RESEARCH DESCRIPTION

My main research interest lies in the interaction of Combinatorics and Probability. Most of my works in the past several years focus on a characterization problem that involves arithmetic structures and on several singularity and universality problems under probabilistic setting. Please see my cv for a complete list of publications.

1. Anti-concentration of inhomogeneous random walks

Some of my main interests are on the so-called Inverse Littlewood-Offord (ILO) problem. Let $x_i, i = 1, \dots, n$ be iid Bernoulli random variables, taking values ± 1 with probability $1/2$. Given a multiset A of n real number $a_1, \dots, a_n$, the (discrete) *concentration probability* of A is defined to be

$$\rho(A) := \sup_a \mathbf{P}\Big(\sum_{i=1}^n a_i x_i = a\Big).$$

Thus $\rho(A)$ is at least the returning probability $\mathbf{P}(\sum_{i=1}^n a_i x_i = 0)$ and this definition is . Motivated by their study of random polynomials, in the 1940s Littlewood and Offord [43] raised the question of bounding $\rho(A)$. They showed that if the a_i are nonzero then $\rho(A) = O(n^{-1/2} \log n)$. Shortly after the Littlewood-Offord paper, Erdős [24] gave a combinatorial proof of the refinement $\rho(A) \leq \binom{n}{n/2} 2^{-n}$.

Since the pioneer results of Erdős and Littlewood and Offord, there has been an impressive wave of reasearch to improve the inequality by imposing new assumptions on the a_i's. These improvements are reflected in the work of Erdős and Moser [23], Halász [30], Katona[39], Kleitman [40], Sárkőzy and Szemerédi [68], Stanley [75], and others.

About fifteen years ago, Tao-Vu and Rudelson-Vershynin brought a different view to the problem. We first discuss the work by Tao and Vu in [80, 81] where they tried to find the underlying reason as to why $\rho(A)$ is large, say $\rho(A) \geq n^{-C}$ for some $C > 0$. This creates a new direction called *inverse Littlewood-Offord problem*.

Let us introduce an important concept of additive structures, *generalized arithmetic progressions* (GAPs). A subset P of $\mathbf{R}$ is a *GAP of rank* r if it can be expressed as in the form

$$P = \Big\{g_0 + m_1 g_1 + \dots + m_r g_r | N_i \leq m_i \leq N_i', m_i \in \mathbf{Z}\Big\}.$$

The numbers g_i are the *generators* of P. The numbers N_i, N_i' are the *dimensions* of P. We say that P is *proper* if every element of P can be written in such linear combination in a unique way. If $-N_i = N_i'$ for all i and if $g_0 = 0$, we say that P is *symmetric*.

Assume that P is a proper symmetric GAP of rank $r = O(1)$ and size $n^{O(1)}$, and assume that all the elements of A are contained in P. Then, by the additive property $|nP| \leq n^r |P|$ of P, we easily have $\rho(V) = \Omega(n^{-O(1)})$. This example shows that if the elements of A belong to a symmetric proper GAP with a small rank and small cardinality, then $\rho(A)$ is very large. A few years ago, Tao and Vu [80, 81] proved several results showing that this is essentially the only reason:

Theorem 1.1. *Assume that $\rho(A) \geq n^{-C}$ for some $C > 0$, then most of the elements of A belong to a symmetric proper GAP of bounded rank $O(1)$ and of small size $n^{O(1)}$.*

We next introduce the independent work by Rudelson and Vershynin [63, 64] where they studied the (continuous) small ball probability $\rho_r(A) = \sup_a \mathbf{P}\Big(|\sum_{i=1}^n a_i x_i - a| \leq r\Big)$ in terms of common diophantine structures of the a_i. Fix parameters κ and γ (which may depend on n), where $\gamma \in (0,1)$, for any nonzero vector $(a_1, \dots, a_n)$ define the *least common denominator* to be

$$\mathbf{LCD}_{\kappa,\gamma}(A) := \inf\Big\{\theta > 0 : \mathrm{dist}((\theta a_1, \dots, \theta a_n), \mathbf{Z}^n) < \min(\gamma \|(\theta a_1, \dots, \theta a_n)\|_2, \kappa)\Big\}.$$

Theorem 1.2. *Assume that $a_1^2 + \dots + a_n^2 \geq 1$. Then, for every $\kappa > 0$ and $\gamma \in (0,1)$, and for $\varepsilon \geq 1/\mathbf{LCD}_{\kappa,\gamma}(x)$ we have*

$$\rho_\varepsilon(A) = O\Big(\frac{\varepsilon}{\gamma} + e^{-\Theta(\kappa^2)}\Big).$$

I have been trying to understand this phenomenon throughout the following notes.

1. **Almost optimal characterization**. In a joint work with Vu [60] we gave a fine characterization of random walks of large concentration probability with optimal dependences of the parameters; we also showed that if the small ball probability is large, then most of the entries a_i are very close to a GAP of small cardinality and small rank. This result was used in [12, 19, 51, 52, 53, 58, 59].

2. **Multilinear forms**. One can view the quantity $\sum_{i=1}^n a_i x_i$ in the definition of $\rho(A)$ as a linear form of the random vector $\mathbf{x} = (x_1, \dots, x_n)$. It is natural to generalize the concept to higher degree polynomial. For simplicity, let us focus on quadratic forms. Given an $n \times n$ symmetric matrix $A = (a_{ij})$ of real entries, we define the *quadratic concentration probability* of A by

$$\rho_q(A) := \sup_{a \in \mathbf{R}} \mathbf{P}\Big(\sum_{i,j} a_{ij} x_i x_j = a\Big).$$

It was shown in [14, 15], as a nontrivial application of the Erdős and Littlewood-Offord inequality, that if most of the coefficients a_{ij} are nonzero, then $\rho_q(A) \leq n^{-1/2+o(1)}$. This bound is almost best possible, as demonstrated by the quadratic form $\sum_{ij} x_i x_j$. In the reverse direction, we would like to characterize those A which have large quadratic concentration probability. In this setting, there are two different sources of examples where $\rho_q(A)$ can be large. The first source comes from additive structures: assume that all the coefficients a_{ij} belong to a GAP of small rank $O(1)$ and small size $n^{O(1)}$, then similar to the linear case, one has $\rho_q(A) = n^{-O(1)}$. The second source has an algebraic nature: if the matrix A has low rank, such as $a_{ij} = k_i b_j + k_j b_i$ with arbitrary b_i and with integers k_i so that $\mathbf{P}(\sum_i k_i x_i = 0) = n^{-O(1)}$, then the probability $\mathbf{P}(\sum_{i,j} a_{ij} x_i x_j = 0)$ has order of $n^{-O(1)}$. In general, if a_{ij} can be decomposed into additive and algebraic structures as above, then $\rho_q(A)$ is also large. In [50], I was able to prove that these are essentially the only examples that have large quadratic concentration probability.

In a joint work with O'Rourke [57] we continued to study the anti-concentration of multilinear forms of bounded degree, giving a weak characterization. These results were applied in [50, 56, 57].

3. **Non-abelian setting**. The concentration probability can be extended to $a_i \in G$ for general non-abelian group G,

$$\rho(a_1, \dots, a_n) := \sup_a \mathbf{P}\Big(\prod_{i=1}^n a_i^{x_i} = a\Big),$$

where $x_i, i = 1, \dots, n$ are iid Bernoulli random variables.

