Random matrices: A Survey

Van H. Vu

Department of Mathematics
Rutgers University

Basic models of random matrices

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

Examples. real gaussian, complex gaussian, Bernoulli (± 1 with probability $1/2$).

Basic models of random matrices

Let ξ be a real or complex-valued random variable with mean 0 and variance 1.
Examples. real gaussian, complex gaussian, Bernoulli (± 1 with probability $1/2$).

Non-symmetric model. $M_n(\xi)$ denotes the random $n \times n$ matrix whose entries are i.i.d. copies of ξ.

Basic models of random matrices

Let ξ be a real or complex-valued random variable with mean 0 and variance 1.
Examples. real gaussian, complex gaussian, Bernoulli (± 1 with probability $1/2$).

Non-symmetric model. $M_n(\xi)$ denotes the random $n \times n$ matrix whose entries are i.i.d. copies of ξ.

Symmetric model. M_n^{sym} denotes the random symmetric $n \times n$ matrix whose upper triangular entries are i.i.d. copies of ξ.

Basic models of random matrices

Let ξ be a real or complex-valued random variable with mean 0 and variance 1.
Examples. real gaussian, complex gaussian, Bernoulli (± 1 with probability $1/2$).

Non-symmetric model. $M_n(\xi)$ denotes the random $n \times n$ matrix whose entries are i.i.d. copies of ξ.

Symmetric model. M_n^{sym} denotes the random symmetric $n \times n$ matrix whose upper triangular entries are i.i.d. copies of ξ.

Remark. For the symmetric model, one can often have a different distribution for the diagonal entries.

Basic models of random matrices

Let ξ be a real or complex-valued random variable with mean 0 and variance 1.
Examples. real gaussian, complex gaussian, Bernoulli (± 1 with probability $1/2$).

Non-symmetric model. $M_n(\xi)$ denotes the random $n \times n$ matrix whose entries are i.i.d. copies of ξ.

Symmetric model. M_n^{sym} denotes the random symmetric $n \times n$ matrix whose upper triangular entries are i.i.d. copies of ξ.

Remark. For the symmetric model, one can often have a different distribution for the diagonal entries.

Related models. Adjacency matrix of a random graphs (Erdös-Rény $G(n, p)$), random regular graphs, etc).

Some Main Problems

Statistics, Numerical Analysis. Spectral decomposition (Hwang, Wishart 1920s) Complexity of a computational problem involving a random matrix (von Neumann-Goldstine 1940s).

Some Main Problems

Statistics, Numerical Analysis. Spectral decomposition (Hwang, Wishart 1920s) Complexity of a computational problem involving a random matrix (von Neumann-Goldstine 1940s).

Mathematical Physics/Probability. Distributions of eigenvalues (global and local statistics) (Wigner 1950s).

Some Main Problems

Statistics, Numerical Analysis. Spectral decomposition (Hwang, Wishart 1920s) Complexity of a computational problem involving a random matrix (von Neumann-Goldstine 1940s).

Mathematical Physics/Probability. Distributions of eigenvalues (global and local statistics) (Wigner 1950s).

Combinatorics. Various combinatorial problems (Komlós 1960s).

There is a wonderful interaction between the theory of random matrices and other areas of mathematics (number theory, additive combinatorics, theoretical computer science etc).

Combinatorial Problems

Singularity. How often is a random matrix singular ?

Singularity. How often is a random matrix singular ?
Determinant. What is the typical value of the determinant ? How is it distributed ?

Combinatorial Problems

Singularity. How often is a random matrix singular ?
Determinant. What is the typical value of the determinant ? How is it distributed ?
Permanent. What is the typical value of the determinant ? How is it distributed ?

Singularity. How often is a random matrix singular ?
Determinant. What is the typical value of the determinant ? How is it distributed ?
Permanent. What is the typical value of the determinant ? How is it distributed ?
Eigenvectors. How does a typical eigenvector look like ?

The singularity problem: non-symmetric case

Let ξ be Bernoulli (so we consider random ± 1 matrices).
Question. What is p_n, the probability that M_n is singular ?

Conjecture. (folklore/notorious) $p_n = (1/2 + o(1))^n$.

The lower bound is obvious:

$$\mathbf{P}(\text{there are two equal rows/columns}) = (1 + o(1))n^2 2^{-n}.$$

Upper bound: $o(1)$ (Komlós 67).

