Spies and Traitors: Random Matrix Kaleidoscopes and their Turncoat Eigenvalues

Neelima Borade (nborad2@uic.edu,University of Illinois at Chicago) , Renyuan Ma (renyuanma01@gmail.com, Bowdoin College) and Steven Miller(sjm1@williams.edu, Williams College)

Motivation

Applications to Cryptography

Wang's 2007 RLCE proposal uses the following random block diagonal matrix to encode a message.

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

Since each A is drawn from the same ensemble, the eigenvalue behavior of this matrix is well-predicted by the limiting eigenvalue distribution of the A ensemble.
We study what happens when we fill the empty space in the RLCE matrix with other random block matrices and show that doing so produces new, unpredictable behaviors that may have applications in cryptography.

Background

Normalized Spectral Measure

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

Eigenvalue Trace Lemma

$$\sum_{j=1}^{2^d N} \lambda_j^k(\mathscr{D}_d) = \text{Trace}(\mathscr{D}_d^k)$$

Average kth moment

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

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

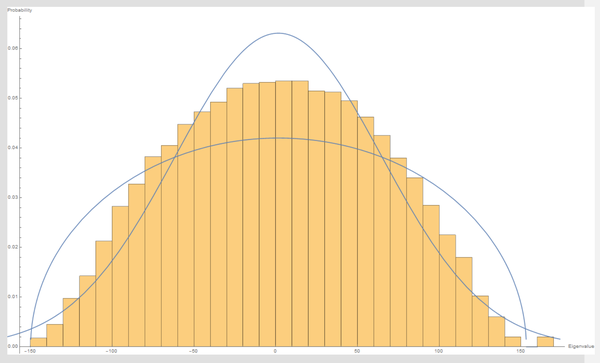
Decomposing the $\mathscr{D}_d$ matrix

$$\mathscr{D}_3 = \begin{bmatrix} A\ B_1 & B_2 & & \\ B_1\ A & & B_3 & \\ B_2 & A\ B_1 & & \\ & B_1\ A & & \\ & & A\ B_1 & B_2 \\ B_3 & & B_1\ A & \\ & & B_2 & A\ B_1 \\ & & & B_1\ A \end{bmatrix} \quad \mathscr{C} = \underbrace{\begin{bmatrix} C & & \\ & \cdots & \\ & & C \end{bmatrix}}_{C = A - B_0} \quad \underbrace{\mathscr{B}_3 = \begin{bmatrix} B_0\ B_1 & B_2 & & \\ B_1\ B_0 & & B_3 & \\ B_2 & B_0\ B_1 & & \\ & B_1\ B_0 & & \\ & & B_0\ B_1 & B_2 \\ B_3 & & B_1\ B_0 & \\ & & B_2 & B_0\ B_1 \\ & & & B_1\ B_0 \end{bmatrix}}_{B_0 \in B_d \text{ ensemble}}$$

Source Matrices

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

Example of case where d =1



Results

Lemma

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

$$\mathbb{E}[Tr(\Pi_{i=1,j=1}^{i=p,j=p} A^{l_i} B^{J_j})] \leq \mathbb{E}[Tr(A^K)]^{\frac{l}{K}} \mathbb{E}[Tr(B^K)]^{\frac{J}{K}}.$$

From this we deduce that,contribution of $\frac{\mathbb{E}[\text{Tr}(MixedProducts)]}{(2^d N)^{\frac{k}{2}+1}}$ is:$\frac{FiniteConstant}{2^d} \to 0$

Theorem

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

Note, when d is finite we get a distribution that is somewhere between the distributions of A and the B_d ensemble.

Future work

Let A, B be $N \times N$ random matrices, with independent entries i.i.d. from a fixed probability distribution p with mean 0 and variance 1.
Suppose that the limiting eigenvalue distributions of A, B have all moments finite and appropriately bounded. Then,

$$\min\{M_k(A), M_k(B)\} \leq M_k(\mathscr{D}_1(A, B)) \leq \max\{M_k(A), M_k(B)\}$$

Acknowledgements

Work supported by
NSF Grant DMS1561945
NSF Grant DMS1659037
Williams College
Bowdoin College