Let $u_1, \dots, u_r$ be elements of G, and let $(N_1, \dots, N_r)$ be a vector of positive integers. Then the set of all products in the u_i and their inverses in which each u_i and its inverse appear at most N_i times is called a *progression of rank r and size lengths $N_1, \dots, N_r$*, and is denoted by $P(u_1, \dots, u_r; N_1, \dots, N_r)$ (or P for short). A *nilprogression* of rank r and step s is a progression $P(u_1, \dots, u_r; N_1, \dots, N_r)$ with the property that every iterated commutator of degree $s+1$ in the generators $u_1, \dots, u_r$ equals the identity id_G. A *coset nilprogression* of rank r and step s is a set of the form $\pi^{-1}(P)$, where P is a nilprogression of rank r and step s in a quotient group G_0/H, where H is a finite normal subgroup of a subgroup G_0 of G and $\pi : G_0 \to G_0/H$ is the quotient map.

Similarly to the abelian case, elements of a coset nilprogression of small cardinality are examples of sets of high concentration probability. By adapting the method of [10, 78], I was able to obtain the converse of the above (in a rather weak sense) that if $\rho(a_1, \dots, a_n) \geq n^{-O(1)}$ then $n^{1-o(1)}$ consecutive elements a_i belong to a coset nilprogression of cardinality $n^{O(1)}$ with $r, s = O(1)$ (please see [54]).

A common feature of our results is that the random variables x_i can be fairly general. For instance the results in (1) and (2) are valid for any x_i of finite $(2+\varepsilon)$-moment for $\varepsilon > 0$.

2. Singularity and universality in random matrices and random polynomials

For most of the results listed below the related statistics in the Gaussian case are either trivial or well studied; we show that these statistics are asymptotically universal (at least at the macroscopic level) with respect to the random inputs. Techniques used to prove these results include anti-concentration results (Section 1), comparison methods (such as the Lindeberg exchange method), and various tools from combinatorics (to deal with ± 1 randomness) and from basic geometric analysis and linear algebra (to deal with matrices and with high dimensional objects). The general theme looks quite similar but each problem requires a different set of ideas.

First allow us to discuss a couple of results on roots of random polynomials.

1. **Expected number of real roots of Kac polynomials**. Let ξ be a real random variable having no atom at 0, zero mean and unit variance. Our object of study is the random polynomial $P_n(x) := \sum_{i=0}^n \xi_i x^i$, where ξ_i are iid copies of ξ. This polynomial is often referred to as Kac's polynomial, and has been extensively investigated in the literature.

Let N_n be the number of real roots of $P_n(x)$. The issue of estimating N_n was already raised by Waring as far back as 1782 ([85, page 618], [41]), and has generated a large amount of literature. Extending earlier results by Bloch and Pólya [6], in a series of breakthrough papers [44, 45, 46, 47] in the early 1940s, Littlewood and Offord proved (for many atom variables ξ such as Gaussian, Bernoulli or uniform on $[-1, 1]$) that with probability $1 - o(1)$, $\frac{\log n}{\log \log \log n} \ll N_n \ll \log^2 n$.

Around the same time, Kac [36] developed a general formula for the expectation of number of real roots

$$\mathbf{E}N_n = \int_{-\infty}^{\infty} dt \int_{-\infty}^{\infty} |y| p(t, 0, y) dy,$$

where $p(t,x,y)$ is the probability density for $P_n(t) = x$ and $P'_n(t) = y$. In the Gaussian case, one can easily evaluate the RHS and get

$$\mathbf{E}N_{n,\mathbf{N}(0,1)} = \frac{1}{\pi}\int_{-\infty}^{\infty}\sqrt{\frac{1}{(t^2-1)^2}+\frac{(n+1)^2t^{2n}}{(t^{2n+2}-1)^2}}dt = (\frac{2}{\pi}+o(1))\log n.$$

For non-Gaussian distributions, however, Kac's formula is often very hard to evaluate. In a subsequent paper [37], Kac himself handled the case when ξ is uniformly distributed on the interval $[-1,1]$ and Stevens [76] extended it further to cover a large class of ξ having continuous and smooth distributions with certain regularity properties. For discrete distributions, the integral formula does not appear useful and it took a while until Erdős and Offord in 1956 [25] found a completely new approach to handle the Bernoulli case. For this case, they proved that with probability $1 - o(\frac{1}{\sqrt{\log\log n}})$

$$N_n = \frac{2}{\pi}\log n + o(\log^{2/3} n \log\log n).$$

In the late 1960s and early 1970s, Ibragimov and Maslova [31, 32, 33, 34] successfully refined Erdős-Offord's method to handle any variable ξ with mean 0. They proved that for any ξ with mean zero which belong to the domain of attraction of the normal law,

$$\mathbf{E}N_n = \frac{2}{\pi}\log n + o(\log n).$$

Other developments were made in the late 1980s by Wilkins [87] and in the early 1990s by Edelman and Kostlan [19], who evaluated the explicit integral formula above very carefully and provided a precise estimate for the Gaussian case

$$\mathbf{E}N_{n,\mathbf{N}(0,1)} = \frac{2}{\pi}\log n + C_{\mathbf{N}(0,1)} + o(1).$$

where $C_{\mathbf{N}(0,1)} \approx .625738072..$ is an explicit constant (and one can even write $o(1)$ as sum of explicit functions of n, which gives a complete Taylor expansion.) The remarkable fact about the integral formula is that the error term $\mathbf{E}N_{n,\mathbf{N}(0,1)} - \frac{2}{\pi}\log n$ tends to a limit as n tends to infinity. Numerical evidence tends to support the conjecture that $\mathbf{E}N_n - \frac{2}{\pi}\log n$ do go to a limit, as n to tends to infinity. However, the situation is delicate as this limit seems to depend on the distribution of the atom variable ξ and *is not* universal. In a joint work with O. Nguyen and V. Vu [58] we made a first step by showing that the error term in question is bounded.

Theorem 2.1. *Let ξ be a random variable with mean zero and variance one and bounded $(2+\epsilon)$-moment. Then*

$$|\mathbf{E}N_{n,\xi} - \frac{2}{\pi}\log n| = O_{\epsilon,\xi}(1).$$

In a more recent result, with Y. Do and V. Vu [19] we answered this problem for a natural class of distributions, as an application of a general theorem concerning the repulsion between real roots of Kac's polynomials.

For any positive integer N, we say that ξ has uniform distribution with parameter N (or *type I*) if $\mathbf{P}(\xi = i) = 1/(2N)$ independently, $i \in \{\pm 1, \pm 2, \dots, \pm N\}$. Furthermore, we say that a random variable ξ of mean zero has *type II* distribution with parameter (p, ε_0) if its has a p-integrable density function and its $(2+\varepsilon_0)$-moment is bounded.

Theorem 2.2. *Let ξ be a random variable with either type I or type II with fixed parameters. Then*

$$\mathbf{E}N_{n,\xi} = \frac{2}{\pi}\log n + C_\xi + o(1),$$

where C_ξ is an absolute constant depending on ξ.