Short proof of Komlós theorem

$$p_n \le \sum_{i=1}^{n-1} \mathbf{P}(X_{i+1} \in \text{ Span}(X_1, \dots, X_i)).$$

Fact. A subspace V of dim d contains at most 2^d Bernoulli vectors (as any vector in V is determined by a set of d coordinates). So

$$p_n \le \sum_{i=1}^{n-1} \frac{2^i}{2^n} =$$

Short proof of Komlós theorem

$$p_n \leq \sum_{i=1}^{n-1} \mathbf{P}(X_{i+1} \in \text{ Span}(X_1, \dots, X_i)).$$

Fact. A subspace V of dim d contains at most 2^d Bernoulli vectors (as any vector in V is determined by a set of d coordinates). So

$$p_n \leq \sum_{i=1}^{n-1} \frac{2^i}{2^n} = 1 - \frac{2}{2^n}.$$

$$p_n \leq \sum_{i=1}^{n-1} \mathbf{P}(X_{i+1} \in \text{ Span}(X_1, \dots, X_i)).$$

Fact. A subspace V of dim d contains at most 2^d Bernoulli vectors (as any vector in V is determined by a set of d coordinates). So

$$p_n \leq \sum_{i=1}^{n-1} \frac{2^i}{2^n} = 1 - \frac{2}{2^n}.$$

It is enough to show that the contribution of the last $k := \log\log n$ terms is $o(1)$. We will show

$$\mathbf{P}(X_n \in \text{ Span}(X_1, \dots, X_{n-1})) \leq \frac{1}{\log^{1/3} n}.$$

A $m \times n$ matrix is l-universal if for any set of l indices $i_1, \dots, i_l$ and any set of signs $\epsilon_1, \dots, \epsilon_l$, there is a row X where the i_jth entry of X has sign ϵ_j, for all $1 \le j \le l$.

Fact. $l = \log n$. A random $n \times n$ Bernoulli matrix is l-universal with probability at least $1 - \frac{1}{n}$.

Proof. $\mathbf{P}(\textit{fails}) \le \binom{n}{l} 2^l (1 - \frac{1}{2^l})^n \le \exp(2l \log n - 2^l n) \le n^{-1}$.

So with probability $1 - \frac{1}{n}$, any vector v orthogonal to $X_1, \dots, X_{n-1}$ should have at least l non-zero coordinate. Then

$$\mathbf{P}(X_n \in \text{ Span}(X_1, \dots, X_{n-1})) \le \mathbf{P}(X_n \cdot v = 0) = O(l^{1/2}) < \frac{1}{\log^{1/3} n}.$$

Lemma (Littlewood-Offord-Erdős, 1940s)

If $a_1, \dots, a_l$ are non zero numbers, then

$$\mathbf{P}(a_1 \xi_1 + \dots + a_l \xi_l = 0) = O(l^{-1/2}).$$

Further developments

Further developments

$O(n^{-1/2})$ (Komlós 77),

Further developments

$O(n^{-1/2})$ (Komlós 77),
$.999^n$ (Kahn-Komlós -Szemerédi 95),

Further developments

$O(n^{-1/2})$ (Komlós 77),
$.999^n$ (Kahn-Komlós -Szemerédi 95),
$(3/4 + o(1))^n$ (Tao-V. 06),

Further developments

$O(n^{-1/2})$ (Komlós 77),
$.999^n$ (Kahn-Komlós -Szemerédi 95),
$(3/4 + o(1))^n$ (Tao-V. 06),
$(1/\sqrt{2} + o(1))^n$ (Bourgain-V-Wood 09).

Tools

Dominating principle (Halász, KKSZ).
Inverse LIttlewood-Offord theory (TV)

$$|\cos x| \leq \frac{3}{4} + \frac{1}{4}\cos 2x.$$

Tools

Dominating principle (Halász, KKSZ).
Inverse LIttlewood-Offord theory (TV)

$$|\cos x| \leq \frac{3}{4} + \frac{1}{4}\cos 2x.$$

Fractional dimension (BVW)

$$|\cos x|^2 \leq \frac{1}{2} + \frac{1}{2}\cos 2x.$$

General theorem (BVW 09).

