Recent progress in combinatorial random matrix theory

Van H. Vu

Department of Mathematics
Yale University

Survey: Recent progress in combinatorial random matrix theory

https://arxiv.org/abs/2005.02797

- M_n: random matrix of size n whose entries are i.i.d. Rademacher random variables (taking values ± 1 with probability $1/2$). I
- M_n^{sym}: random symmetric matrix of size n whose (upper triangular) entries are i.i.d. Rademacher random variables.
- Adjacency matrix of a random graph. This matrix is $(0,1)$ symmetric.
- Laplacian of a random graph.

Let p_n be the probability that M_n is singular:

$$p_n \geq 2^{-n}.$$

By choosing any two rows (columns) and considering signs

$$p_n \geq (4 - o(1))\binom{n}{2}2^{-n} = (\frac{1}{2} + o(1))^n. \qquad (1)$$

Conjecture (Singularity, non-symmetric)

$$p_n = (\frac{1}{2} + o(1))^n.$$

Phenomenon I. *The dominating reason for singularity of a random matrix is the dependency between a few rows/columns.*

Conjecture

$$p_n = (2 + o(1))n^2 2^{-n}.$$

Komlós (1967): $p_n = o(1)$.
Komlós (1975): $p_n = O(n^{-1/2})$.
Kahn-Komlós-Szemrédi (1996): $p(n) \leq .999^n$.
Tao-V. (2004): $p_n = O(.958^n)$.
Tao-V. (2007): $p(n) \leq (3/4 + o(1))^n$.
Bourgain-V.-P. M. Wood (2009): $p(n) \leq (\frac{1}{\sqrt{2}} + o(1))^n$.

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

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

In 2018, Tikhomirov proved the Singularity Conjecture

Theorem (Tikhomirov 2018)

$$p_n = (\frac{1}{2} + o(1))^n.$$

In 2018, Tikhomirov proved the Singularity Conjecture

Theorem (Tikhomirov 2018)

$$p_n = (\frac{1}{2} + o(1))^n.$$

April 2020, Irmatov claimed the strong form (singularity comes from two equal rows)

$$p_n = (2 + o(1))n^2 2^{-n}.$$

Litvak and Tikhomirov (about the same time) announced a similar result, but for sparse matrices.

Anti-concentration. The probability that a random variable takes value in a small interval is small.

Let $\mathbf{v} = \{v_1, \ldots, v_n\}$ be a set of n non-zero real numbers and $\xi_1, \ldots, \xi_n$ be i.i.d random Rademacher variables. Define $S := \sum_{i=1}^{n} \xi_i v_i$, $p_{\mathbf{v}}(a) = \mathbf{P}(S = a)$, and $p_{\mathbf{v}} = \sup_{a \in \mathbf{Z}} p_{\mathbf{v}}(a)$.

Theorem (Littlewood-Offord-Erdös, 1943)

$$p_{\mathbf{v}} \le \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O(n^{-1/2}).$$

Build M_n by adding one random row at a time. Assume that the first $n-1$ rows are independent and form a hyperplane with normal vector $\mathbf{v} = (v_1, \dots, v_n)$. Conditioned on these rows, the probability that M_n is singular is

$$\mathbf{P}(X \cdot \mathbf{v} = 0) = \mathbf{P}(\xi_1 v_1 + \cdots + \xi_n v_n = 0),$$

where $X = (\xi_1, \dots, \xi_n)$ is the last row.

Phenomenon II. [Inverse Littlewood-Offord theory] *If* $\mathbf{P}(X \cdot \mathbf{v} = 0)$ *is relatively large, then the coefficients* $v_1, \dots, v_n$ *posses a strong additive structure.*

Build M_n by adding one random row at a time. Assume that the first $n-1$ rows are independent and form a hyperplane with normal vector $\mathbf{v} = (v_1, \dots, v_n)$. Conditioned on these rows, the probability that M_n is singular is

$$\mathbf{P}(X \cdot \mathbf{v} = 0) = \mathbf{P}(\xi_1 v_1 + \cdots + \xi_n v_n = 0),$$

where $X = (\xi_1, \dots, \xi_n)$ is the last row.