2. **Universality for the number of intersections for random eigenfunctions on flat tori**. Let $\mathcal{M}$ be a smooth Riemannian manifold. Let F be a real-valued eigenfunction of the Laplacian on $\mathcal{M}$ with eigenvalues λ^2,

$$-\Delta F = \lambda^2 F.$$

The nodal set N_F is defined to be

$$N_F := \{x \in \mathcal{M}, F(x) = 0\}.$$

The study of N_F is extremely important in analysis and differential geometry. Here we are simply interested in the case when $\mathcal{M}$ is the flat tori $\mathbf{T}^d = \mathbf{R}^d/\mathbf{Z}^d$ with $d \geq 2$; more specifically we will be focusing on the intersection set of N_F with a given reference curve.

Let $\mathcal{C} \subset \mathcal{M}$ be a curve assumed to have unit length with the arc-length parametrization $\gamma : [0,1] \to \mathcal{M}$. The nodal intersection between F and $\mathcal{C}$ is defined as

$$\mathcal{Z}(F) := \#\{x : F(x) = 0\} \cap \mathcal{C}.$$

It is known that all eigenvalues λ^2 have the form $4\pi^2 m, m \in \mathbf{Z}^+$. Let $\mathcal{E}_\lambda$ be the collection of $\mu = (\mu_1, \mu_2) \in \mathbf{Z}^2$ such that

$$\mu_1^2 + \mu_2^2 = m.$$

Denote $N = N_m = \#\mathcal{E}_\lambda$, that is $N = r_2(m)$. The toral eigenfunctions $f(x) = e^{2\pi i\langle \mu, x\rangle}, \mu \in \mathcal{E}_\lambda$ form an orthonormal basis in the eigenspace corresponding to λ^2. The following determinisitic results due to Bourgain and Rudnick are gathered from [4, 5, 6].

Theorem 2.3. *Let $\mathcal{C} \subset \mathbf{T}^2$ be a real analytic curve with nowhere vanishing curvature, then*

$$\lambda^{1-o(1)} \leq \mathcal{Z}(F) \leq c\lambda,$$

where the implied constants depend on γ.

We next introduce a probabilistic setting first studied by Rudnick and Wigman [66]. Consider the random Gaussian function

$$F(t) = \frac{1}{\sqrt{N}} \sum_{\mu \in \mathcal{E}_\lambda} \varepsilon_\mu e^{2\pi i\langle \mu, \gamma(t)\rangle},$$

where ε_μ are iid complex standard Gaussian with a saving $\varepsilon_{-\mu} = \bar{\varepsilon}_\mu$ so that F is real valued.

The random function F is called *arithmetic random wave* [3, 42], whose distribution is invariant under rotation by the Gaussian property of the coefficients. The following are main results from [66] and [67].

Theorem 2.4. *Let $\mathcal{C} \subset \mathbf{T}^2$ be a smooth curve on the torus, with nowhere vanishing curvature and of total length one. Then the expected number of nodal intersections is $\mathbf{E}_\mathbf{g}\mathcal{Z} = \sqrt{2m}$ and the variance is bounded by $\mathrm{Var}_\mathbf{g}(\mathcal{Z}) = O(\frac{m}{N})$. Furthermore, for a generic m*

$$\mathrm{Var}_\mathbf{g}(\mathcal{Z}) = \frac{m}{N}\int_\mathcal{C}\int_\mathcal{C} 4\Big(\frac{1}{N}\Big\langle \frac{\mu}{|\mu|}, \dot\gamma(t_1)\Big\rangle^2 \Big\langle \frac{\mu}{|\mu|}, \dot\gamma(t_2)\Big\rangle^2 - 1\Big) dt_1 dt_2 + O(\frac{m}{N^{3/2}}).$$

In a subsequent paper, Rudnick, Wigman and Yesha [67] also studied the problem for $\mathbf{T}^3$ and obtained some partial results. Roughly speaking, the proofs of these results are based on Kac-Rice formula, but because this formula is not valid uniformly, the authors had to chop the curve into many pieces to remove certain unpleasant singularity.

Motivated by the universality phenomenon in probability, together with M-C. Chang, O. Nguyen and V. Vu [12] we studied the behavior of $\mathcal{Z}(F)$ for other random eigenfunctions F beside the Gaussian ones. More specifically, consider the random function

$$F(t) = \frac{1}{\sqrt{N}} \sum_{\mu \in \mathcal{E}_\lambda} \varepsilon_\mu e^{2\pi i \langle \mu, \gamma(t) \rangle},$$

where $\varepsilon_\mu = \varepsilon_{1,\mu} + i\varepsilon_{2,\mu}$ and $\varepsilon_{1,\mu}, \varepsilon_{2,\mu}, \mu \in \mathcal{E}_\lambda$ are iid random variables with the saving constraint $\varepsilon_{-\mu} = \bar{\varepsilon}_\mu$. We were able to show that

Theorem 2.5. *With generic λ and γ, and for iid random variables ε_μ of mean zero, variance one and of bounded $(2+\varepsilon)$-moment, for any fixed k we have*

$$\mathbf{E}_{\varepsilon_\mu} \mathcal{Z}^k = \mathbf{E}_{\mathbf{g}} \mathcal{Z}^k + O(\lambda^k / N^c),$$

where $c = c(k, \gamma) > 0$ is an absolute constant.

This seems to be the first ever universality result (in terms of randomness) for the random wave model.

3. **Polynomial systems of many variables**. Let $\mathbf{d} = (d_1, \dots, d_{n-1})$ be a degree sequence, and $\mathbf{f} = \{f_1, \dots, f_{n-1}\}$ be a collection of $n-1$ homogeneous polynomials in n variables of degree $d_1, \dots, d_{n-1}$ respectively, where $f_l(x_1, \dots, x_n) = \sum_{\substack{\alpha=(\alpha_1,\dots,\alpha_n) \\ \alpha_1+\dots+\alpha_n=d_l}} \binom{d_l}{\alpha}^{1/2} a_\alpha{}^{(l)} \mathbf{x}^\alpha$ with $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

In their seminal works [69, 70, 71, 72, 73], Shub and Smale initiated a systematic study of Newton's method for finding common roots of the f_i over the unit vectors in $\mathbf{C}^n$.

Define the Weyl-norm of the system $\mathbf{f}$ by $\|\mathbf{f}\|_W := \sqrt{\|f_1\|_W^2 + \dots + \|f_{n-1}\|_W^2}$, where $\|f_l\|_W^2 := \sum_\alpha |a_\alpha^{(l)}|^2$. We denote the condition number of the system by

$$\mu_{complex}^{(1)}(\mathbf{f}) := \sup_{\mathbf{x} \in S^{n-1}, f_1(\mathbf{x}) = \dots = f_{n-1}(\mathbf{x}) = 0} \|\mathbf{f}\|_W \times \|(D_{\mathbf{x}}|_{T_{\mathbf{x}}})^{-1} \Delta\|_2.$$

where $D_{\mathbf{x}}|_{T_{\mathbf{x}}}$ is the Jacobian of the system $\mathbf{f}$ restricted to the tangent space at $\mathbf{x}$, and Δ is the diagonal matrix of entries $(\sqrt{d_l}, 1 \le l \le n-1)$.

To analyze the effectiveness of Newton's method for finding commons roots of the f_i, Shub and Smale [70], and independently Kostlan [29] show that, under an invariant probability measure (i.e. when the coefficients $a_\alpha^{(l)}$ are iid standard Gaussian), the condition number of $\mathbf{f}$ is small with high probability.