Littlewood-Offord theorems

Improvements of LOE lemma with extra assumptions on the a_i. For instance, if the a_i are different, then (Erdős-Moser, Sárközy-Szemerédi 1960s) showed

$$\mathbf{P}(a_1\xi_1 + \cdots + a_l\xi_l = 0) = O(l^{-3/2}).$$

Stanley showed the extremal set is an arithmetic progression. Kleitman, Katona, Franlk-Füredi, Halaśz, etc.

Tao-V. 05: If the probability in question is large, then $\{a_1, \ldots, a_n\}$ can be characterized.
If $P \geq n^{-A}$, then (most of) a_i belong to an AP of lenght n^B.
The relation between A and B is of importance. A near optimal bound was obtained by Tao-V. (07), that lead to the establishment of the Circular Law Conjecture concerning the eigenvalues of M_n (Budapest 08, Bulletin AMS 09).

Inverse Littlewood-Offord theorems

Using a different approach, Nguyen-V. (09+) obtained the optimal relation. As a corollary, one obtains all forward LOE results such as Sárkozy-Szemerédi theorem.
One can also obtain an asymptotic, stable, version of Stanley's result (algebra-free).

See: Hoi Nguyen's talk (December).

The singularity problem: symmetric case

Let ξ be Bernoulli (so we consider random ± 1 matrices).
Question. What is p_n^{sym}, the probability that M_n^{sym} is singular ?

Conjecture. (B. Weiss 1980s) $p_n^{sym} = o(1)$.

This is the symmetric version of Komlós 1967 theorem.

Theorem (Costello-Tao-V. 2005)

$p^{sym} = O(n^{-1/4})$.

Quadratic Littlewood-Offord

Recently, Kevin Costello (2009) improved the bound to $n^{-1/2+\epsilon}$, which seems to be the limit of the method.

Lemma (Costello 09)

Consider the quadratic form $Q = \sum_{1 \le i,j \le n} a_{ij}\xi_i\xi_j$ *with* $a_{ij} \neq 0$*. Then*

$$\mathbf{P}(Q = 0) \le n^{-1/2+\epsilon}.$$

Question. Higher degree polynomials ?

Quadratic Littlewood-Offord

Recently, Kevin Costello (2009) improved the bound to $n^{-1/2+\epsilon}$, which seems to be the limit of the method.

Lemma (Costello 09)

Consider the quadratic form $Q = \sum_{1 \le i,j \le n} a_{ij}\xi_i\xi_j$ with $a_{ij} \neq 0$. Then

$$\mathbf{P}(Q = 0) \le n^{-1/2+\epsilon}.$$

Question. Higher degree polynomials ?
Conjecture. (V. 2006) $p^{sym}(n) = (1/2 + o(1))^n$.

Rank of random graphs

The Costello-Tao-V. result also holds for $A(n,p)$, the adjacency matrix of $G(n,p)$ with constant p.

Rank of random graphs

The Costello-Tao-V. result also holds for $A(n,p)$, the adjacency matrix of $G(n,p)$ with constant p.

Question. What about non-constant p ?

If $p < (1-\epsilon)\log n/n$, $A(n,p)$ is almost surely singular, as the graph has non-isolated vertices.

Theorem (Costello-V. 06)

For $p > (1+\epsilon)\log n/n$, $A(n,p)$ is a.s. non-singular.

Theorem (Costello-V. 07)

For $p = c\log n/n$ with $0 < c < 1$, the co-rank of $A(n,p)$ (a.s.) comes from small local obstructions.

A set S is a local obstruction if the number of neighbors of S is less than $|S|$. Small means $|S| \leq K(c)$.
For $p = c/n$, Bordenare and Lelarge (09) computed the asymptotics of the rank. I wonder if one can characterize the co-rank.

Random regular graphs

Conjecture. [V. 2006] $A(n, d)$ (adjacency matrix of a random regular graphs of degree d) is a.s non-singular for all $3 \leq d \leq n/2$.

The second eigenvalue

Conjecture. $A(n, d)$ (adjacency matrix of a random regular graphs of degree d) has second eigenvalue $O(\sqrt{d})$ for all $3 \le d \le n/2$.

Known for $d = O(1)$ (Freedman, Kahn-Szemerédi 1989). Recently Freedman showed

$$\lambda = (2 + o(1))\sqrt{d-1}.$$

The KSz argument seems to extend to cover up to $d \le n^{1/2}$. For $d = n/2$, the best current bound is $O(\sqrt{n \log n})$.