Phenomenon II. [Inverse Littlewood-Offord theory] *If* $\mathbf{P}(X \cdot \mathbf{v} = 0)$ *is relatively large, then the coefficients* $v_1, \dots, v_n$ *posses a strong additive structure.*

Continuous version: smallest singular value (Tao-V, Rudelson-Vershinin, Tikhomirov, Tikhomirov-Litvak).

Estimate p_n^{sym}, the probability that the symmetric matrix M_n^{sym} singular.

Conjecture (B. Weiss, 1980s)

$p_n^{sym} = o(1)$.

Estimate p_n^{sym}, the probability that the symmetric matrix M_n^{sym} singular.

Conjecture (B. Weiss, 1980s)

$p_n^{sym} = o(1)$.

Theorem (Costello-Tao-V. 2006)

$p_n^{sym} = o(1)$.

Build the matrix by growing its from size k to $k+1$. Last step: from $(n-1)\times(n-1)$ submatrix M^{sym}_{n-1}, to obtain M^{sym}_n, we add a random row $X=(\xi_1,\dots,\xi_n)$ and its transpose

$$\det M^{sym}_n = \sum_{1\le i,j\le n-1} a_{ij}\xi_i\xi_j + \det M^{sym}_{n-1},$$

where a_{ij} are the cofactors of M_{n-1}.
If M^{sym}_n is singular, then its determinant is 0,

$$Q := \sum_{1\le i,j\le n-1} a_{ij}\xi_i\xi_j = -\det M^{sym}_{n-1}.$$

Theorem (LOE for quadratic forms: Costello-Tao-V. 2006, Make-O. Nguyen-V. 2014)

If $a_{ij}\neq 0$, then

$$\mathbf{P}(Q=x)=\tilde{O}(n^{-1/2}).$$

Conjecture (Singularity, symmetric)

$p_n^{sym} = (1/2 + o(1))^n$.

Costello-Tao-V.(2006): $n^{-1/4}$.
Costello (2010): $n^{-1/2+\epsilon}$
Nguyen (2012) $n^{-\omega(1)}$.
Vershynin (2014): $\exp(-n^c)$, for some small constant $c > 0$.
Ferber-Jain (2019) $c = 1/4$.
Campos-Mattos-Morris-Morrison(2020): $c = 1/2$.

Conjecture (Singularity, symmetric)

$p_n^{sym} = (1/2 + o(1))^n$.

Costello-Tao-V.(2006): $n^{-1/4}$.
Costello (2010): $n^{-1/2+\epsilon}$
Nguyen (2012) $n^{-\omega(1)}$.
Vershynin (2014): $\exp(-n^c)$, for some small constant $c > 0$.
Ferber-Jain (2019) $c = 1/4$.
Campos-Mattos-Morris-Morrison(2020): $c = 1/2$.

Question. Inverse Littlewood-Offord theory for quadratic forms ?

The same proof holds for the adjacency matrix of the random graph $G(n, 1/2)$.

Question. What about other densities ?

If $p < \log n/n$, there are isolated vertices, so the matrix is singular.

Theorem (Threshold of Singularity; Costello-V. 2008)

For any constant $\epsilon > 0$*, with probability* $1 - o(1)$*,*

$$A(n, (1+\epsilon)\log n/n) = 0.$$

The same proof holds for the adjacency matrix of the random graph $G(n, 1/2)$.

Question. What about other densities ?

If $p < \log n/n$, there are isolated vertices, so the matrix is singular.

Theorem (Threshold of Singularity; Costello-V. 2008)

For any constant $\epsilon > 0$*, with probability* $1 - o(1)$*,*

$$A(n, (1+\epsilon)\log n/n) = 0.$$

Basak-Rudelson (2018): $\log n/n + \gamma(n)/n$ where $\gamma(n)$ is any function tending to infinity.