Theorem 2.6. *Assume that the coefficients $a_\alpha^{(l)}$ are iid standard complex-Gaussian random variables, then*

$$\mathbf{P}(\mu_{complex}^{(1)}(\mathbf{f}^{Gau}) > 1/\varepsilon) = O(n^4 N^2 \mathcal{D} \varepsilon^4).$$

Here $\mathcal{D} := \prod d_i$ is the Bezout number and $N := \sum_{i=1}^{n-1} \binom{n-1+d_i}{d_i}$. Roughly speaking, Theorem 2.6 asserts that with high probability all the common roots of the f_i are far from being multiple. This is a crucial ingredient in Shub-Smale's analysis of Newton's method.

Beside finding common complex roots, another important problem is to find common real roots. In a recent series [16, 17, 18], Cucker, Krick, Malajovich and Wschebor have studied this problem in detail.

For convenience, Cucker et. al. introduced the following more general condition number.

$$\mu^{(2)}_{real}(\mathbf{f}) := \sup_{\mathbf{x}\in S^{n-1}} \min\Big\{\sqrt{n}\max_i \|f_i\|_W \times \|(D_{\mathbf{x}}|_{T_{\mathbf{x}}})^{-1}\Delta\|_2, \frac{\max_i \|f_i\|_W}{\max_i |f_i(\mathbf{x})|}\Big\}.$$

With respect to this condition number, Cucker, Krick, Malajovich and Wschebor [18] were able to give an analog of Theorem 2.6, again for Gaussian system. Roughly speaking (see for instance [16] or [11, Section 19]), Cucker, Krick, Malajovich and Wschebor showed that there exists an iterative algorithm that returns the number of real zeros of $\mathbf{f}$ and their approximations and performs $O(\log(nD\mu^{(2)}_{real}(\mathbf{f})))$ iterations with a total cost of $O([C(n+1)D^2(\mu^{(2)}_{real})^2]^{2(n+1)}N\log(nD\mu^{(2)}_{real}(\mathbf{f}))$. Henceforth, the probabilistic analysis of $\mu^{(2)}_{real}$ plays a key role in their study.

The proofs of Shub and Smale regarding $\mu^{(1)}$, and of Cucker et. al. regarding $\mu^{(2)}$, on the other hand, heavily rely on the invariance property of (real and complex) Gaussian distributions, and are extremely involved. Under the universality and the "smoothed analysis" point of view (see for instance [74]), it is natural and important to study the condition numbers $\mu^{(1)}$ and $\mu^{(2)}$ for polynomial systems under more general distributions such as Bernoulli. This problem is also closely related to a question raised by P. Burgisser and F. Cucker in [11, Problem 7]. By using the geometric technique developed by Rudelson and Vershynin [63], I was able to partially analyze the behavior of $\mu^{(2)}$ under discrete distributions (for slightly perturbed systems), we extract here a simplified version.

Theorem 2.7. [52] *Assume that $a^{(l)}_\alpha$ are iid Bernoulli random variables. Then with probability tending to one, there does not exist non-zero vector $\mathbf{x}\in\mathbf{R}^n$ with $\mathbf{f}(\mathbf{x})=0$ and $\mathrm{rank}(D_{\mathbf{x}}|_{T_{\mathbf{x}}}) < n-1$.*

We next turn to random matrices.

1. **Wegner-type estimate for eigenvalue repulsion**. Gaps between consecutive eigenvalues have a central place in the theory of random matrices. The limiting (global) gap distribution for gaussian matrices (GUE and GOE) has been known for some time [48]. Recent progresses on the universality conjecture showed that these limiting distributions are universal with the class of Wigner matrices. However, at the microscopic level, there are many open problems concerning basic questions.

The first natural question is the limiting distribution of a given gap $\delta_i := \lambda_{i+1} - \lambda_i$. For GUE, this was computed very recently by Tao [77]. Within the class of Wigner matrices, again the four moment theorem by Tao and Vu [82] asserts that this distribution is universal, provided the four matching moment condition. The matching moment condition was recently removed by Erdős and Yau [22] using sophisticated techniques from the theory of parabolic PDE to analyze a Dyson Brownian motion, allowing for a computation of the gap distribution for random matrix ensembles such as the GOE or Bernoulli ensembles.

Another issue is to understand the size of the *minimum* gap $\delta_{\min} := \min_{1\le i\le n-1}(\delta_{i+1}-\delta_i)$. For the GUE ensemble, Bourgade and Ben-Arous [7] showed that the minimum gap $\delta_{\min}$ is of order $n^{-5/6}$ and computed the limiting distribution. We are not aware of a polynomial lower bound (of any fixed exponent) for δ_{min} for discrete random matrices, which are of importance in applications in random graph theory and theoretical computer science. Even proving that $\delta_{\min} > 0$ (in other words the random matrix has simple spectrum) with high probability in the discrete case is already a highly non-trivial problem, first raised by Babai in the 1980s (motivated by his study of the isomorphism problem [2]). This latter problem was solved only very recently by Tao and Vu.

For Wigner matrices, by the semi-circle law [48], most eigenvalues are in the interval $[-2\sqrt{n}, 2\sqrt{n}]$, thus the average gap is of order $n^{-1/2}$. The question is to estimate the probability that a particular gap is significantly smaller than the average.

We now continue to discuss a few results related to this question. Tao and Vu showed in [82] that for every constant $c_0 > 0$ there exists $c_1 > 0$ such that for Wigner matrices and for fixed $\varepsilon > 0$ one has $\sup_{\varepsilon n \le i \le (1-\varepsilon)n} \mathbf{P}(\delta_i \le n^{-c_0 - \frac{1}{2}}) \ll n^{-c_1}$. The weakness of this theorem is that c_1 is small (much smaller than 1, regardless the value of c_0), and thus one cannot use the union bound to conclude that $\delta_i > 0$ simultaneously for all i.

In [20], Erdős et. al. proved for real Wigner matrices $\frac{1}{n}\sum_{\varepsilon n \le i \le (1-\varepsilon)n} \mathbf{P}(\delta_i \le \delta n^{-1/2}) \ll \delta^2$, for any constant $\varepsilon, \delta > 0$, with a similar result also available at the edge of the spectrum. The quadratic decay δ^2 here comes from an eigenvalue repulsion phenomenon, reflecting the first-order decay of the two-point correlation function $\rho_2(x, y)$ of the GOE ensemble as one approaches the diagonal $x = y$. However, this result only give a bound on the average probability, and furthermore δ needs to be a constant. Under some strong smoothness and decay hypotheses on the entries of a Hermitian Wigner matrix X_n, it was shown by Erdős, Schlein, and Yau [21] that one has the Wegner estimate

$$\mathbf{P}\left(En^{1/2} - \delta n^{-1/2} \le \lambda_i \le \lambda_{i+l} \le En^{1/2} + \delta n^{-1/2} \text{ for some } i\right) \ll \delta^{(l+1)^2}$$

for any fixed $l \ge 1$ and any $\varepsilon > 0$ and any bounded $E \in \mathbf{R}$. An analogue of this result for real smooth ensembles, with the exponent k^2 replaced by $k(k+1)/2$, was established in [9, Appendix B]. In a recent paper with Tao and Vu we showed following.

