Spies and Traitors: Random Matrix Kaleidoscopes and their Turncoat Eigenvalues

UMass REU Conf

Neelima Borade and Renyuan Ma

(nborad2@uic.edu UIC) (renyaunma01@gmail.com Bowdoin College)

SMALL REU 2019

Williams College

Joint work with Keller L. Blackwell, Charles Devlin VI, Wanqiao Xu,

Leticia Mattos da Silva, and Dr. Steven Miller

July 23rd, 2019

The Code of Matrices

Theorem (Berlekamp and van Tilborg, 1978)

Let R be an $N \times N$ random matrix, m^T an N-tuple, and $m' = m^T R$. Given solely m', recovering m^T is NP-hard.

The Code of Matrices

Theorem (Berlekamp and van Tilborg, 1978)

Let R be an $N \times N$ random matrix, m^T an N-tuple, and $m' = m^T R$. Given solely m', recovering m^T is NP-hard.

Applications to Cryptography

- Private key: G

The Code of Matrices

Theorem (Berlekamp and van Tilborg, 1978)

Let R be an $N \times N$ random matrix, m^T an N-tuple, and $m' = m^T R$. Given solely m', recovering m^T is NP-hard.

Applications to Cryptography

- Private key: G
- Public key: $(\prod S_i)\, GP$ *(S_i, P are random matrices)*

The Code of Matrices

Theorem (Berlekamp and van Tilborg, 1978)

Let R be an $N \times N$ random matrix, m^T an N-tuple, and $m' = m^T R$. Given solely m', recovering m^T is NP-hard.

Applications to Cryptography

- Private key: G
- Public key: $(\prod S_i)\, GP$ *(S_i, P are random matrices)*
- Encryption: $m' = m^T (\prod S_i)\, GP$

Key Question

$$S_i = ???$$

Motivation to study iterated disco

Key Question

$$S_i = ???$$

Motivation to study iterated disco

Key Question

$$S_i = ???$$

RLCE (Wang, 2007)

$$S_1 = \begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix}$$

Source Matrices

Component Matrices A, B_d

A is a random $N \times N$ Hermitian matrix, $\{B_d\}$'s are a family of $2^{d-1}N \times 2^{d-1}N$ random Hermitian matrices. Assume all B_d's have same limiting eigenvalue distribution, and that $\mathcal{M}_k(A) < \infty$, $\mathcal{M}_k(B_d) < \infty$. Note that we assume all entries are from mean 0, variance 1 distribution.

$$\mathcal{D}_1 = \begin{bmatrix} A & B_1 \\ B_1 & A \end{bmatrix}$$

$$\mathcal{D}_2 = \begin{bmatrix} A & B_1 & & \\ B_1 & A & & B_2 \\ & & A & B_1 \\ B_2 & & B_1 & A \end{bmatrix}$$

Source Matrices

Component Matrices A, B_d

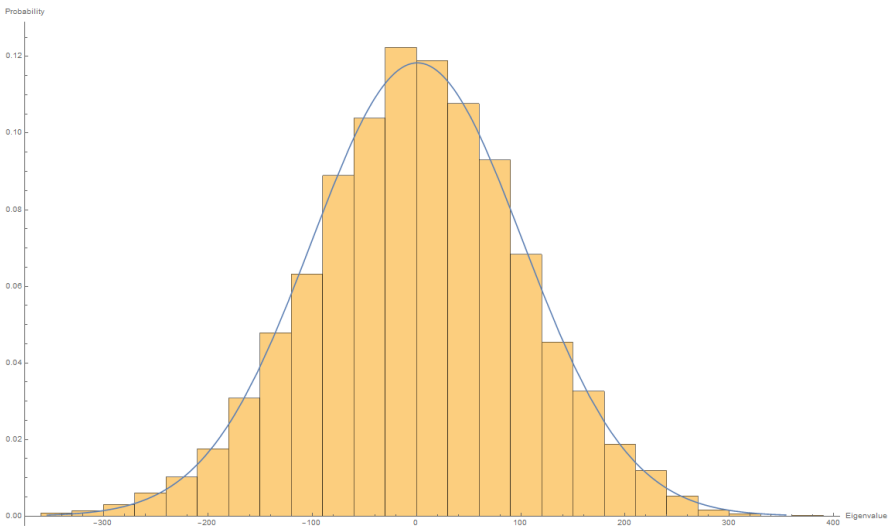
A is a random $N \times N$ Hermitian matrix, $\{B_d\}$'s are a family of $2^{d-1}N \times 2^{d-1}N$ random Hermitian matrices. Assume all B_d's have same limiting eigenvalue distribution, and that $\mathcal{M}_k(A) < \infty$, $\mathcal{M}_k(B_d) < \infty$. Note that we assume all entries are from mean 0, variance 1 distribution.

$$\mathcal{D}_3 = \begin{bmatrix} A & B_1 & B_2 & & B_3 \\ B_1 & A & & & \\ B_2 & & A & B_1 & \\ & & B_1 & A & \\ B_3 & & & & A & B_1 & B_2 \\ & & & & B_1 & A & \\ & & & & B_2 & & A & B_1 \\ & & & & & & B_1 & A \end{bmatrix}$$

Example

A: Gaussian (Massey, Miller, and Sinsheimer, 2007)

