Lecture 5: More on Random Matrices

In which we study the operator norm of Wigner matrices.

Let G be an undirected random graph sampled from the Erdös-Renyi $G_{n,\frac{1}{2}}$ distribution, meaning that G has n vertices, each unordered pair $\{u, v\}$ has probability $1/2$ of being an edge of G, and the choices for different pairs are mutually independent.

Last time we showed that the Matrix Chernoff Bounds imply that with high probability $||A - \mathbb{E}\,A|| \leq 2\sqrt{n \log n}$. Today we discuss two other techniques to prove concentration bounds for random matrices, and we illustrate them with an estimate of $||A - \mathbb{E}\,A||$. It will be more convenient to work with the Wigner matrix $W = 2 \cdot (A - \mathbb{E}\,A)$, which is a random symmetric matrix with zero diagonal and ± 1 off-diagonal entries.

1 Reasoning about ϵ-nets

The operator norm of Hermitian matrices can be characterized as the continuous optimization problem

$$||M|| = \max_{x:||x||=1} |x^T M x|$$

and our first idea is to introduce a combinatorial problem that approximates it.

Call $\mathcal{S}$ the unit sphere in $\mathbb{R}^n$, and call a set $N \subseteq \mathcal{S}$ an ϵ-net if for every element $x \in \mathcal{S}$ there exists an element $y \in N$ such that $||x - y|| \leq \epsilon$.

The existence of relatively small ϵ-nets of $\mathcal{S}$ can be argued by the following argument: start with an empty set $N = \emptyset$, then repeat the operation of adding to N an element of $\mathcal{S}$ that is at distance at least ϵ from all the current elements of N, until such operation is not possible any more. When the above procedure stops, we have an ϵ-net of $\mathcal{S}$, because the stopping condition of the procedure is precisely the condition of N being an ϵ-net of $\mathcal{S}$. Now, draw a ball of radius $\epsilon/2$ around each point of N: these balls are all disjoint, and they are all contained in the ball of radius $1 + \epsilon/2$

around the origin, so the number of steps that the above procedure can take is at most the ratio between the volume of a ball of radius $1 + \epsilon/2$ and a ball of radius $\epsilon/2$ in $\mathbb{R}^n$, and this ratio is at most $(c/\epsilon)^n$, for an absolute constant c. In particular, we have

Lemma 1 *There is an $1/4$-net N of the unit sphere in $\mathbb{R}^n$ such that $|N| \leq 2^{O(n)}$.*

We can use an ϵ-net to provide a combinatorial approximation of the operator norm.

Lemma 2 *If N is an $1/4$-net of the unit sphere, then*

$$||M|| \leq 2 \max_{y \in N} |y^T M y|$$

PROOF: Let x be a unit vector such that $|x^T M x| = ||M||$ and let y be a unit vector in N such that $||x - y|| \leq 1/4$, then

$$\begin{aligned}
||M|| &= |x^T M x| \\
&\leq |(x-y)^T M x| + |y^T M x| \\
&\leq |(x-y)^T M x| + |y^t M (x-y)| + |y^T M y| \\
&\leq ||x-y|| \cdot ||M|| \cdot ||x|| + ||y|| \cdot ||M|| \cdot ||x-y|| + |y^T M y| \\
&\leq \frac{1}{2} ||M|| + |y^T M y|
\end{aligned}$$

□

The optimum of the combinatorial problem $\max_{y \in N} |y^T W y|$ can be bounded using a Chernoff bound and a union bound. We first prove the Chernoff bound that we are going to use.

Lemma 3 *Let $r_1, \ldots, r_n$ be mutually independent ± 1 Rademacher random variables and let $a_1, \ldots, a_n$ be arbitrary real coefficients. Then, for every $t > 0$ we have*

$$\mathbb{P}\left[\sum_i r_i a_i \geq t\right] \leq e^{-\frac{t^2}{2 \sum_i a_i^2}}$$

PROOF: We are going to use the inequality

$$\frac{1}{2} e^x + \frac{1}{2} e^{-x} \leq e^{\frac{x^2}{2}}$$

which is true for every x and that is provable by looking at the difference between the Taylor series on the right and the Taylor series on the left, and seeing that the difference is a sum of even powers, and hence non-negative.