Theorem 2.8 ([59])**.** *There is a constant $0 < c < 1$ such that the following holds for the gaps $\delta_i := \lambda_{i+1}(X_n) - \lambda_i(X_n)$ of real symmetric Wigner matrices X_n. For any quantities $n^{-c} \le \alpha \le c$ and $\delta \ge n^{-c/\alpha}$, we have*

$$\sup_{1 \le i \le n-1} \mathbf{P}(\delta_i \le \delta n^{-\frac{1}{2}}) = O\Big(\frac{\delta}{\sqrt{\alpha}}\Big).$$

More generally, one can take $c_1 = 1, c_2 = 3$, $c_l \ge \frac{l^2+2l}{3}$ for $l \ge 3$ so that

$$\sup_{1 \le i \le n-l} \mathbf{P}(|\lambda_{i+l}(X_n) - \lambda_i(X_n)| \le \delta n^{-\frac{1}{2}}) = O\Big(\Big(\frac{\delta}{\sqrt{\alpha}}\Big)^{c_l}\Big).$$

Note that in the first statement, taking $\alpha = n^{-c}$ implies that X_n has multiple eigenvalues with probability at most $O(\exp(-n^c))$ for some constant $c > 0$, this result improves over [84]. The key feature of our result is that the bound δ^{c_l} yields the evidence of *quadratic* repulsion between nearby eigenvalues.

2. **Logarithmic determinant**. As determinant is one of the most fundamental matrix functions, it is a natural problem in the theory of random matrices to study the distribution of its determinant. Motivated by a result of Goodman [28], and of Girko [27], together with Vu we showed the following

Theorem 2.9 ([61])**.** *Assume that the entries $a_{ij}, 1 \le i, j \le n$ of an n by n matrix are iid Bernoulli taking values ± 1 with probability 1/2, then*

$$\sup_{x \in \mathbf{R}} \Big|\mathbf{P}\big(\frac{\log(|\det A_n|) - \frac{1}{2}\log(n-1)!}{\sqrt{\frac{1}{2}\log n}} \le x\big) - \mathbf{P}(\mathbf{N}(0,1) < x)\Big| \le \log^{-1/3+o(1)} n.$$

In fact this theorem holds for much more general distributions of mean zero and variance one. Note that we can rewrite the statistics under consideration as $\sum_i f(\lambda_i)$, with $f(x) = \log|x|$ and λ_i are

the singular values of A_n. These (normalized and non-normalized) statistics have been studied quite extensively in the literature, mostly under various smoothness assumption on f. Unfortunately these treatments do not extend to our problem due to the singularity of $\log x$.

Roughly speaking, the proof of Theorem 2.9 relies on the fact that the determinant can be written as product of distances d_i from the i-th column $\mathbf{c}_i$ to the subspace generated by columns $\mathbf{c}_{i+1}, \dots, \mathbf{c}_n$. For random matrices of iid entries, these quantities can be controlled rather precisely via tools of concentration of measure. The CLT then follows by the "independence" of these distances d_i.

The situation for Wigner matrices W_n is more subtle mainly by two reasons. Firstly, as the symmetric entries are dependent, the subspaces now depends on the columns, and so the task to control the distances becomes harder. Secondly, the distances d_i are not "independent" anymore so that one can apply CLT for martingales. One can overcome the second point by using the co-factor expansion to write the determinant $det(W_n)$ into product form $\prod_{i=1}^n w_i$, where each w_i can be expressed as a quadratic form $\sum_{1\leq k,l\leq i} a_{kl}x_k x_l$, with x_k being iid and independent from $(a_{kl})_{1\leq k,l\leq i}$, the entries of the inverse matrix W_i^{-1} with W_i being the principle minor of size i of W_n. However, as W_i^{-1} is rather unstable, this direct method does not seem to work. Nevertheless, Tao and Vu [83] were able to obtain a CLT-type result for $\log|\det(W_n)|$ as long as the entries are iid copies of a real random variable ξ satisfying the matching moment condition up to fourth order.

Theorem 2.10. *Assume that $a_{ij}, 1 \leq i \leq j \leq n$ are iid copies of a real random variable ξ such that $\mathbf{E}\xi^k = \mathbf{E}(\mathbf{N}(0,1)^k), 1 \leq k \leq 4$. Then*

$$\frac{\log|\det W_n| - \frac{1}{2}\log n! + \frac{1}{4}\log n}{\sqrt{\log n}} \to \mathbf{N}(0,1).$$

The key ingredient of this result of Tao and Vu is their four-moment matching theorem from [82]. This approach is very useful but it excludes many interesting ensembles such as the Bernoulli case.

3. **Normal vectors**. Fixed a random variable ξ of mean zero and variance one and consider the random vector $\mathbf{v} = (\xi_1, \dots, \xi_n)$, whose entries are iid copies of ξ. Sample $n-1$ iid copies $\mathbf{v}_1, \dots, \mathbf{v}_{n-1}$ of $\mathbf{v}$. We would like to study the normal vector of the hyperplane spanned by the $\mathbf{v}_i$. In matrix term, we let $A = (a_{ij})_{1\leq i\leq n-1, 1\leq j\leq n}$ be a random matrix of size $n-1$ by n where the entries a_{ij} are iid copies of ξ; the $\mathbf{v}_i$ are the row vectors of A. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{F}^n$ be a unit vector that is orthogonal to the $\mathbf{v}_i$ (Here and later $\mathbf{F}$ is either $\mathbf{R}$ or $\mathbf{C}$, depending on the support of ξ.) First note that recent studies in the singularity probability of random non-Hermitian matrices (such as [63, 80]) show that under very general conditions on ξ, with extremely high probability A has rank $n-1$. In this case $\mathbf{x}$ is uniquely determined up to the sign ± 1 when $\mathbf{F} = \mathbf{R}$ or by a uniformly chosen rotation $\exp(\mathbf{i}\theta)$ when $\mathbf{F} = \mathbf{C}$.

When the entries of A are iid standard gaussian $\mathbf{g_F}$, it is not hard to see that $\mathbf{x}$ is distributed as a random unit vector sampled according to the Haar measure in S^{n-1} of $\mathbf{F}^n$. Motivated by the universality phenomenon, it is natural to ask if these properties are universal, namely that they hold if ξ is non-gaussian. In [62] we confirms this prediction in a strong sense.

Theorem 2.11. *Suppose that a_{ij} are iid copies of a normalized sub-gaussian random variable ξ, i.e. $\mathbf{P}(|\xi| \geq t) = O(\exp(-ct^2))\forall t$, then the followings hold.*

- *There are constants $C, C_1 > 0$ such that for any $m \geq C_1 \log n$*

$$\mathbf{P}(\|\mathbf{x}\|_\infty \geq \sqrt{m/n}) \leq Cn^2 \exp(-m/C).$$

- *There exists a positive constant c such that the following holds: for any d-tuple $(i_1, \dots, i_m)$, with $d = n^c$, the joint law of the tuple $(\sqrt{n}x_{i_1}, \dots, \sqrt{n}x_{i_d})$ is asymptotically independent standard normal.*

This result implies a few other things such as control of entries of the inverse matrix of random iid matrices. It also helps verify the bound $\mathbf{P}(\sigma_n \geq tn^{-1/2}) \leq C_1 \exp(-C_2 t)$ where σ_n is the least singular value of a random iid matrix.

