Littlewood-Offord estimates and the singularity problem of random matrices

Hoi H. Nguyen

University of Pennsylvania

NSF/CBMS conference, UAH, 4-8 June 2012

Random matrix models

Let ξ be a real or complex-valued random variable with mean 0 and variance 1.

- **Non-symmetric iid model**: M_n denotes the random matrix of order n whose entries are independent and indentically distributed (iid) copies of ξ.

  Examples: Bernoulli, real/complex Gaussian.

- **Wigner symmetric model**: $M_n^{\mathbf{sym}}$ denotes the random symmetric matrix of order n whose upper diagonal entries are iid copies of ξ.

  Examples: symmetric Bernoulli, symmetric Gaussian (GOE).

- **Wigner symmetric model**: $M_n^{\mathbf{sym}}$ denotes the random symmetric matrix of order n whose upper diagonal entries are iid copies of ξ.

  Examples: symmetric Bernoulli, symmetric Gaussian (GOE).

- **Wigner Hermitian model**: H_n denotes the random Hermitian matrix of order n whose upper diagonal entries are iid copies of a complex valued r.v. ξ.

  Examples: Hermitian Gaussian (GUE).

Universality phenomenon

Many facts about the distribution of eigenvalues of random matrices seem to be **universal** *in the limit $n \to \infty$, they do not depend on the precise matrix model used.*

Thus, for instance, discrete and continuous models often have the same statistics in the limit.

Empirical spectral distribution

Given a matrix M_n, the *empirical spectral distribution* (ESD) μ_{M_n} of M_n is defined as

$$\mu_{M_n} = \frac{1}{n} \sum_{i=1}^{n} \delta_{\lambda_i(M_n)},$$

where $\lambda_1(M_n), \ldots, \lambda_n(M_n)$ are the eigenvalues of M_n.

Wigner's semicircular law

The most well-known example of **universality** is for the bulk distribution of eigenvalues of Wigner matrices:

Wigner's semicircular law

The most well-known example of **universality** is for the bulk distribution of eigenvalues of Wigner matrices:

- **Wigner's semicircular law**: for a Wigner Hermitian random matrix:

$$\mu_{\frac{1}{\sqrt{n}} H_n} \to \frac{1}{2\pi}(4 - x^2)_+{}^{1/2} \mathrm{d}x$$

as n tends to ∞.

Wigner's semicircular law

The most well-known example of **universality** is for the bulk distribution of eigenvalues of Wigner matrices:

- **Wigner's semicircular law**: for a Wigner Hermitian random matrix:

$$\mu_{\frac{1}{\sqrt{n}}H_n} \to \frac{1}{2\pi}(4-x^2)_+{}^{1/2}\mathrm{d}x$$

  as n tends to ∞.

- Established by Wigner for GOE in 1955, and then repeatedly generalized and refined by many researchers.

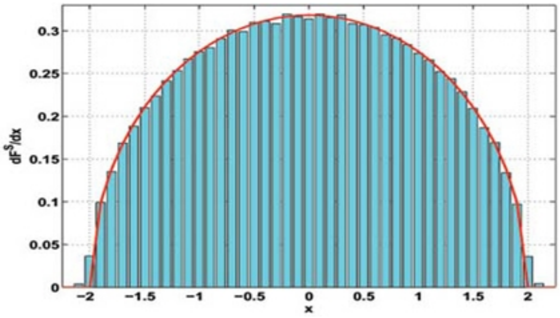

Figure: The ESD of a 100 by 100 random GUE (Picture by Alan Edelman)

Marchenko-Pastur quarter-circle law

- **Quarter-circle law**: for an iid non-symmetric random matrix

$$\mu_{(\frac{1}{n}M_nM_n^*)^{1/2}} \to \frac{1}{\pi}(4-x^2)_+^{1/2}\mathbf{1}_{[0,2]}\mathrm{d}x$$

as n tends to ∞.