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt$$



10K × 10K SPT

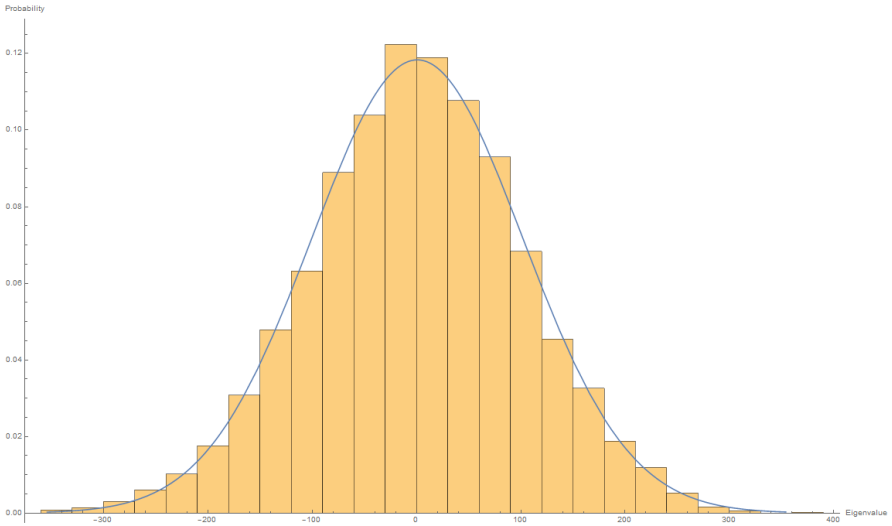
Example

A: Gaussian (Massey, Miller, and Sinsheimer, 2007)

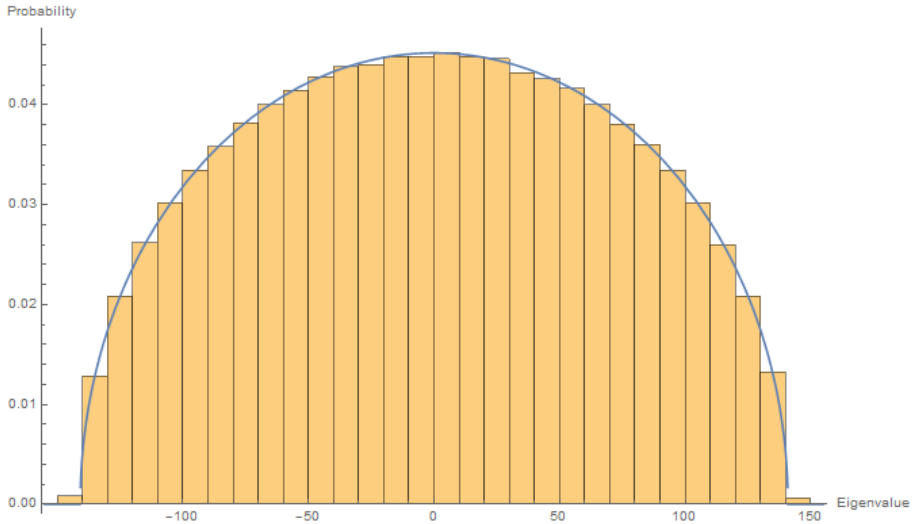
$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt$$

B: Semi-circle (Wigner, 1955)

$$f(x) = \begin{cases} \frac{1}{2\pi}\sqrt{4-x^2}, & |x| \leq 2 \\ 0, & |x| > 2. \end{cases}$$