4. **Lyapunov exponents for random matrices**. Let $A_i, i \geq 1$ be a sequence of independent identically distributed random matrices of a given distribution μ in the space of square matrices of size n of real-valued entries. Let B_N be the matrix product

$$B_N = A_1 \dots A_N.$$

Assume that $\mathbf{E} \log^+(\|A_i\|) < \infty$. The Lyapunov exponents $\gamma_1, \dots, \gamma_n$ associated to A_i are defined inductively by $\gamma_1 = \gamma$ and for $k \geq 2$,

$$\sum_{i=1}^{k} \gamma_i = \lim_{N \to \infty} \frac{1}{N} \mathbf{E} \log \| \wedge^k B_N \|.$$

Following the two celebrated results of Furstenberg and Oseledec, for some nice distribution μ it is natural to ask if we can give fine approximation for the Lyapunov's exponents or a quantification of the rate of convergence.

These aspects have been widely studied by many researchers, especially for unimodular and/or symplectic matrices of fixed size in connection to the theory of Schrödinger operators. Our main focus is on a model of random matrices of *large* dimension which are not necessarily unimodular. Especially, we will consider those A_i random matrices where the entries are iid copies of a common real random variable ξ of mean zero and variance $1/n$. This ensemble had been considered by Cohen, Isopi and Newman in the 80s [13, 35, 49] in connection to May's proposal of a specific quantitative relationship between complexity and stability within certain ecological models.

Theorem 2.12. [49, Equation (6)] *Assume that the entries of A_i are iid copies of $\frac{1}{\sqrt{n}} N(0,1)$. Let $\mu_1 \geq \dots \geq \mu_n$ be the Lyapunov's exponents of the matrix product B_N. Then*

$$\mu_i = \frac{1}{2}(\log 2 + \Psi(\frac{n-i+1}{2}) - \log n),$$

where $\Psi(d) = \Gamma'(d)/\Gamma(d)$ is the digamma function.

This result was also generalized in [35] to ξ having bounded density and $\mathbf{E}((\sqrt{n}\xi)^4) < \infty$. These results address the values of the exponents for various random matrices of smooth type. For speed of convergence, the only result we found for the iid model is due to Kargin [38, Proposition 3] who considered the rate of convergence of the top exponents.

Theorem 2.13. *Let $\varepsilon > 0$ be given. Assume that the entries of A_i are iid copies of $\frac{1}{\sqrt{n}} N(0,1)$. Then for all sufficiently small t, and all $n \geq n_0(t)$ and $N \geq 1$*

$$\mathbf{P}(|\frac{1}{N} \log \|B_N\|| > t + \varepsilon/N) \leq 2(1 + 2/\varepsilon)^n \exp(-\frac{1}{8} N n t^2).$$

As we have mentioned, all of the results in the literature with respect to the iid model assumed the common distribution ξ to be sufficiently smooth so that $\frac{1}{N} \log \|B_N\|$ with $N \to \infty$ is well defined almost surely. The smoothness assumption is natural, as if A_i were singular with positive probability,

then our chain B_N would become singular with probability one; in this case it is still reasonable to study the top Lyapunov exponent but not other exponents. However, even when the exponents are not well defined, can we still say useful things about the growth of the chain B_N for some *effective* range of N? This question is natural because in many practical problems, it is not known a priori that our random matrix model is smooth. In addition, to estimate the Lyapunov's exponents using computer, one actually computes $\frac{1}{N}\log \sigma_i(B_N)$ for some sufficiently large (but not too large) N.

Trying to address these issues, with a universality approach in mind, we considered the matrix models A_i where the entries of $\sqrt{n}A_i$ are iid copies of a subgaussian random variable ξ of mean zero, variance one. One representative example of our matrices is the iid Bernoulli ensemble. In [53] I was able to show

Theorem 2.14. *There exist constants c, C depending on ε, ξ such that the followings hold.*

- *For any $t \geq 1/n$ we have*

$$\mathbf{P}\Big(|\frac{1}{N}\log \|B_N\|| \geq t + \varepsilon/N)\Big) \leq (1+2/\varepsilon)^n\big[\exp(-c\min\{t^2,t\}Nn) + Nn^{-cn}\big].$$

- *For any $t \geq 1/n$ we have*

$$\mathbf{P}\Big(|\frac{1}{N}\log \sup_{\mathbf{x}_1\in S^{n-1},\mathbf{x}_2\in S^{n-1}} \|B_N\mathbf{x}_1 \wedge B_N\mathbf{x}_2\|| \geq t+\varepsilon/N)\Big) \leq (1+2/\varepsilon)^n\big[\exp(-c\min\{t^2,t\}Nn)+Nn^{-cn}\big].$$

- *We also have*

$$\mathbf{P}\Big(\inf_{\mathbf{x}\in S^{n-1}} \frac{1}{N}\log \|B_N\mathbf{x}\| \leq -(\frac{1}{2}+\varepsilon)\log n\Big) \leq C^n\exp(-N/2) + Nn^{-\omega(1)}.$$

In short, (1) extends Theorem 2.13 to general matrix ensembles with the extra assumptions that $N \ll n^{cn}$ and $n_0(t) = O(1/t)$. It shows that although the chain dies out eventually (for discrete ξ), one can still see the concentration of the very top exponents as long as N is not exceedingly large.

3. Some further study

Regarding our results on "Anti-concentration of inhomogeneous random walks", I would like to obtain a more satisfying characterization for multilinear forms. In the non-abelian setting, I propose to seek for a continuous variant for locally compact groups. Another problem is to find appropriate applications of this non-abelian setting.

For "Universality for the number of intersections for random eigenfunctions on flat tori", I suspect that the variance for general ξ is also as small as in the Gaussian case, but this is a delicate matter (even for the Gaussian case). There are many things left to be discovered, such as central limit theorem for fluctuations; length of the nodal lines (such as [42]); extension to other manifolds, etc. Similarly for "Polynomial systems of many variables", understanding of basic statistics for other random systems beside the Gaussian one is completely missing from the picture.

With respect to the note on "Wegner-type estimate for eigenvalue repulsion", our next goal is to obtaining the conjectural bound $\sup_{1\leq i\leq n-1}\mathbf{P}(\delta_i \leq \delta n^{-\frac{1}{2}}) = O((\frac{\delta}{\sqrt{\alpha}})^2)$ from Theorem 2.8. A related problem is to improving Vershynin's bound $\mathbf{P}(\sigma_n \leq \delta n^{-\frac{1}{2}}) = O(\delta^{1/9} + \exp(-n^c))$ from [86] on the least singular value of random symmetric matrices to $O(\delta + \exp(-n^c))$.

About our result on "Logarithmic determinant", as stated, I would like to obtain a CLT variant for logarithmic determinant of random symmetric Bernoulli matrices. To the best of my understanding, this problem is still open even with recently developed tools for proving universality in RMT. Relatedly, I plan to study a variant of logarithmic law for permanent of iid Gaussian matrices G_n. There are other open questions for this Gaussian model such as the (weak) anti-concentration conjecture by Aaronson [1] that $|\mathbf{perm}(G_n)| \geq \sqrt{n!}/n^{O(1)}$ with high probability, or the conjecture by Fyodorov [26] that the empirical distribution of roots of the permanental polynomial $\mathbf{perm}(G_n - xI_n)$ obeys the circular law.