Marchenko-Pastur quarter-circle law

- **Quarter-circle law**: for an iid non-symmetric random matrix

$$\mu_{(\frac{1}{n}M_nM_n^*)^{1/2}} \longrightarrow \frac{1}{\pi}(4-x^2)_+^{1/2}\mathbf{1}_{[0,2]}\mathrm{d}x$$

as n tends to ∞.

- Established by Marchenko and Pastur in 1967. Again, many further refinements and proofs.

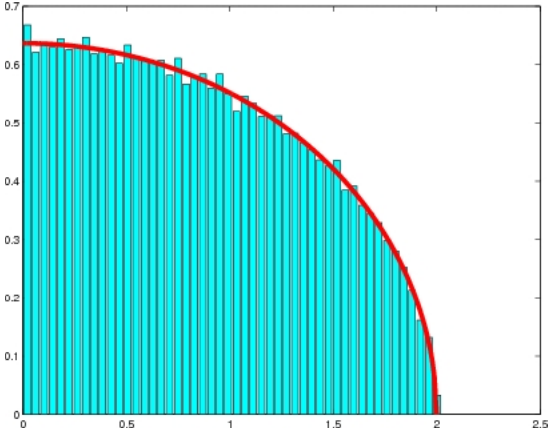

Figure: The ESD of a 100 by 100 random iid Gaussian matrix (Picture by Antonio Tulino)

Circular law

- **Circular law**: for an iid non-symmetric random matrix

$$\mu_{\frac{1}{\sqrt{n}}M_n} \to \mathbf{1}_{x^2+y^2\le 1}\mathrm{d}x\mathrm{d}y$$

as n tends to ∞.

Circular law

- **Circular law**: for an iid non-symmetric random matrix

$$\mu_{\frac{1}{\sqrt{n}}M_n} \to \mathbf{1}_{x^2+y^2\le 1}\mathrm{d}x\mathrm{d}y$$

as n tends to ∞.

- Established for gaussian matrices by Mehta in 1967. Generalized by many authors, and in full generality by Tao-Vu-Krishnapur [2008].

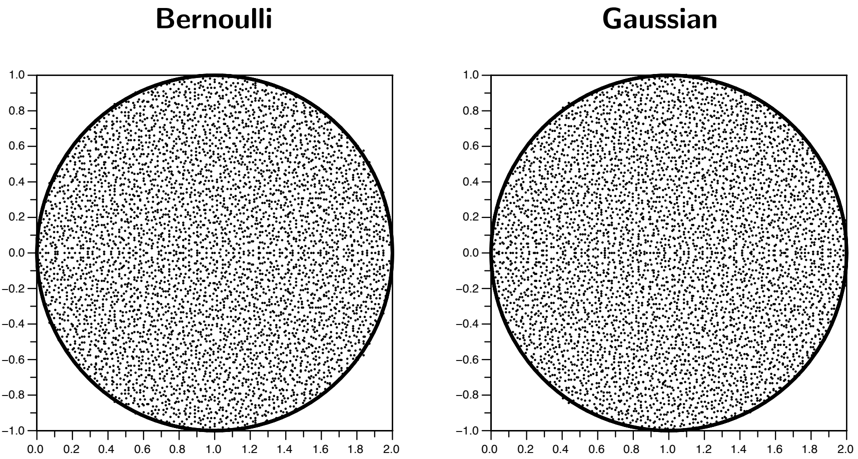

Figure: The ESD of 5000 by 5000 random iid Bernoulli and Gaussian matrices (Picture by Phillip Woods)

proof of the circular law: key ideas

- Roughly speaking, we need to control (for any fixed z)

$$\frac{1}{n}\log|\det(\frac{1}{\sqrt{n}}M_n - zI_n)|.$$

proof of the circular law: key ideas

- Roughly speaking, we need to control (for any fixed z)

$$\frac{1}{n}\log|\det(\frac{1}{\sqrt{n}}M_n - zI_n)|.$$

- Crucial problem: we need to show that the distances are not too small with very high probability.

proof of the circular law: key ideas

- Roughly speaking, we need to control (for any fixed z)

$$\frac{1}{n}\log|\det(\frac{1}{\sqrt{n}}M_n - zI_n)|.$$

- Crucial problem: we need to show that the distances are not too small with very high probability.