First, we have the inequalities

$$\mathbb{P}\left[\sum_i r_i a_i \geq t\right] = \mathbb{P}\left[e^{c \cdot \sum_i r_i a_i} \geq e^{ct}\right] \leq \frac{\mathbb{E}\, e^{c \cdot \sum_i r_i a_i}}{e^{ct}}$$

which hold for all $c > 0$ (we will optimize c later). Then we compute

$$\mathbb{E}\, e^{c \cdot \sum_i r_i a_i} = \prod_i \mathbb{E}\, e^{c r_i a_i} = \prod_i \left(\frac{1}{2} e^{c a_i} + \frac{1}{2} e^{-c a_i}\right) \leq \prod_i e^{c^2 a_i^2 / 2} = e^{c^2 \sum_i a_i^2 / 2}$$

Now we choose c so that

$$c^2 \sum_i \frac{a_i^2}{2} = \frac{ct}{2}$$

and we have the desired statement. □

Coming back to our goal of estimating the operator norm of a Wigner matrix W with Rademacher entries, if we fix any unit vector y we have

$$y^T W y = 2 \sum_{i<j} W_{i,j} y_i y_j$$

where $W_{i,j}$ are a collection of $\binom{n}{2}$ mutually independent Rademacher random variables, and the coefficients $y_i y_j$ satisy

$$\sum_{i<j} (y_i y_j)^2 \leq \frac{1}{2} \sum_{i,j} y_i^2 y_j^2 = \frac{1}{2} \left(\sum_i y_i^2\right)^2 = \frac{1}{2}$$

and so

$$\mathbb{P}[y^T W y > t] = \mathbb{P}\left[\sum_{i<j} W_{i,j} y_i y_j \geq \frac{t}{2}\right] \leq e^{-\frac{(t/2)^2}{2 \cdot 1/2}} = e^{-t^2/4}$$

Since the distribution of W is the same as the distribution of $-W$, we have

$$P[|y^T W y| > t] \leq 2 e^{-t^2/4}$$

If N is a set of unit vectors, a union bound gives us

$$\mathbb{P}\left[\exists y \in N: \ y^T W y > t\right] \leq |N| \cdot 2 \cdot e^{-t^2/4}$$

If N is a $1/4$-net of the unit sphere containing $2^{O(n)}$ elements,

$$\mathbb{P}[||W|| \geq t] \leq \mathbb{P}\left[\exists y \in N : |y^T W y| \geq t/2\right] \leq 2^{O(n)} \cdot e^{-\Omega(t^2)}$$

and so there is an absolute constant C such that if we choose $t = C \cdot \sqrt{n}$ the above probability is exponentially small in n.

Thus we have proved

Theorem 4 *There exists an absolute constant C such that the adjacency matrix A of a graph G sampled from $G_{n,\frac{1}{2}}$ satisfies, with probability $1 - 2^{-\Omega(n)}$,*

$$||A - \mathbb{E}\, A|| \leq C\sqrt{n}$$

2 The trace method

It is known that the operator norm of a Wigner matrix is concentrated around $(2 + o(1)) \cdot \sqrt{n}$. The technique that yields the above tight result is the *trace method*. The idea of the trace method is that, if M is a real symmetric matrix then for every integer k we have

$$||M||^{2k} \leq \mathrm{Tr}(M^{2k}) \leq n \cdot ||M||^{2k}$$

because, if $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of M, then

$$\mathrm{Tr}(M^{2k}) = \sum_i \lambda_i^{2k} = \sum_i |\lambda_i|^{2k}$$

and the above sum includes at least one term of value $||M||^{2k}$ and all the n terms are at most $||M||^{2k}$. Note that, if $k >> \log n$, $(\mathrm{Tr}(M^{2k}))^{1/2k}$ is a very good approximation of $||M||$.

If M is a random matrix, we also have

$$\mathbb{P}[||M|| \geq t] \leq \mathbb{P}[\mathrm{Tr}(M^{2k}) \geq t^{2k}] \leq \frac{\mathbb{E}\,\mathrm{Tr}(M^{2k})}{t^{2k}}$$

which is small if we take t to be a bit larger than $(\mathbb{E}\,\mathrm{Tr}(M^{2k}))^{1/2k}$

Our next goal will be to understand $\mathbb{E}\,\mathrm{Tr}(W^{2k})$, where W is a Wigner matrix.