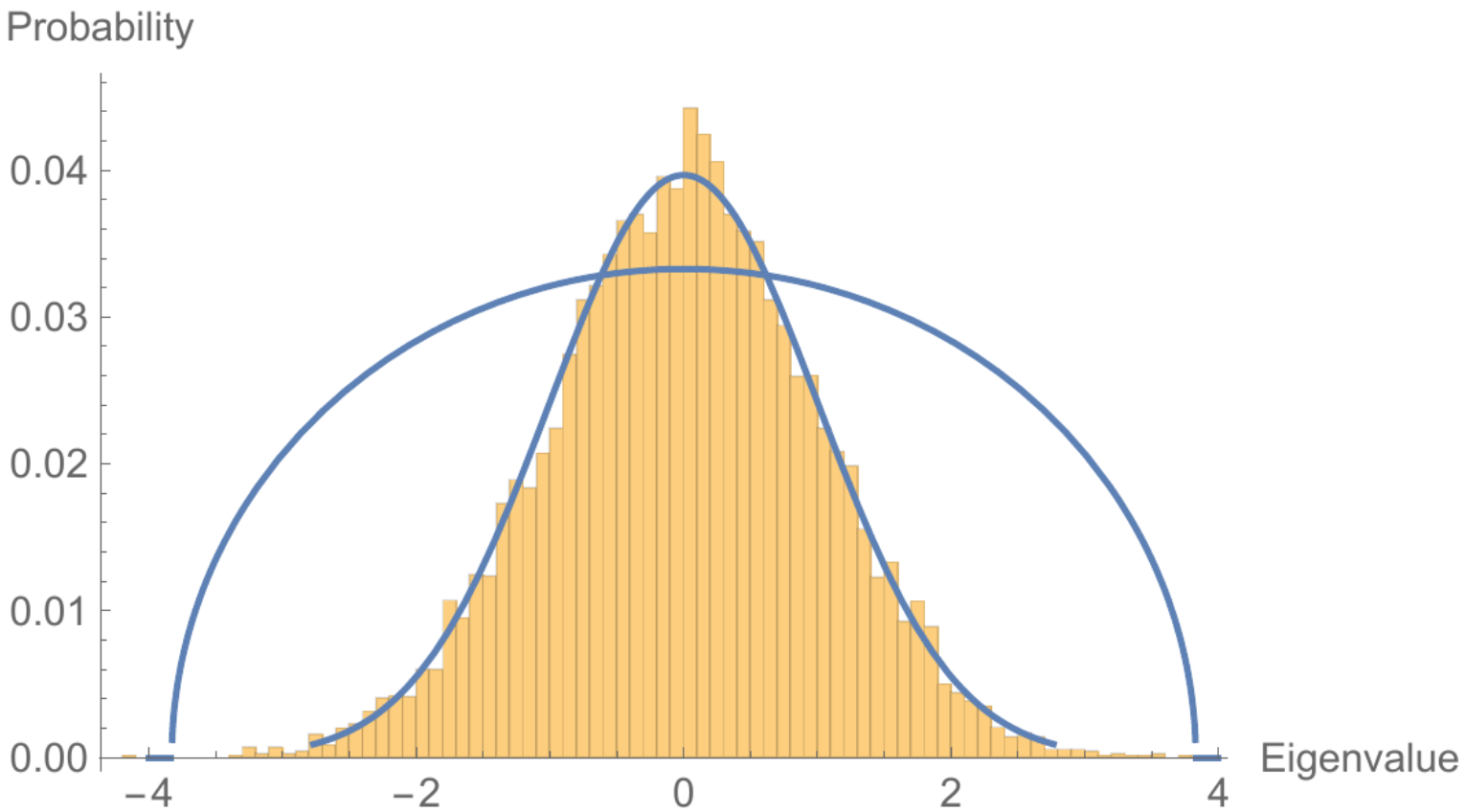


10K × 10K SPT

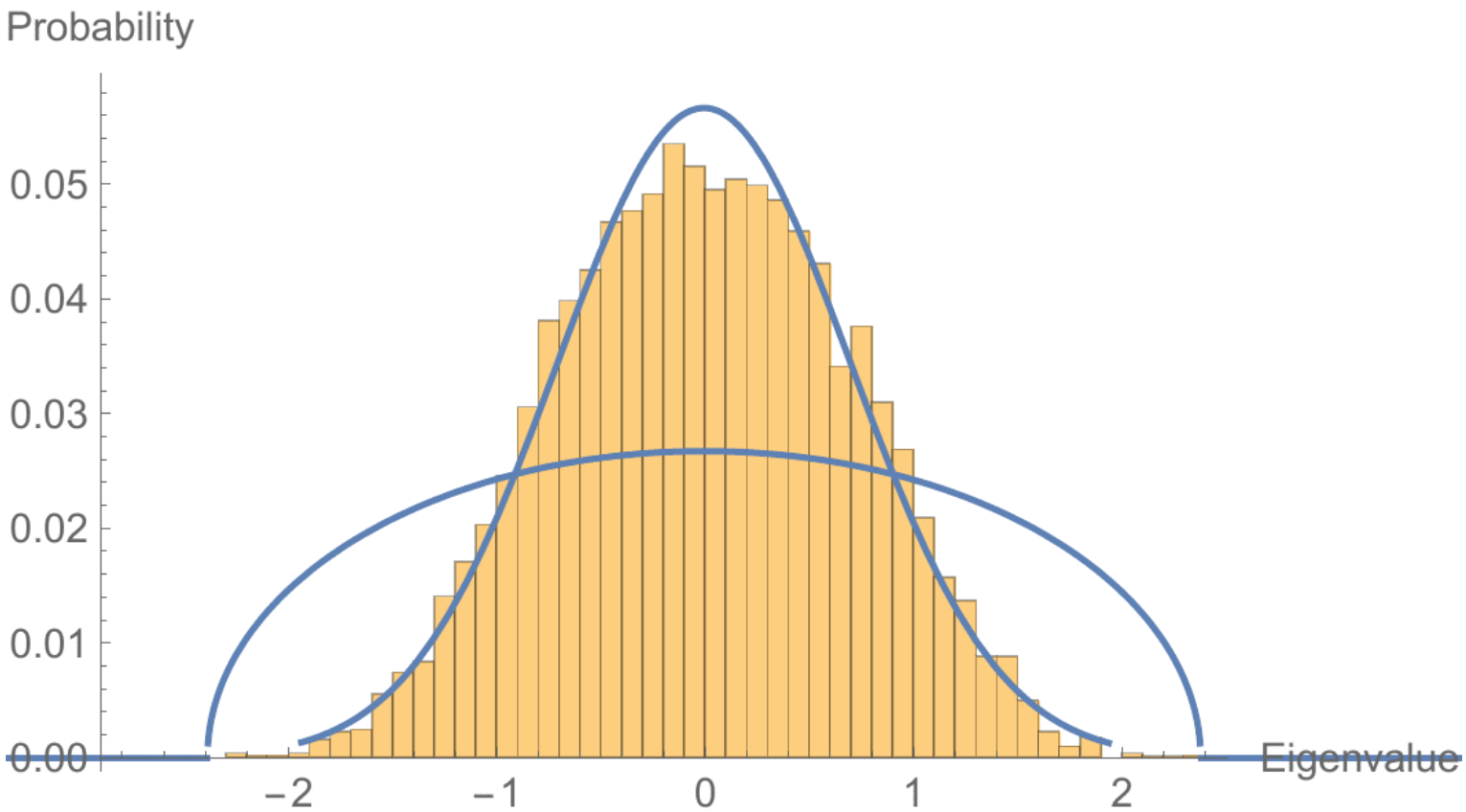


10K × 10K Real Symmetric

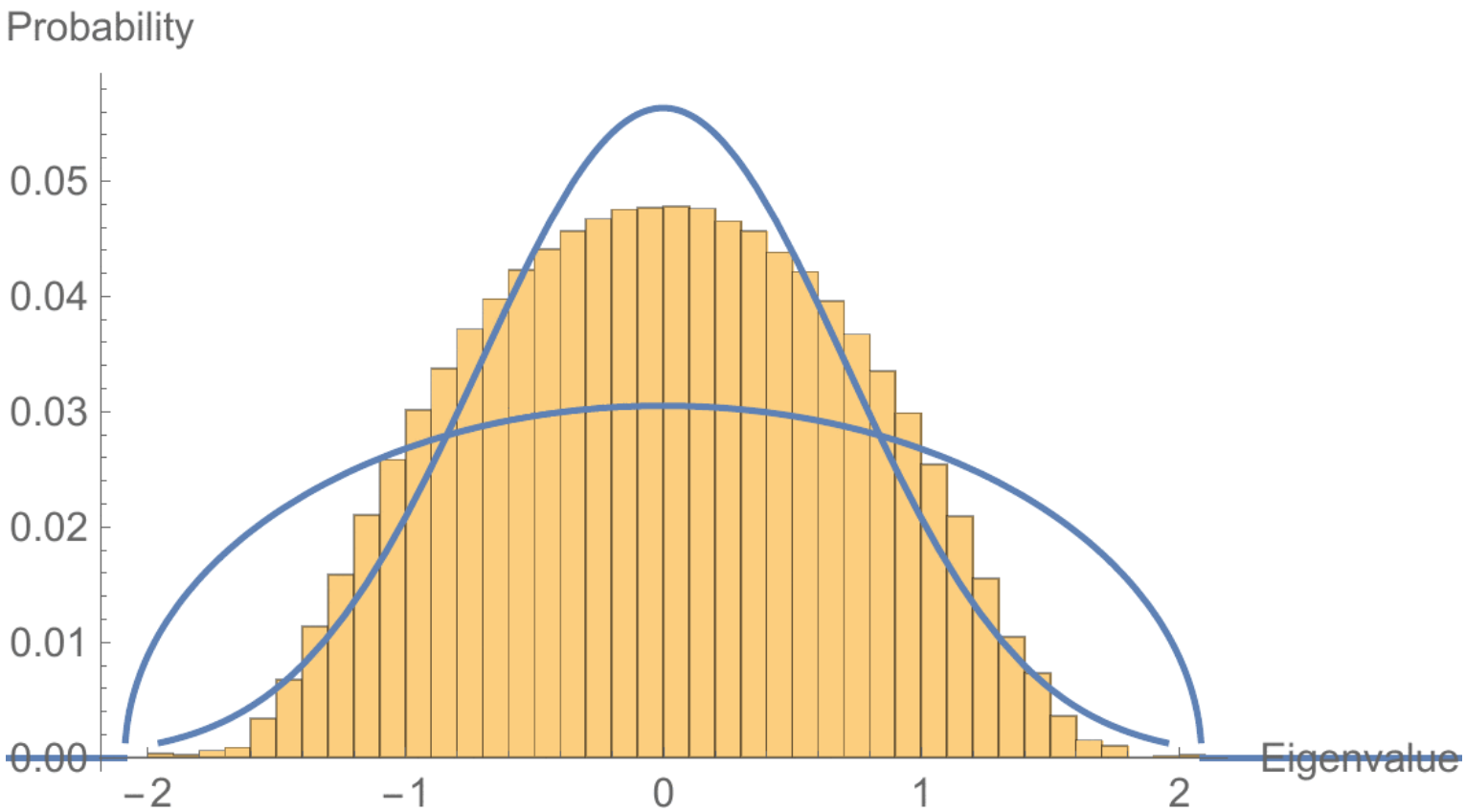
Infinite disco of STP and RS



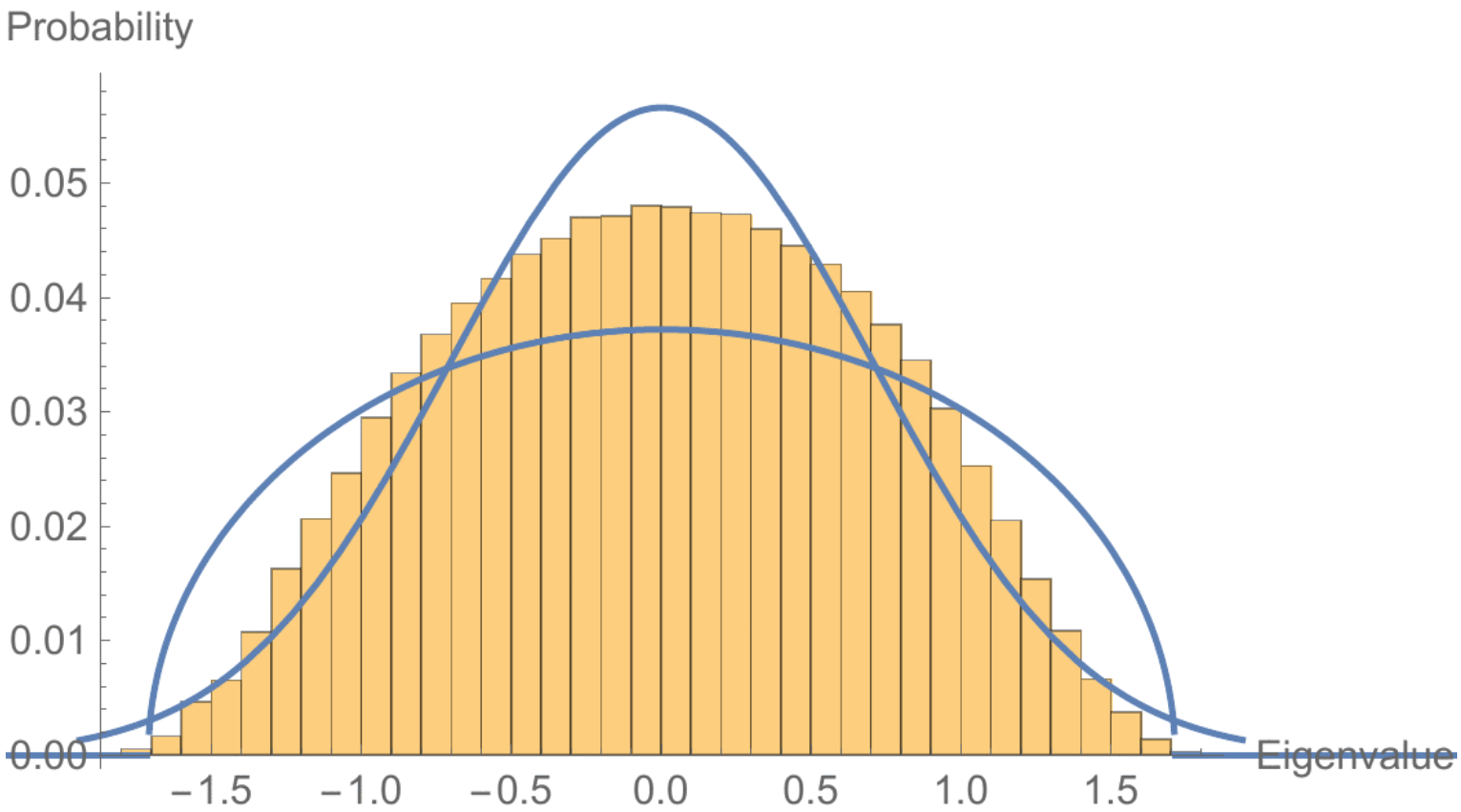
Infinite disco of STP and RS



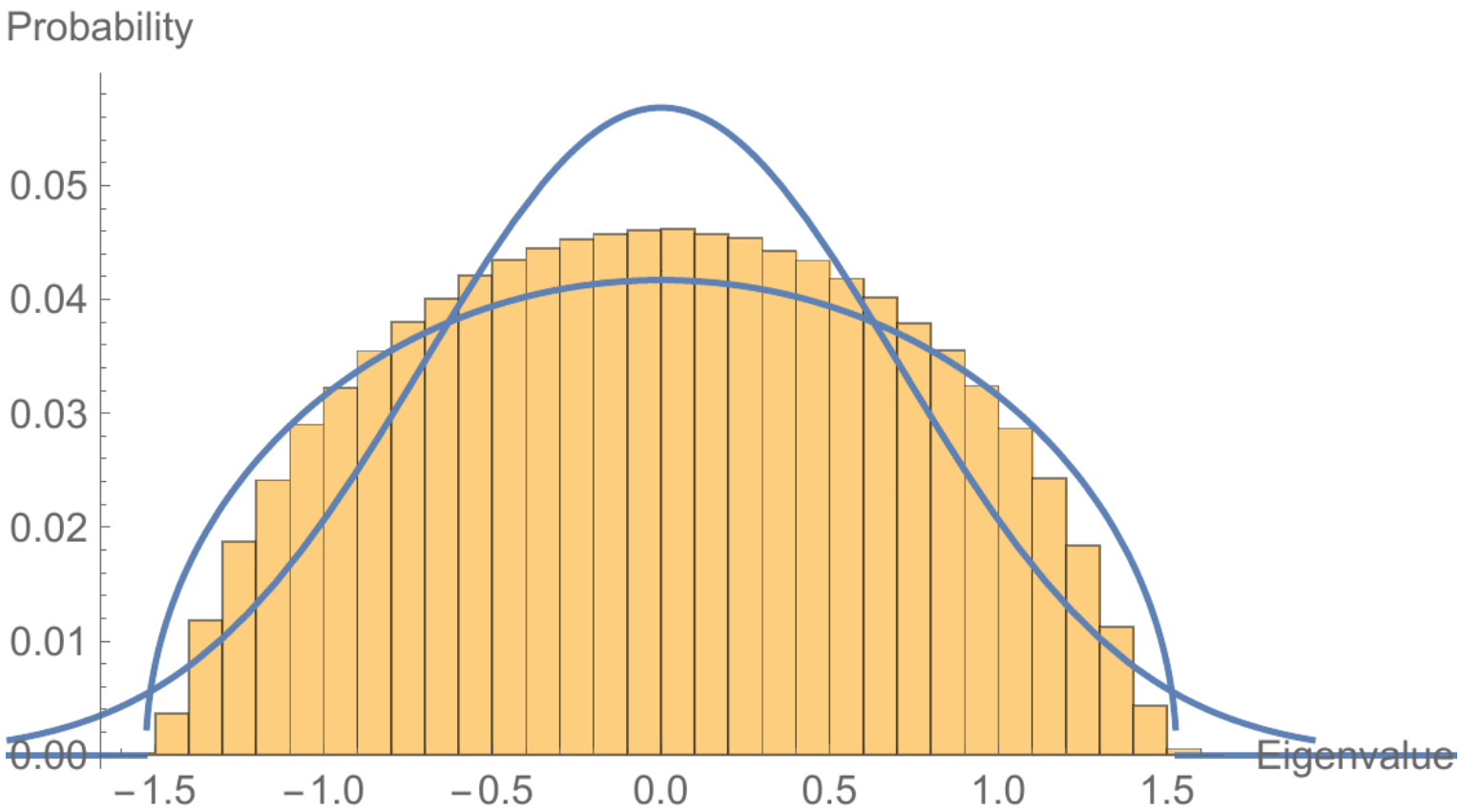
Infinite disco of STP and RS



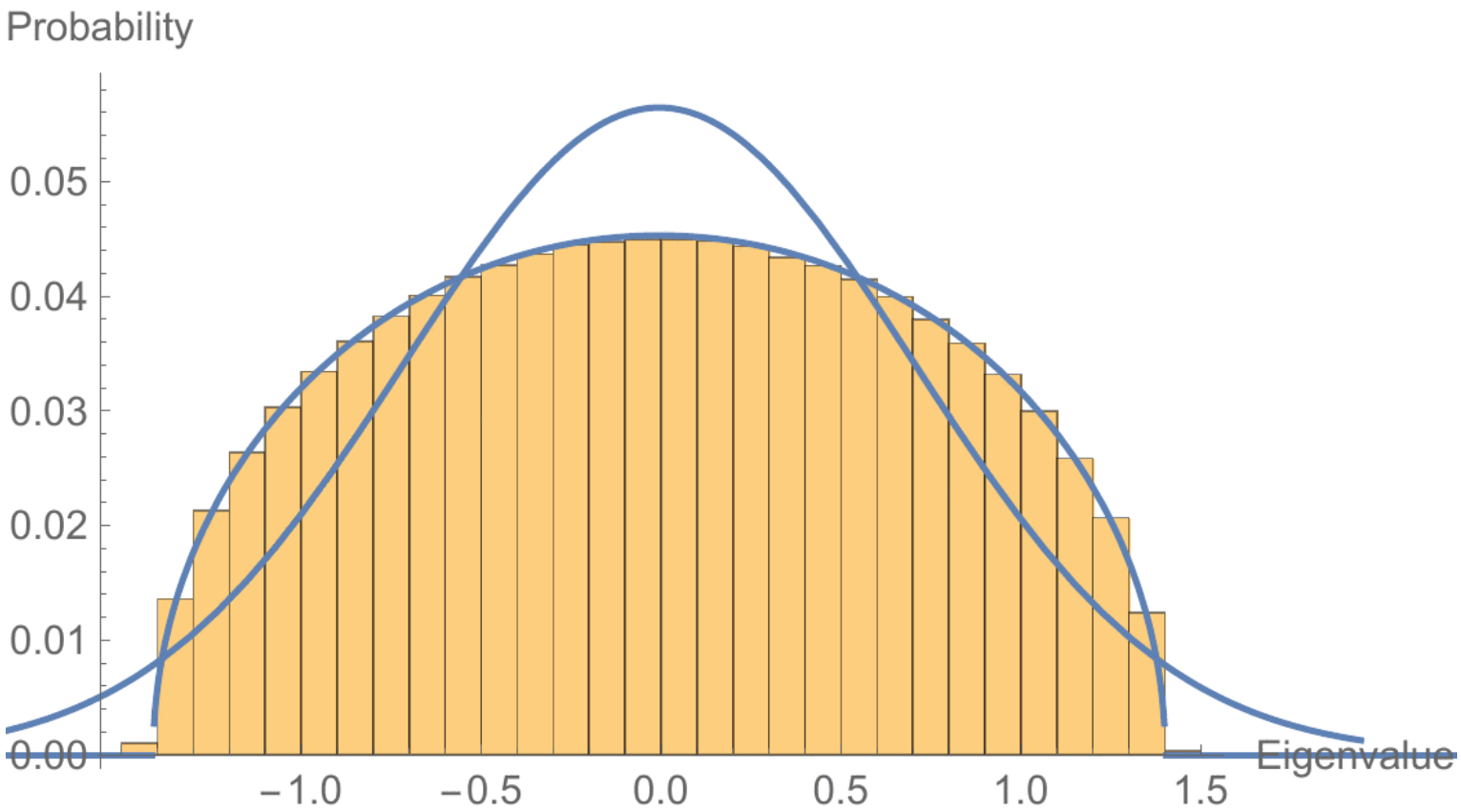
Infinite disco of STP and RS



Infinite disco of STP and RS



Infinite disco of STP and RS



Limiting behavior of distribution of Inifnite Disco