Trying to extend our paper on "Normal vectors", the same thing (optimal delocalization and gaussianity) should hold for normal vectors of Wigner matrices without the first row (which in turns would yield optimal control on the entries of inverse random Wigner matrices; I have obtained some slightly weaker bound along the line in [55]). Ideally, I would like to see if there is a flexible method that would work for eigenvectors of Wigner matrices (without the use of eigenvector flow method from [8]), and more generally the extremal vectors of "balanced systems" (such as the random unit vectors $\mathbf{x} = (x_1, \ldots, x_n)$ that maximizes the sum $\sum_{1 \leq i \leq j \leq k} a_{ijk} x_i x_j x_k$ with a_{ijk} being iid copies of a nice random variable of zero mean.)

References

[1] S. Aaronson and A. Arkhipov, The Computational Complexity of Linear Optics, Theory of Computing, Volume 9 (4), 2013, pp. 143-252.

[2] L. Babai, D. Grigoryev and D. Mount, Isomorphism of graphs with bounded eigenvalue multiplicity, *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, 310-324 (1982).

[3] Berry, M. V. Regular and irregular semiclassical wave functions. J. Phys. A 10 (1977), no. 12, 2083-2091.

[4] J. Bourgain and Z. Rudnick, Restriction of toral eigenfunctions to hypersurfaces, C. R. Acad. Sci. Paris, Ser. I 347 (2009) 1249-1253.

[5] J. Bourgain and Z. Rudnick, Restriction of toral eigenfunctions to hypersurfaces and nodal sets , Geometric and Functional Analysis: Volume 22, Issue 4 (2012), Page 878-937.

[6] J. Bourgain and Z. Rudnick, Nodal intersections and L_p restriction theorems on the torus. To appear in Israel J. Math., arXiv:1308.4247.

[7] P. Bourgade and G. Ben Arous, Extreme gaps in the eigenvalues of random matrices, Annals of Probability, 41 (2013) no. 4, 2648-2681.

[8] P. Bourgade and H.-T. Yau, The eigenvector moment flow and local quantum unique ergodicity, to appear in Communications in Mathematical Physics.

[9] P. Bourgade, L. Erdős, H.-T. Yau and J. Yin, Fixed energy universality for generalized Wigner matrices, `arxiv.org/abs/1407.5606`.

[10] E. Breuillard, B. Green, and T. Tao, The structure of approximate groups, Publications Mathmatiques Institut de Hautes tudes Scientifiques, 116 (2012), 115-221.

[11] P. Burgisser and F. Cucker, Condition, The Geometry of Numerical Algorithms, Springer, Heidelberg, 2013.

[12] M-C. Chang, H. Nguyen, O. Nguyen and V. Vu, Random eigenfunctions on flat tori: universality for the number of intersections, preprint.

[13] J. E. Cohen and C.M. Newman, The stability of large random matrices and their products. Ann. Probab. 12 (1984) 283-310.

[14] K. Costello, Bilinear and quadratic variants on the Littlewood-Offord problem, Israel Journal of Mathematics, 2015.

[15] K. Costello, T. Tao and V. Vu, Random symmetric matrices are almost surely non-singular, Duke Math.J.135 (2006), 395-413.

[16] F. Cucker, T. Krick, G. Malajovich and M. Wschebor, A numerical algorithm for zero counting. I: Complexity and accuracy, J. Complexity 24 (2008) 582-605.

[17] F. Cucker, T. Krick, G. Malajovich and M. Wschebor, A numerical algorithm for zero counting. II: Distance to Ill-posedness and smoothed analysis, J. Fixed Point Theory Appl. 6 (2009) 285-294.

[18] F. Cucker, T. Krick, G. Malajovich and M. Wschebor, A Numerical Algorithm for Zero Counting. III: Randomization and Condition, Advances in Applied Mathematics 48 (2012), 215-248.

[19] Y. Do, H. Nguyen and V. Vu, Real roots of random polynomials: expectation and repulsion, Proceedings London Mathematical Society (2015), Vol. 111 (6), 1231-1260.

[20] L. Erdős, A. Knowles, H.-T. Yau and J. Yin, Spectral statistics of Erdős-Rényi Graphs II: Eigenvalue spacing and the extreme eigenvalues, Communications in Mathematical Physics, 314 (2012), no. 3, 587-640.
[21] L. Erdős, B. Schlein and H.-T. Yau, Wegner estimate and level repulsion for Wigner random matrices, IMRN, 2010, no. 3, 436-479.
[22] L. Erdős and H.-T. Yau, Gap Universality of Generalized Wigner and beta-ensembles, `arxiv.org/abs/1211.3786`.
[23] P. Erdős and L. Moser, Elementary Problems and Solutions: Solutions: E736, American Mathematical Monthly, 54 (1947), no. 4, 229-230.
[24] P. Erdős, On a lemma of Littlewood and Offord, Bull. Amer. Math. Soc. 51 (1945), 898–902.
[25] P. Erdős and A. C. Offord, On the number of real roots of a random algebraic equation, Proc. London Math. Soc. 6 (1956), 139–160.
[26] Y. Fyodorov, On Permanental Polynomials of Certain Random Matrices , International Mathematics Research Notices Volume 2006, 1-37.
[27] V. Girko, The central limit theorem for random determinants (Russian), translation in Theory Probab. Appl. 24 (1979), no. 4, 729-740.
[28] Goodman, Distribution of the determinant of a complex Wishart distributed matrix, Annal of Statistics, 34 (1963), 178-180.
[29] E. Kostlan, Random polynomials and the statistical fundamental theorem of algebra, unpublished (1987).
[30] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, Period. Math. Hungar. 8 (1977), no. 3-4, 197-211.
[31] I. A. Ibragimov and N. B. Maslova, The average number of zeros of random polynomials, Vestnik Leningrad. Univ. 23 (1968), 171–172.
[32] I. A. Ibragimov and N. B. Maslova, The mean number of real zeros of random polynomials. I. Coefficients with zero mean, Theor. Probability Appl. 16 (1971), 228–248.
[33] I. A. Ibragimov and N. B. Maslova, The mean number of real zeros of random polynomials. II. Coefficients with a nonzero mean., Theor. Probability Appl. 16 (1971), 485–493.
[34] I. A. Ibragimov and N. B. Maslova, The average number of real roots of random polynomials, Soviet Math. Dokl. 12 (1971), 1004-1008.
[35] M. Isopi and C. M. Newman, The triangle law for Lyapunov xxponents of large random matrices, Commun. Math. Phys. 143, 591-598 (1992).
[36] M. Kac, On the average number of real roots of a random algebraic equation, Bull. Amer. Math. Soc. 49 (1943) 314–320.
[37] M. Kac, On the average number of real roots of a random algebraic equation. II. Proc. London Math. Soc. 50, (1949), 390–408.
[38] V. Kargin, Products of Random Matrices: dimension and growth in norm, Annals of Applied Probability, 2010, Vol. 20, No. 3, 890-906.
[39] G. Katona, On a conjecture of Erdős and a stronger form of Sperner's theorem. Studia Sci. Math. Hungar 1 (1966), 59-63.
[40] D. Kleitman, On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors, Advances in Math. 5 1970 155-157 (1970).
[41] E. Kostlan, On the distribution of roots of random polynomials, Chapter 38, From Topology to Computation: Proceeding of the Samefest, edited by M. W. Hirsch, J.E. , Marsden and M. Shub, Springer-Verlag, NY 1993.
[42] M. Krishnapur, P. Kurlberg and I. Wigman, Nodal length fluctuations for arithmetic random waves. Ann. of Math. (2) 177 (2013), no. 2, 699-737.
[43] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III. Rec. Math. Mat. Sbornik N.S. 12 , (1943). 277–286.
[44] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. II. Proc. Cambridge Philos. Soc. 35, (1939), 133-148.
[45] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III. , Rec. Math. [Mat. Sbornik] N.S. 54, (1943), 277-286.
[46] J. E. Littlewood and A. C. Offord, On the distribution of the zeros and a-values of a random integral function. I., J. Lond. Math. Soc., 20 (1945), 120-136.http://arxiv.org/abs/1312.0933
[47] J. E. Littlewood and A. C. Offord, On the distribution of the zeros and values of a random integral function. II., Ann. Math. 49 (1948), 885–952. Errata, 50 (1949), 990-991. 976), 35-58.
[48] M. L. Mehta, Random matrices and the statistical theory of energy levels, *Academic Press*, New York, NY, 1967.
[49] C. M. Newman, The Distribution of Lyapunov Exponents: Exact Results for Random Matrices, Commun. Math. Phys. 103, 121-126 (1986).
[50] H. Nguyen, Inverse Littlewood-Offord problems and the singularity of random symmetric matrices, Duke M. J., vol. 161, 4 (2012), 545-586.