We have

$$\mathbb{E}\,\mathrm{Tr}(W^{2k}) = \mathbb{E}\sum_i (W^{2k})_{i,i} = \sum_{i_1,i_2,\ldots,i_{2k}} \mathbb{E}\, W_{i_1,i_2} W_{i_2,i_3} \cdots W_{i_{2k-1}i_{2k}} W_{i_{2k}i_1}$$

we can characterize the terms in the summation in the following way

- If the sequence of unordered pairs $\{i_1, i_2\}, \{i_2, i_3\}, \cdots, \{i_{2k-1}, i_{2k}\}, \{i_{2k}, i_1\}$ is such that every unordered pair occurs in the sequence an even number of times, then

$$\mathbb{E}\, W_{i_1,i_2} W_{i_2,i_3} \cdots W_{i_{2k-1}i_{2k}} W_{i_{2k}i_1} = 1$$

- If the sequence of unordered pairs $\{i_1, i_2\}, \{i_2, i_3\}, \cdots, \{i_{2k-1}, i_{2k}\}, \{i_{2k}, i_1\}$ is such that at least one unordered pair occurs in the sequence an odd number of times, then

$$\mathbb{E}\, W_{i_1,i_2} W_{i_2,i_3} \cdots W_{i_{2k-1} i_{2k}} W_{i_{2k} i_1} = 0$$

This means that $\mathbb{E}\,\mathrm{Tr}(W^{2k})$ is equal to *the number of sequence* $i_1, \ldots, i_{2k} \in \{1, \ldots, n\}^{2k}$ *such that the sequence of unordered pairs* $\{i_1, i_2\}, \{i_2, i_3\}, \cdots, \{i_{2k-1}, i_{2k}\}, \{i_{2k}, i_1\}$ *has at least one unordered pair occurring an odd number of times.*

This number can be shown to be $(2+o(1))^{2k} \cdot n^{1+k/2}$, via fairly involved combinatorial arguments, and this gives the tight bound on the operator norm of Wigner matrices.

To give a sense of how one approaches such combinatorial problems, we will prove the weaker bound $2^{2k+1} \cdot n^{1+k} \cdot (k+1)^{k-1}$, which could be used to prove that the operator norm of Wigner matrices is, with high probability, $O(\sqrt{n \log n})$.

To prove the weaker bound, consider how much information we need to specify a sequence $i_1 \ldots i_{2k}$ with the specified property. Let us think of $V := \{1, \ldots, n\}$ as the vertex set of an undirected graph, and as $i_1, \ldots, i_{2k}$ as a sequence of vertices, with repetitions, that are encountered in the closed walk $i_1 \to i_2 \to \cdots \to i_{2k} \to i_1$, which traverses the edges $\{i_1, i_2\}, \ldots, \{i_{2k}, i_1\}$. Our condition is that every edge is traversed an even number of times, which means that at most k distinct edges are traversed a positive number of times. The vertices encountered in the closed walk form a connected graph together with the edges encountered in the closed walk, which means that the sequence $i_1, i_2, \ldots, i_{2k}$ contains at most $k+1$ distinct vertices.

This suffices to upper bound the number of sequences as being at most $n^{k+1} \cdot (k+1)^{2k}$, because there are at most n^{k+1} ways of choosing $k+1$ vertices and then at most $(k+1)^{2k}$ ways of creating a sequences of length $2k$ out of them. We will slightly improve this bound with a more careful accounting.

If we want to produce an bit-enconding of a sequence $i_1 \ldots i_{2k}$ with the required property, we can first use $2k$ bits to specify which position j corresponds to a vertex i_j encountered for the first time in the walk and which position j corresponds to a vertex i_j that had already been encountered before. Then we can list the distinct vertices occurring in the sequence, in the order in which they first occur, which takes $\ell \cdot \log_2 n$ bits if there are ℓ distinct vertices, and finally, for the remaining $2k - \ell$ positions, we have to specify which of the ℓ distinct vertices occurs there. In total we have

$$2k + \ell \cdot \log_2 n + (2k - \ell) \cdot \log_2 \ell$$

bits. Assuming $k << n$, we have $\ell << n$, and the above expression is larger for larger ℓ and is at most the value taken for the worst-case $\ell = k+1$

$$2k + (k+1)\log_2 n + (k-1) \cdot \log_2 k + 1$$

The number of distinct sequences that can be represented injectively using at most

T bits is at most 2^{T+1} and so the number of sequences with the property is at most $2^{2k+1} \cdot n^{k+1} \cdot (k+1)^{k-1}$.