Theorem(B., Borade, Devlin, Ma, Miller, Silva, and X., 2019)

The limiting eigenvalue distribution of $\mathcal{D}_d(A, \{B_d\})$ converges with order $\mathcal{O}\left(2^{-d}\right)$ to the limiting normalized eigenvalue distribution of the B_d ensemble as $N \to \infty$ and $d \to \infty$.

Defining Probability Space

We normalize the eigenvalues of $\mathcal{D}_d$ by $\sqrt{2^d N}$:

$$\mu_{\mathcal{D}_d, 2^d N}(x)dx = \frac{1}{2(2^d N)} \sum_{j=1}^{2^d N} \delta\left(x - \frac{\lambda_j(\mathcal{D}_d)}{\sqrt{2^d N}}\right)$$

Defining Probability Space

We normalize the eigenvalues of $\mathcal{D}_d$ by $\sqrt{2^d N}$:

$$\mu_{\mathcal{D}_d, 2^d N}(x)dx = \frac{1}{2(2^d N)} \sum_{j=1}^{2^d N} \delta\left(x - \frac{\lambda_j(\mathcal{D}_d)}{\sqrt{2^d N}}\right)$$

The kth Moment of D_i

$$M_k(\mathcal{D}_d) = \lim_{N\to\infty} \mathbb{E}\left[\frac{1}{(2^d N)^{\frac{k}{2}+1}} \sum_{j=1}^{2^d N} \lambda_j^k(\mathcal{D}_d)\right]$$

What do we know about $\lambda_j(\mathcal{D}_d)$?

Eigenvalue Trace Lemma

$$\sum_{j=1}^{2^d N} \lambda_j^k(\mathcal{D}_d) \;=\; \text{Trace}(\mathcal{D}_d^k) \;=\; \sum_{1 \le j_1, \ldots, j_k \le 2^d N} d_{j_1,j_2} d_{j_2,j_3} \cdots d_{j_k,j_1}$$

What do we know about $\lambda_j(\mathcal{D}_d)$?

Eigenvalue Trace Lemma

$$\sum_{j=1}^{2^d N} \lambda_j^k(\mathcal{D}_d) \;=\; \text{Trace}(\mathcal{D}_d^k) \;=\; \sum_{1 \le j_1, \ldots, j_k \le 2^d N} d_{j_1,j_2} d_{j_2,j_3} \cdots d_{j_k,j_1}$$

$$M_k(\mathcal{D}_d) \;=\; \lim_{N \to \infty} \frac{1}{(2^d N)^{\frac{k}{2}+1}} \mathbb{E}\left[\text{Trace}(\mathcal{D}_d^k)\right]$$

What do we know about $\lambda_j(\mathcal{D}_d)$?