- More general: study the least singular value for square matrix $M_n + F_n$,

$$\sigma_n(M_n+F_n) = \inf_{\|x\|=1}\|(M_n+F_n)x\|,$$

(Recent: Tao-Vu, Rudelson-Vershynin)

- Given a radius β, given $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{C}^n$, we define the *concentration probability* of $\mathbf{a}$ to be

$$\rho_\beta(\mathbf{a}) := \sup_a \mathbf{P}(|a_1 x_1 + \cdots + a_n x_n - a| \leq \beta),$$

where $x_1, \dots, x_n$ are iid copies of a given random variable ξ of zero mean and unit variance.

- Given a radius β, given $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{C}^n$, we define the *concentration probability* of $\mathbf{a}$ to be

$$\rho_\beta(\mathbf{a}) := \sup_a \mathbf{P}(|a_1 x_1 + \cdots + a_n x_n - a| \leq \beta),$$

where $x_1, \dots, x_n$ are iid copies of a given random variable ξ of zero mean and unit variance.

- Discrete counterpart (assuming, say, a_i are integers and x_i are iid Bernoulli):

$$\rho(\mathbf{a}) := \sup_a \mathbf{P}(a_1 x_1 + \cdots + a_n x_n = a).$$

- Littlewood and Offord (1940s) raised the question of bounding $\rho_\beta(\mathbf{a})$. They showed that if all $|a_i| \geq 1$ and if x_i are Bernoulli random variables, then

$$\rho_1(\mathbf{a}) = \sup_a \mathbf{P}_{\mathbf{x}}(\sum_{1 \leq i \leq n} a_i x_i - a| \leq 1) = O(n^{-1/2} \log n).$$

- Littlewood and Offord (1940s) raised the question of bounding $\rho_\beta(\mathbf{a})$. They showed that if all $|a_i| \ge 1$ and if x_i are Bernoulli random variables, then

$$\rho_1(\mathbf{a}) = \sup_a \mathbf{P}_\mathbf{x}(\sum_{1\le i\le n} a_i x_i - a| \le 1) = O(n^{-1/2}\log n).$$

- Very soon after, Erdős gave a proof for the following refinement.

$$\rho_1(\mathbf{a}) \le \binom{n}{\lfloor n/2 \rfloor}/2^n.$$

- Littlewood and Offord (1940s) raised the question of bounding $\rho_\beta(\mathbf{a})$. They showed that if all $|a_i| \geq 1$ and if x_i are Bernoulli random variables, then

$$\rho_1(\mathbf{a}) = \sup_a \mathbf{P}_\mathbf{x}(|\sum_{1\leq i\leq n} a_i x_i - a| \leq 1) = O(n^{-1/2}\log n).$$

- Very soon after, Erdős gave a proof for the following refinement.

$$\rho_1(\mathbf{a}) \leq \binom{n}{\lfloor n/2 \rfloor}/2^n.$$

- Many other generalizations by Erdős-Moser, Füredi-Frankl, Griggs, Halász, Katona, Kleitman, Sárközy-Szemerédi, Vaughan-Wooley, and others.

Tao-Vu: the inverse approach

Tao-Vu: the inverse approach

Question

What is the underlying reason for, say

$$\rho_\beta(\mathbf{a}) = \sup_a \mathbf{P}_{\mathbf{x}}(|a_1 x_1 + \cdots + a_n x_n - a| \le \beta) = n^{-100}?$$

Definition

A set $Q \subset \mathbf{R}$ is a *generalized arithmetic progression (GAP) of rank r* if it can be expressed as in the form

$$Q = \{g_0 + n_1 g_1 + \cdots + n_r g_r | N_i \le n_i \le N_i', n_i \in \mathbf{Z} \text{ for all } 1 \le i \le r\}$$

for some $g_0, \ldots, g_r, N_1, \ldots, N_r, N_1', \ldots, N_r'$.

