{G}^n}\left[\sum_i \boldsymbol{g}_i A^i \preceq B \right] \right| \leq \text{polylog } k \qquad (8)$$

Our result: Littlewood-Offord for spectrahedra

Let $A^1, \ldots, A^n$ be positive matrices s.t. $\sum_i \|A^i\|^2 \geq 1$. For every Λ

$$\Pr_{\boldsymbol{x}\sim\mathcal{U}_n}\left[\lambda_{\max}\left(\sum_i \boldsymbol{x}_i A^i - B \right) \in [-\Lambda, \Lambda] \right] \leq O(\Lambda).$$

Prior: Littlewood-Offord'43, Erdős'45 proved it for halfspaces, OST'19 for polytopes

Hence (7) implies (8) except tiny probability. Done!

Conclusion and open questions

Recall: positive spectrahedron $F(x) = \left[x_1 A^1 + \cdots + x_n A^n \preceq B\right]$ where $A^i, B \succeq 0$

A PRG that δ-fools the class of positive width-M spectrahedra with seed length $\mathrm{poly}(\log n, \log k, M, 1/\delta)$

Open questions:

1. Remove regularity?
2. Remove positivity?
3. What is the Gaussian surface area of spectrahedron?
4. Improve the $1/\delta$ dependence?
5. A general invariance principle for spectral functions?

THANK YOU