Eigenvalue Trace Lemma

$$\sum_{j=1}^{2^d N} \lambda_j^k(\mathcal{D}_d) \;=\; \mathrm{Trace}(\mathcal{D}_d^k) \;=\; \sum_{1\le j_1,\ldots,j_k\le 2^d N} d_{j_1,j_2} d_{j_2,j_3} \cdots d_{j_k,j_1}$$

$$M_k(\mathcal{D}_d) \;=\; \lim_{N\to\infty} \frac{1}{(2^d N)^{\frac{k}{2}+1}} \mathbb{E}\left[\mathrm{Trace}(\mathcal{D}_d^k)\right]$$

Odd k vanishes

$$M_k(\mathcal{D}_d) \;=\; \lim_{N\to\infty} \frac{1}{(2^d N)^{\frac{k}{2}+1}} \sum_{1\le j_1,\ldots,j_k\le 2^d N} \mathbb{E}\left[d_{j_1,j_2} d_{j_2,j_3} \cdots d_{j_k,j_1}\right] = 0.$$

Decomposing the $\mathcal{D}_d$ matrix

Let B_0 be from the same distribution of $\{B_d\}$. Define $C = A - B_0$ We can decompose $\mathcal{D}_d$ as follows:

$$\mathcal{D}_d = \mathcal{B} + \mathcal{C}$$

Decomposing the $\mathcal{D}_d$ matrix

Let B_0 be from the same distribution of $\{B_d\}$. Define $C = A - B_0$ We can decompose $\mathcal{D}_d$ as follows:

$$\mathcal{D}_d = \mathcal{B} + \mathcal{C}$$

where,

$$\mathcal{C} = \begin{bmatrix} C & & \\ & \ddots & \\ & & C \end{bmatrix}$$

Decomposing the $\mathcal{D}_d$ matrix

Let B_0 be from the same distribution of $\{B_d\}$. Define $C = A - B_0$ We can decompose $\mathcal{D}_d$ as follows:

$$\mathcal{D}_d = \mathcal{B} + \mathcal{C}$$

where,

$$\mathcal{C} = \begin{bmatrix} C & & \\ & \ddots & \\ & & C \end{bmatrix}$$

Moments of $C = A - B_0$

C is Hermitian and all moments of C are finite.

Defining $\mathcal{B}$

Choose from the ensemble of B_d's a random $N \times N$ matrix B_0 and define

$$\mathcal{B}_3 = \begin{bmatrix} B_0 & B_1 & B_2 & & & \\ B_1 & B_0 & & & & \\ & B_2 & B_0 & B_1 & & \\ & & B_1 & B_0 & & \\ & & & & B_3 & \\ & & & & & B_0 & B_1 & B_2 \\ & & & & & B_1 & B_0 & \\ & & & & & B_2 & & B_0 & B_1 \\ & & & & & & & B_1 & B_0 \end{bmatrix}$$

Sketch of proof

Consider the decomposition:

$$\mathcal{M}_k(\mathcal{D}) = \lim_{d,\, N\to\infty} \frac{1}{(2^d N)^{\frac{k}{2}+1}} \mathbb{E}\left[\mathrm{Tr}\left((\mathcal{B}+\mathcal{C})^k\right)\right]$$

$$= \lim_{d,\, N\to\infty} \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}.$$

Sketch of proof

Consider the decomposition:

$$\mathcal{M}_k(\mathcal{D}) = \lim_{d,\, N\to\infty} \frac{1}{(2^d N)^{\frac{k}{2}+1}} \mathbb{E}\left[\mathrm{Tr}\left((\mathcal{B}+\mathcal{C})^k\right)\right]$$

$$= \lim_{d,\, N\to\infty} \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}.$$

$$\mathcal{M}_k(B_i) \quad \leftrightarrow \quad \text{Contribution of } \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$$

$$\frac{\mathcal{M}_k(C)}{2^{\frac{dk}{2}}} \to 0 \quad \leftrightarrow \quad \text{Contribution of } \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$$

$$\frac{\mathit{FiniteConstant}}{2^d} \to 0 \quad \leftrightarrow \quad \text{Contribution of } \frac{\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right]}{(2^d N)^{\frac{k}{2}+1}}$$

Contribution of $\frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$ is $\mathcal{M}_k(B_i)$ as $N,\ d \to \infty$

Theorem(Luntzlara, Blackwell, B., Devlin, M., Miller, Silva, Wang and Xu, 2019)

The normalized eigenvalue distribution of $\mathcal{D}_1(A, B)$ is the same as that of A and B if A and B are chosen from ensembles with the same normalized eigenvalue distributions.

Contribution of $\frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$ is $\mathcal{M}_k(B_i)$ as $N,\ d \to \infty$

Theorem(Luntzlara, Blackwell, B., Devlin, M., Miller, Silva, Wang and Xu, 2019)

The normalized eigenvalue distribution of $\mathcal{D}_1(A, B)$ is the same as that of A and B if A and B are chosen from ensembles with the same normalized eigenvalue distributions.

$$\mathcal{B} = \begin{bmatrix} B_0 & B_1 & & & & & B_3 \\ B_1 & B_0 & B_2 & & & & \\ & B_2 & & B_0 & B_1 & & \\ & & & B_1 & B_0 & & \\ & & & & B_3 & & \\ B_0 & B_1 & & & & B_2 & \\ B_1 & B_0 & & & & & \\ & & B_2 & & & B_0 & B_1 \\ & & & & & B_1 & B_0 \end{bmatrix}$$

Contribution of $\frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$ is $\frac{\mathcal{M}_k(C)}{2^{\frac{dk}{2}}} \to 0$ as $N\ d \to \infty$

$$\mathcal{C}^k = \begin{bmatrix} C^k & & \\ & \ddots & \\ & & C^k \end{bmatrix} \implies \mathrm{Tr}(\mathcal{C}^k) = 2^d \mathrm{Tr}(C^k)$$

$$\implies \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}} = \frac{2^d \mathcal{M}_k(C)}{2^{\frac{dk}{2}+d}}$$

$$= \frac{\mathcal{M}_k(C)}{2^{\frac{dk}{2}}} \to 0 \text{ as } d \to \infty.$$

Challenges

Expansion of the product $(\mathcal{B}+\mathcal{C})^k$ yields a non-commutative, bi-variate matrix polynomial:

$$\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right] = \sum \mathbb{E}\left[\mathrm{Tr}\left(\mathcal{B}^{I_1}\mathcal{C}^{J_1}\cdots\mathcal{B}^{I_p}\mathcal{C}^{J_p}\right)\right]$$

Where $\sum I_p = I$, $\sum J_p = J$, and $I + J = k$.