Definition

A set $Q \subset \mathbf{R}$ is a *generalized arithmetic progression (GAP) of rank r* if it can be expressed as in the form

$$Q = \{g_0 + n_1 g_1 + \cdots + n_r g_r | N_i \le n_i \le N_i', n_i \in \mathbf{Z} \text{ for all } 1 \le i \le r\}$$

for some $g_0, \dots, g_r, N_1, \dots, N_r, N_1', \dots, N_r'$.

It is convenient to think of Q as the image of an **integer box** $B := \{(n_1, \dots, n_r) \in \mathbf{Z}^r | N_i \le n_i \le N_i'\}$ under the linear map

$$\Phi : (n_1, \dots, n_r) \mapsto g_0 + n_1 g_1 + \cdots + n_r g_r.$$

Definition

A set $Q \subset \mathbf{R}$ is a *generalized arithmetic progression (GAP) of rank r* if it can be expressed as in the form

$$Q = \{g_0 + n_1 g_1 + \cdots + n_r g_r | N_i \le n_i \le N_i', n_i \in \mathbf{Z} \text{ for all } 1 \le i \le r\}$$

for some $g_0, \dots, g_r, N_1, \dots, N_r, N_1', \dots, N_r'$.

It is convenient to think of Q as the image of an **integer box** $B := \{(n_1, \dots, n_r) \in \mathbf{Z}^r | N_i \le n_i \le N_i'\}$ under the linear map

$$\Phi : (n_1, \dots, n_r) \mapsto g_0 + n_1 g_1 + \cdots + n_r g_r.$$

- If the map is one to one, we say that the GAP is *proper*.
- If $g_0 = 0$ and $N_i = -N_i'$, we say that the GAP is *symmetric*.

Example (discrete setting)

- Assume that the a_i are elements of a symmetric proper generalized arithmetic progression Q of rank r and size $n^{O(1)}$.

Example (discrete setting)

- Assume that the a_i are elements of a symmetric proper generalized arithmetic progression Q of rank r and size $n^{O(1)}$.

- Then $\sum_{i=1}^n a_i x_i$ is always an element of nQ. Thus if x_i are Bernoulli random variables, then

$$\rho_\beta(\mathbf{v}) = \sup_v \mathbf{P}(a_1 x_1 + \cdots + a_n x_n = a) \geq 1/|nQ| = n^{-O(1)}.$$

Inverse results for $\rho_\beta(\mathbf{a})$

Theorem (Tao-Vu 2007, N.-Vu, 2010)

Assume that

$$\rho_\beta(\mathbf{a}) = \sup_a \mathbf{P}_{\mathbf{x}}(|a_1x_1 + \cdots + a_nx_n - a| \le \beta) = n^{-O(1)}.$$

Then most of the a_i can be well-approximated by elements of a generalized arithmetic progression of rank $O(1)$ and size $n^{O(1)}$.

What can we say about the a_i if x_i are not independent and

$$\sup_a \mathbf{P}_{\mathbf{x}}(|a_1x_1 + \cdots + a_nx_n - a| \leq \beta) = n^{-O(1)}?$$

What can we say about the a_i if x_i are not independent and

$$\sup_a \mathbf{P}_{\mathbf{x}}(|a_1x_1 + \cdots + a_nx_n - a| \le \beta) = n^{-O(1)}?$$

- (Tao 2010, zero-sum matrix) Let $M_n = (m_{ij})$ be a random iid matrix, and define Z_n as $z_{ij} = m_{ij} - \frac{1}{n}(m_{i1} + \cdots + m_{in})$. Then $\mu_{\frac{1}{\sqrt{n}}Z_n}$ converges to the circular law.