Addario-Berry-Eslava (2014) Hitting time: we generate the random graph by adding random edges one by one (the next random edge is uniformly chosen from the set of all available edges). Let T be the first time when the graph has no isolated vertices.

Addario-Berry-Eslava (2014) Hitting time: we generate the random graph by adding random edges one by one (the next random edge is uniformly chosen from the set of all available edges). Let T be the first time when the graph has no isolated vertices.

Theorem (Hitting time of Singularity)

With probability $1 - o(1)$, *the graph is full rank at time* T.

Question. Below the threshold, what is the co-rank ?

Phenomenon I. *The dominating reason for singularity of a random matrix is the dependency between a few rows/columns.*

Theorem (Costello-V. 2010)

For any constant $\epsilon > 0$ *and* $(1/2+\epsilon)\log n/n < p < (1-\epsilon)\log n/n$, *with probability* $1-o(1)$, $A(n,p)$ *equals the number of isolated vertices.*

For a smaller p, one needs to take into account other small structures such as *cherries* (a cherry is a pair of vertices of degree one with a common neighbor; in the matrix, this subgraph forces two identical rows).
Costello-V. showed that if $p = \Theta(\log n/n)$, the co-rank are determined by small subgraphs with more vertices than edges.

When $p = c/n, c > 1$, $G(n,p)$ consists of a giant component and many small components. Since $Giant(n,p)$ has cherries , the adjacency matrix of $Giant(n,p)$ is singular (with high probability).

Conjecture (k-core)

Let $c > 1$ be a constant and set $p = c/n$. There is a constant k_0 such that for all $k \geq k_0$ the following holds. With probability $1 - o(1)$, the adjacency matrix of the k-core of $Giant(n,p)$ is non-singular.

Theorem (Bordenave, Lelarge, and Salez (2011))

Consider $G(n, c/n)$ for some constant $c > 0$. Then with probability $(1 - o(1))n$,

$$rank(A(n, c/n)) = (2 - q - e^{-cq} - cqe^{-cq} + o(1))n,$$

where $0 < q < 1$ is the smallest solution of $q = \exp(-c \exp -cq)$.

Coja-Oghlan-Ergür-Gao-Hetterich-Rolvier: asymptotic rank of random matrices with prescribed number of non-zeroes in each row/column.

Random regular graph $G_{n,d}$. For $d = 2$, $G_{n,d}$ is just the union of disjoint circles. A circle with length divisible by 4 is singular.

Conjecture (Singularity of Random regular graphs, V. 2006)

For any $3 \leq d \leq n-1$, with probability $1 - o(1)$ $A_{n,d}$ is non-singular.

Landon, Sose, and Yau (2016): true for $d \geq n^c$ for any constant c. The most challenging case, d being a constant, was solved recently by Meszaros (2018) and Huang (2018).

Theorem (Meszaros 2018, Huang 2018)

For any fixed $d \geq 3$, the probability that $A_{n,d}$ is singular is $o(1)$.

The finite field embedding idea:
Embed $\{-1, 1\}$ in F_q for some prime q.
Show that with high probability, no vector $v \in F_q^n$ satisfies $M_n v = 0$. (Union bound; Anti-concentration in finite fields.)
Adjust q to optimize the failure probability.

The finite field embedding idea:
Embed $\{-1, 1\}$ in F_q for some prime q.
Show that with high probability, no vector $v \in F_q^n$ satisfies $M_n v = 0$. (Union bound; Anti-concentration in finite fields.)
Adjust q to optimize the failure probability.

Theorem (Nguyen-Wood (2018))

For different primes $q_1, \dots, q_k$, $\det M_n \pmod{q_i}$ are asymptotically independent.

M_n defines a map from $\mathbf{Z}^n$ to itself. As M_n is non-singular, this map is (whp) injective.
But is it *surjective* ? The answer is ""NO" as $\det M_n$ is divisible by 2^{n-1}.

M_n defines a map from $\mathbf{Z}^n$ to itself. As M_n is non-singular, this map is (whp) injective.
But is it *surjective* ? The answer is ""NO" as $\det M_n$ is divisible by 2^{n-1}.