Determinant: non-symmetric case

Question. What is the typical value of $|\det M_n|$?

Turán (1940s): By linearity of expectation,

$$\mathbf{E}(\det M_n^2) = n! = n^{(1+o(1)n}.$$

Determinant: non-symmetric case

Question. What is the typical value of $|\det M_n|$?

Turán (1940s): By linearity of expectation,

$$\mathbf{E}(\det M_n^2) = n! = n^{(1+o(1)n}.$$

Conjecture. A.s. $|\det M_n| = n^{(1/2+o(1))n}$.

Determinant: non-symmetric case

Question. What is the typical value of $|\det M_n|$?
Turán (1940s): By linearity of expectation,

$$\mathbf{E}(\det M_n^2) = n! = n^{(1+o(1)n}.$$

Conjecture. A.s. $|\det M_n| = n^{(1/2+o(1))n}$.

Theorem (Tao-V. 2004)

A.s.

$$|\det M_n| = n^{(1/2+o(1))n}.$$

Ideas

Determinant is the volume of the parallelepiped spanned by the row vectors.
Use the height times base formula.
Most of the distances are strongly concentrated.

Lemma (Tao-V. 04)

The distance from a random vectorin $\mathbf{R}^n$ to a fixed subspace of dimension d is, with high prob, $\sqrt{n-d}+$ small error.

The remaining few distances are not too small !.

Determinant: Distribution

Question. We know $\mathbf{P}(\det = 0) = \exp(-\Theta(n))$. What about $\mathbf{P}(\det = z)$, for integer $z \neq 0$?

I think $\mathbf{P}(\det = z) = \exp(-\omega(n))$, perhaps $\leq n^{-cn}$ for some constant $c > 0$.

Question. Limiting distribution of $|\det|$

$$\frac{\log|\det M_n| - \frac{1}{2}\log(n-1)!}{c\sqrt{\log n}} \to N(0,1).$$

(Girko (???) 80s).

Determinant: Concentration

For the next discussion, consider a slightly more general model: Let M be a deterministic matrix with entries $0 < c < m_{ij} < C$. Let ξ be a random variable with mean 0 and variance one and M_n be the random matrix with entries $m_{ij}\xi_{ij}$. (So the entries have different variances.)

Question. How strongly is $|\det M_n|$ concentrated ?

Determinant: Concentration

For the next discussion, consider a slightly more general model: Let M be a deterministic matrix with entries $0 < c < m_{ij} < C$. Let ξ be a random variable with mean 0 and variance one and M_n be the random matrix with entries $m_{ij}\xi_{ij}$. (So the entries have different variances.)

Question. How strongly is $|\det M_n|$ concentrated ?

Motivation. Estimating permanent using random determinant.

Given a matrix A, define $m_{ij} := \sqrt{a_{ij}}$, then

$$\mathrm{Per}\, A := \mathbf{E}|\det M_n|^2.$$

Markov chain: Jerrum-Sinclair, J-S-Vigoda (00). Random determinant: Barvinok (00): $\exp(cn)$ with ξ guassian, Friedland-Rider-Zeitouni (04) $\exp(\epsilon n)$ with ξ guassian (under boundedness).

Theorem (Costello-V. 07)

With high probability and ξ guassian or Bernoulli

$$|\det M_n|/\mathbf{E}|\det M_n| \leq \exp(n^{2/3+o(1)}).$$

Markov chain: Jerrum-Sinclair, J-S-Vigoda (00). Random determinant: Barvinok (00): $\exp(cn)$ with ξ guassian, Friedland-Rider-Zeitouni (04) $\exp(\epsilon n)$ with ξ guassian (under boundedness).

Theorem (Costello-V. 07)

With high probability and ξ guassian or Bernoulli

$$|\det M_n|/\mathbf{E}|\det M_n| \leq \exp(n^{2/3+o(1)}).$$

Conjecture. (Kostello-V. 07) With high probability, $|\det M_n|/\mathbf{E}|\det M_n| \leq n^{O(1)}$.

Permanent: non-symmetric case

Question. What is the typical value of $|\,\mathrm{Per} M_n|$?

Turán's : $\mathbf{E}(\,\mathrm{Per} M_n^2) = n!$.