[51] H. Nguyen, Random doubly stochastic matrices: the circular law, Ann. of Prob., (2014), Vol. 42, No. 3, 1161-1196.
[52] H. Nguyen, On a condition number of random polynomial systems, Mathematics of Computation (2016) 85, 737-757.
[53] H. Nguyen, Asymptotic Lyapunov exponents for large random matrices, to appear in Annals of Applied Probability.
[54] H. Nguyen, Anti-concentration of inhommogeneous random walks, preprint.
[55] H. Nguyen, Concentration of distances in Wigner matrices, in revision, Linear Algebra and its Applications.
[56] H. Nguyen and S. O'Rourke, The elliptic law, IMRN (2015), Vol. 2015, 7620-7689.
[57] H. Nguyen and S. O'Rourke, On the concentration of random multilinear forms and the universality of random block matrices, PTRF (2015), Vol. 162, 1, 97-154.
[58] H. Nguyen, O. Nguyen and V. Vu, On the number of real roots of random polynomials, Communications in Contemporary Mathematics (2016) Vol. 18, 4, 1550052.
[59] H. Nguyen, T. Tao and V. Vu, Random matrices: tail bounds for gaps between eigenvalues, PTRF (2017) Vol. 167, 3, 777-816.
[60] H. Nguyen and V. Vu, Optimal inverse Littewood-Offord theorems, Advances in Mathematics, Volume 226, 6, (2011), 5298-5319.
[61] H. Nguyen and V. Vu, Random matrices: law of the determinant, Ann. Prob., (2014), Vol. 42, No. 1, 146-167.
[62] H. Nguyen and V. Vu, Normal vector of a random hyperplane, to appear in IMRN.
[63] M. Rudelson and R. Vershynin, The Littlewood-Offord Problem and invertibility of random matrices, Advances in Mathematics 218 (2008), 600-633.
[64] M. Rudelson and R. Vershynin, Smallest singular value of a random rectangular matrix, Communications on Pure and Applied Mathematics 62 (2009), 1707-1739.
[65] M. Rudelson and R. Vershynin, Non-asymptotic theory of random matrices: extreme singular values, Proceedings of the International Congress of Mathematicians. Volume III, 1576-1602, Hindustan Book Agency, New Delhi, 2010.
[66] Z. Rudnick and I. Wigman, Nodal Intersection for random eigenfunctions on the torus, Amer. J. of Mathematics, to appear.
[67] Z. Rudnick, I. Wigman and Nadav Yesha, Nodal intersections for random waves on the 3-dimensional torus, Annales de l'institut Fourier, to appear.
[68] A. Sárközy and E. Szemerédi, *Über ein Problem von Erdős und Moser*, Acta Arithmetica 11 (1965), 205-208.
[69] M. Shub and S. Smale , Complexity of Bezouts theorem I: geometric aspects, J. Amer. Math. Soc. 6 (1993) 459-501.
[70] M. Shub and S. Smale, Complexity of Bezouts theorem II: volumes and probabilities, Computational Algebraic Geometry, in: Progr. Math., vol. 109, Birkhuser, 1993, pp. 267-285.
[71] M. Shub and S. Smale, Complexity of Bezouts theorem III: condition number and packing, J. Comp. 9 (1993) 4-14.
[72] M. Shub and S. Smale, Complexity of Bezouts theorem IV: polynomial time, Theo. Com. Sci. 133 (1994) 141-164.
[73] M. Shub and S. Smale, Complexity of Bezouts theorem V: probability of success; extensions, SIAM J. Numer. Anal. 33 (1996) 128-148.
[74] D. A. Spielman and S. H. Teng, Smoothed analysis of algorithms, Proceedings of the International Congress of Mathematicians, Vol. I, 597-606, Higher Ed. Press, Beijing, 2002.
[75] R. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, SIAM J. Algebraic Discrete Methods 1 (1980), no. 2, 168-184.
[76] Stevens, D. C. The average number of real zeros of a random polynomial. CPAM, 22 (1969), 457-477.
[77] T. Tao, The asymptotic distribution of a single eigenvalue gap of a Wigner matrix, Probability Theory and Related Fields, 157 (2013), no. 1-2, 81-106.
[78] T. Tao, Inverse theorems for sets and measures of polynomial growth, Q. J. Math (2017) 68 (1): 13-57.
[79] T. Tao and V. Vu, From the Littlewood-Offord problem to the circular law: universality of the spectral distribution of random matrices, Bulletin of the American Mathematical Society, 46 (2009), 377-396.
[80] T. Tao and V. Vu, Inverse Littlewood-Offord theorems and the condition number of random matrices, Annals of Mathematics (2), 169 (2009), no 2, 595-632.
[81] T. Tao and V. Vu, A sharp inverse Littlewood-Offord theorem, RSA 37 (2010), no. 4, 525-539.
[82] T. Tao and V. Vu, Random matrices: universality of local eigenvalue statistics, Acta Math. 206 (2011), no. 1, 127-204.
[83] T. Tao and V. Vu, A central limit theorem for the determinant of a Wigner matrix, Adv. Math. 231 (2012), no. 1, 74-101.
[84] T. Tao and V. Vu, Random matrices have simple spectrum, submitted, `arxiv.org/abs/1412.1438` .
[85] Todhunter, I. A history of the mathematical theory of probability, Stechert, New York, 1931.
[86] R. Vershynin, Invertibility of symmetric random matrices, Random Structures & Algorithms, 44 (2014), no. 2, 135-182.
[87] J. E. Wilkins, An asymptotic expansion for the expected number of real zeros of a random polynomial, Proc. Amer. Math. Soc. 103 (1988), 1249-1258.