Consider a $n \times (n+1)$ random matrix with iid ± 1 entries. This matrix defines a map from $\mathbf{Z}^{n+1}$ to $\mathbf{Z}^n$.
Question What is the probability that this map is surjective ?

M_n defines a map from $\mathbf{Z}^n$ to itself. As M_n is non-singular, this map is (whp) injective.
But is it *surjective* ? The answer is ""NO" as $\det M_n$ is divisible by 2^{n-1}.

Consider a $n \times (n+1)$ random matrix with iid ± 1 entries. This matrix defines a map from $\mathbf{Z}^{n+1}$ to $\mathbf{Z}^n$.
Question What is the probability that this map is surjective ?

Theorem (Nguyen and Wood 2018)

$$(1 + o(1)) \prod_{k \geq 2} \zeta(k)^{-1} \approx .4358.$$

Question. How big is $\det M_n$.

Question. How big is $\det M_n$.

Each row has length $\sqrt{n}$, so by Hadamard's inequality

$$|\det M_n| \leq n^{n/2}.$$

Tao-V. (2004): whp $|\det M_n| \geq n^{n/2 - o(n)}$.

We now know that $\log|\det M_n|$ satisfies the CLT with mean $(n/2 + o(n))\log n$ and variance $\log n$ (Nguyen-V. 2014). A similar result holds for M_n^{sym} (Bourgade-Mudy 2019)

Conjecture (Determinant)

For any $x \neq 0$, $\mathbf{P}(\det M_n = x) \leq n^{-(1/2+o(1))n}$.

It is not known that M_n has a super- exponential range.

Permanent: $\mathbf{E}(\mathrm{Per}\ M_n)^2 = n!$.
It suggests that $|\mathrm{Per}\ M_n|$ is typically $n^{(1/2-o(1))n}$.

Conjecture

$\mathbf{P}(\mathrm{Per}\ M_n = 0) = o(1)$.

Theorem (Tao-V. 2007)

With probability $1 - o(1)$

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

Conjecture (Permanent)

The probability that $\mathrm{Per}\ M_n = 0$ *is super exponentially small in* n.

A matrix has simple spectrum if its eigenvalues are different.

Question

Are random matrices simple ?

Conjecture (Babai, 1980)

With probability $1 - o(1)$, $G(n, 1/2)$ *has a simple spectrum.*

The motivation came from the well-known result (proved by Leighton-Miller and Babai-Grigoriev-Mount that the notorious graph isomorphism problem is in **P** within the class of graphs with simple spectrum.

Theorem (Tao-V. 2016)

Babai's conjecture holds.

Conjecture (Simplicity)

$s_n = (4 + o(1))^{-n}$.

Conjecture

With probability $1 - o(1)$, the singular values of M_n^{sym} are different.

Notice that the singular values of a symmetric matrix are the absolute values of its eigenvalues. Thus, this conjecture asserts that there is no two eigenvalues adding up to zero.
One can pose the same questions for M_n. In this direction, Ge proved that with probability $1 - o(1)$, the spectrum of M_n is simple. In 2019, Luh and O'rourke proved the first exponential bound, showing that the probability that the spectrum of M_n is not simple is at most 2^{-cn}, for some constant $c > 0$.

An $n \times n$ real matrix A *normal* if $AA^T = A^T A$.

Question

How often is a random matrix normal?

The probability that M_n is symmetric is $2^{-(0.5+o(1))n^2}$,

$$\nu_n \geq 2^{-(0.5+o(1))n^2}.$$

Conjecture (Normality)

$$\nu_n = 2^{-(0.5+o(1))n^2}.$$

Theorem (Deneanu-V. 2017)

$$\nu_n \leq 2^{-(0.302+o(1))n^2}.$$

Conjecture (Integral spectrum)

The probability that M_n^{sym} has an integral spectrum is $2^{-(.5+o(1))n^2}$.

Ahmadi, Alon, Blake, and Shparlinski (2009) $2^{-n/400}$.
Costello and Williams (2016): $2^{-cn^{3/2}}$.