Permanent: non-symmetric case

Question. What is the typical value of $|\,\mathrm{Per} M_n|$?
Turán's : $\mathbf{E}(\,\mathrm{Per} M_n^2) = n!$.

Conjecture. A.s. $|\,\mathrm{Per} M_n| = n^{(1/2+o(1))n}$.

It had been a long standing open conjecture that a.s $|\,\mathrm{Per} M_n| > 0$ (the permanent version of Komlós 1967 theorem).

Theorem (Tao-V. 2008)

A.s.

$$|\ Per\ M_n| = n^{(1/2+o(1))n}.$$

Question. What about limiting distribution and concentration ? (not known even for gaussian case).

Permanent: non-symmetric case

Question. What is the typical value of $|\text{Per} M_n|$?
Turán's : $\mathbf{E}(\text{Per} M_n^2) = n!$.

Conjecture. A.s. $|\text{Per} M_n| = n^{(1/2+o(1))n}$.

It had been a long standing open conjecture that a.s $|\text{Per} M_n| > 0$ (the permanent version of Komlós 1967 theorem).

Theorem (Tao-V. 2008)

A.s.

$$|\,Per\ M_n| = n^{(1/2+o(1))n}.$$

Question. What about limiting distribution and concentration ? (not known even for gaussian case).
Question. What is q_n, the probability that the permanent is zero ?

Permanent: non-symmetric case

Question. What is the typical value of $|\operatorname{Per} M_n|$?
Turán's : $\mathbf{E}(\operatorname{Per} M_n^2) = n!$.

Conjecture. A.s. $|\operatorname{Per} M_n| = n^{(1/2+o(1))n}$.

It had been a long standing open conjecture that a.s $|\operatorname{Per} M_n| > 0$ (the permanent version of Komlós 1967 theorem).

Theorem (Tao-V. 2008)

A.s.

$$|\ Per\ M_n| = n^{(1/2+o(1))n}.$$

Question. What about limiting distribution and concentration ? (not known even for gaussian case).
Question. What is q_n, the probability that the permanent is zero ?
Current bounds. $q_n \leq n^{-b}$. The truth may be n^{-bn}.

Determinant-Permanent: Symmetric case

Still by linearity of expectation

$$\mathbf{E}|\det M_n^{sym}|^2 = n^{(1+o(1)n}$$

$$\mathbf{E}|\,\mathrm{Per} M_n^{sym}|^2 = n^{(1+o(1))n}.$$

Conjecture. A.s. $|\det M_n^{sym}| = n^{(1/2+o(1))n}$.

Conjecture. A.s. $|\,\mathrm{Per} M_n^{sym}| = n^{(1/2+o(1))n}$.

Determinant-Permanent: Symmetric case

Still by linearity of expectation

$$\mathbf{E}|\det M_n^{sym}|^2 = n^{(1+o(1)n}$$

$$\mathbf{E}|\operatorname{Per} M_n^{sym}|^2 = n^{(1+o(1))n}.$$

Conjecture. A.s. $|\det M_n^{sym}| = n^{(1/2+o(1))n}$.

Conjecture. A.s. $|\operatorname{Per} M_n^{sym}| = n^{(1/2+o(1))n}$.

The major difficulty here is that the rows are no longer independent.

Determinant-Permanent: Symmetric case

Still by linearity of expectation

$$\mathbf{E}|\det M_n^{sym}|^2 = n^{(1+o(1)n}$$

$$\mathbf{E}|\operatorname{Per} M_n^{sym}|^2 = n^{(1+o(1))n}.$$

Conjecture. A.s. $|\det M_n^{sym}| = n^{(1/2+o(1))n}$.

Conjecture. A.s. $|\operatorname{Per} M_n^{sym}| = n^{(1/2+o(1))n}$.

The major difficulty here is that the rows are no longer independent.

,

Recently, Tao-V. (2009) confirmed the first conjecture, the second is till open.

Eigenvectors

Consider M_n^{sym}. Its eigenvectors form a orthonormal system

$$v_1, \dots, v_n, \|v_i\| = 1.$$

Question. How do the v_i look like ?
sub-Question. $\|v_i\|_\infty = ?(Linial)$

Theorem (Tao-V. 2009)

With high probability

$$\max_i \|v_i\|_\infty = n^{-1/2+o(1)}.$$