Bound on mixed terms

Theorem.(Blackwell, B., Devlin, M., Miller, Silva, and Xu, 2019)

$A,\ B$ be $m \times m$ Hermitian random matrices. $I_i,\ J_i > 0$ s.t. $\sum_{i=1}^{p} I_i = I$ and $\sum_{i=i}^{p} J_i = J$, where$I + J = K$ $I, J,$ and K are all even. Then

$$\mathbb{E}[\mathrm{Tr}(A^{I_1} B^{J_1} \cdots A^{I_p} B^{J_p})] \leq \mathbb{E}[\mathrm{Tr}(A^K)]^{\frac{I}{K}} \mathbb{E}[\mathrm{Tr}(B^K)]^{\frac{J}{K}}.$$

Tools used to prove bound

Definition:p-Schatten norm of an operator X

$$||X||_p = \left(\sum_{i=1}^{m} \sigma_i^p(X) \right)^{\frac{1}{p}}$$

Here $\sigma_i(X)$ are singular values of X which are square roots of the eigenvalues of the matrix $\overline{X^T X}$.

Tools used to prove bound

Definition:p-Schatten norm of an operator X

$$||X||_p = \left(\sum_{i=1}^{m} \sigma_i^p(X) \right)^{\frac{1}{p}}$$

Here $\sigma_i(X)$ are singular values of X which are square roots of the eigenvalues of the matrix $\overline{X^T X}$.

Generalized Hölder-trace Inequality

Let $X_1, X_2, ..., X_k$ be a set of $m \times m$ matrices. Let $p_1, p_2, ..., p_k \geq 0$ such that $\sum_{i=1}^{k} \frac{1}{p_i} = 1$.

$$|\mathrm{Tr}(X_1 X_2 \cdots X_k)| \leq \prod_{i=1}^{k} ||X_i||_{p_i}.$$

Sketch of proof

Note that k is even. And for Hermitian A, $\sigma_i(A) = |\lambda_i(A)|$.

Sketch of proof

Note that k is even. And for Hermitian A, $\sigma_i(A) = |\lambda_i(A)|$.

$$\begin{aligned}
\mathbb{E}[\mathrm{Tr}(A^{I_1}B^{J_1}\cdots A^{I_p}B^{J_p})] &\leq \mathbb{E}\left[||A||_k^I||B||_k^J\right] \\
&= \mathbb{E}\left[\left(\sum_{i=1}^m \sigma_i^k(A)\right)^{\frac{I}{k}}\right]\mathbb{E}\left[\left(\sum_{i=1}^m \sigma_i^k(B)\right)^{\frac{J}{k}}\right] \\
&= \mathbb{E}\left[\left(\sum_{i=1}^m \lambda_i^k(A)\right)^{\frac{I}{k}}\right]\mathbb{E}\left[\left(\sum_{i=1}^m \lambda_i^k(B)\right)^{\frac{J}{k}}\right] \\
&= \mathbb{E}\left[\mathrm{Tr}(A^k)^{\frac{I}{k}}\right]\mathbb{E}\left[\mathrm{Tr}(B^k)^{\frac{J}{k}}\right] \\
&\leq \mathbb{E}\left[\mathrm{Tr}(A^k)\right]^{\frac{I}{k}}\mathbb{E}\left[\mathrm{Tr}(B^k)\right]^{\frac{J}{k}} \quad \text{(Jensen's inequality).}
\end{aligned}$$

Contribution of $\frac{\mathbb{E}[\mathrm{Tr}(\mathit{MixedProducts})]}{(2^d N)^{\frac{k}{2}+1}}$ is $\frac{\mathit{FiniteConstant}}{2^d} \to 0$

$$\frac{\mathbb{E}[\mathrm{Tr}(\mathcal{B}^{l_1}\mathcal{C}^{J_1}\cdots\mathcal{B}^{l_p}\mathcal{C}^{J_p})]}{(2^d N)^{\frac{k}{2}+1}} \leq \left(\frac{\mathbb{E}[\mathrm{Tr}(\mathcal{B}^K)]}{(2^d N)^{\frac{k}{2}+1}}\right)^{\frac{I}{K}} \left(\frac{\mathbb{E}\left[\mathrm{Tr}(C^k)\right]}{N^{\frac{k}{2}+1}}\right)^{\frac{J}{k}} \frac{1}{2^{dI}}$$

$$= \frac{\mathcal{M}_k(B_i)^{\frac{I}{k}}\mathcal{M}_k(C)^{\frac{J}{k}}}{2^{dI}} \to 0 \text{ as } \mathrm{d} \to \infty.$$

$$\implies \frac{\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right]}{(2^d N)^{\frac{k}{2}+1}} \to 0 \text{ as } N, \quad d \to \infty.$$

Result

$$\mathcal{M}_k(\mathcal{D}) = \lim_{d,\, N\to\infty} \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{B}^k)\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathit{MixedProducts})\right]}{(2^d N)^{\frac{k}{2}+1}} + \frac{\mathbb{E}\left[\mathrm{Tr}(\mathcal{C}^k)\right]}{(2^d N)^{\frac{k}{2}+1}}$$

$$= \lim_{d\to\infty} \mathcal{M}_k(B_i) + \mathcal{O}(\frac{1}{2^d})$$

$$= \mathcal{M}_k(B_i)$$

Thank you!

Thanks to Williams College, UIC and Bowdoin College for funding

Supported by NSF Grant DMS1561945 and NSF Grant DMS165903