What can we say about the a_i if x_i are not independent and

$$\sup_a \mathbf{P}_{\mathbf{x}}(|a_1x_1 + \cdots + a_nx_n - a| \le \beta) = n^{-O(1)}?$$

- (Tao 2010, zero-sum matrix) Let $M_n = (m_{ij})$ be a random iid matrix, and define Z_n as $z_{ij} = m_{ij} - \frac{1}{n}(m_{i1} + \cdots + m_{in})$. Then $\mu_{\frac{1}{\sqrt{n}}Z_n}$ converges to the circular law.
- (Bordenave-Caputo-Chafai 2008) Let $M_n = (m_{ij})$ be a random iid matrix with non-negative ξ of bounded density. Define Z_n to be the Markov matrix (z_{ij}) where $z_{ij} = m_{ij}/(m_{i1} + \cdots + m_{in})$. Then the ESD of $\sqrt{n}(Z_n - \mathbf{E}Z_n)$ converges to the circular law.

What can we say about the a_i if x_i are not independent and

$$\sup_a \mathbf{P}_{\mathbf{x}}(|a_1x_1 + \cdots + a_nx_n - a| \le \beta) = n^{-O(1)}?$$

- (Tao 2010, zero-sum matrix) Let $M_n = (m_{ij})$ be a random iid matrix, and define Z_n as $z_{ij} = m_{ij} - \frac{1}{n}(m_{i1} + \cdots + m_{in})$. Then $\mu_{\frac{1}{\sqrt{n}}Z_n}$ converges to the circular law.
- (Bordenave-Caputo-Chafai 2008) Let $M_n = (m_{ij})$ be a random iid matrix with non-negative ξ of bounded density. Define Z_n to be the Markov matrix (z_{ij}) where $z_{ij} = m_{ij}/(m_{i1} + \cdots + m_{in})$. Then the ESD of $\sqrt{n}(Z_n - \mathbf{E}Z_n)$ converges to the circular law.
- (N.) Let D_n be a random doubly stochastic matrix of size n. Then the ESD of $\sqrt{n}(D_n - \mathbf{E}D_n)$ converges to the *circular law*.

What can we say about the coefficients a_{ij} if

$$\sup_a \mathbf{P}_{\mathbf{x}}(\sum_{1\le i,j\le n} a_{ij}x_ix_j - a| \le \beta) = n^{-O(1)}?$$

What can we say about the coefficients a_{ij} if

$$\sup_a \mathbf{P}_{\mathbf{x}}(\sum_{1\le i,j\le n} a_{ij}x_ix_j - a| \le \beta) = n^{-O(1)}?$$

- (Vershynin, N.) Random symmetric matrices are not singular with with probability.

What can we say about the coefficients a_{ij} if

$$\sup_a \mathbf{P}_{\mathbf{x}}(\sum_{1\le i,j\le n} a_{ij}x_i x_j - a| \le \beta) = n^{-O(1)}?$$

- (Vershynin, N.) Random symmetric matrices are not singular with with probability.
- (O'Rourke-N.) Assume that the entry pairs $(x_{ij}, x_{ji}), i < j$ are iid copies of a vector (ξ_1, ξ_2) with ξ_1, ξ_2 of zero mean, unit variance and $\mathbf{E}\xi_1\xi_2 = \rho$ with some $-1 < \rho < 1$.

What can we say about the coefficients a_{ij} if

$$\sup_a \mathbf{P}_{\mathbf{x}}(\sum_{1\le i,j\le n} a_{ij}x_ix_j - a| \le \beta) = n^{-O(1)}?$$

- (Vershynin, N.) Random symmetric matrices are not singular with with probability.

- (O'Rourke-N.) Assume that the entry pairs $(x_{ij}, x_{ji}), i < j$ are iid copies of a vector (ξ_1, ξ_2) with ξ_1, ξ_2 of zero mean, unit variance and $\mathbf{E}\xi_1\xi_2 = \rho$ with some $-1 < \rho < 1$.

  Then $\mu_{\frac{1}{\sqrt{n}}M_n}$ converges to the **elliptic law** μ_ρ,

$$\mu_\rho(s,t) = \frac{1}{\pi(1-\rho^2)} mes\Big\{(x,y), x \le s, y \le t, \frac{x^2}{(1-\rho)^2} + \frac{y^2}{(1+\rho)^2} < 1\Big\}.$$