A broad description

Much of my research has focused on applications of random matrix theory to analytic number theory. This program of research entails the use of ideas from analysis, probability, and combinatorics, and I will explain some of these connections below. Some highlights of my research that I will focus on here are:

- Work giving insight into the moments of the Riemann zeta function and other L-functions via a study of the distribution of the k-fold divisor function.
- A schema relating random matrix phenomena in number theory to the decomposition of arithmetic functions into ‘oscillatory’ and ‘regular’ parts. (Work on this project has formed a large part of the ongoing individual NSF grant DMS-1701577.)
- Work done on the local distribution of zeros of the Riemann zeta function; this includes a strong Szegő limit theorem for the zeros, the proof of a resurgence effect for the zeta function’s pair correlation measure, and work on ratio theorems.
- The resolution of a nearly 40 year old conjecture regarding the distribution of the well-known family of Rudin-Shapiro trigonometric polynomials, via the study of products of pseudo-random matrices.

In the next two sections I discuss these projects in more detail, and describe plans for future research that stem especially from this list.

Many of the projects I describe below are natural to think about in probabilistic language, and a common thread is the study of random variables that are not quite independent, but are instead weakly dependent, with a dependence characterized by arithmetical/combinatorial considerations. Such structures end up being common in discrete mathematics, though they are not always evident from the outset.

I have made an effort to keep the descriptions here accessible to specialists of areas different than my own. A longer and more technical account with a focus on future projects can be found in the project description of my current NSF grant, made available at

http://www-personal.umich.edu/~rbrad/NSFmaster.ProjectDescription.pdf

Random matrices, L-functions, and arithmetic

Background

Let $g$ be a random element of the group of $N \times N$ complex unitary matrices, with $g$ chosen according to Haar measure. It is well-known that the eigenvalues of $g$ lie on the unit circle. Our

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figures/figure1.png}
\caption{Several realizations of eigenvalues from a $100 \times 100$ unitary matrix on the left, compared to several realizations of 100 points chosen independently on the unit circle on the right.}
\end{figure}
interest will be in the distribution of these eigenvalues, especially of the spacings between them. The eigenvalues (on the left in the diagram above), one notices, do not seem to fall independently of one another, but instead have a much more fixed distribution, repelling almost like electrons, with fewer clusters or gaps than points chosen independently (on the right in the diagram).

Consider another example: fill up an $N \times N$ matrix $A$ with complex entries chosen independently – say the entries are all chosen according to the complex gaussian distribution with mean 0 and variance 1, or alternatively the entries are chosen to take the four values $\pm 1, \pm i$ with equal probability. The eigenvalues of $H = \frac{1}{2}(A + A^*)$ will all lie on the real line, and likewise one may examine the distribution of eigenvalues and spacings between eigenvalues here. Roughly speaking, in both examples the distribution of spacings between eigenvalues follows the same pattern, and for large $N$ this pattern is exactly the same as for the unitary group. This appearance of this same pattern in many different mathematical places is a phenomena called \textit{GUE universality} (after the so-called Gaussian Unitary Ensemble in which the pattern was first observed). Less well understood, this same pattern appears in many places that have little on the surface to do with the eigenvalues of matrices. Examples run from situations as esoteric as the arrival of bus times in the city of Cuernavaca (empirically), to the spacing between zeros of the Riemann zeta function (conjecturally). Much of my own research has gone into better understanding this universality phenomenon in the latter context of analytic number theory.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{zeros.png}
\caption{Several collections of 100 consecutive nontrivial zeta zeros near a random height, rescaled and wrapped around the unit circle.}
\end{figure}

\section*{Moments and divisor sums}

The connection between the Riemann zeta function and random matrices first emerged from work of H. Montgomery \cite{montgomery} in the early 70s, who studied the spacings between zeta zeros. In the time since, this connection has had many spectacular successes and generalizations, and surely one of the most important is a conjecture by J. Keating and N. Snaith \cite{keatingsnai} for moments of the Riemann zeta function:

\begin{equation}
\frac{1}{T} \int_T^{2T} |\zeta(1/2 + it)|^{2k} dt \sim a_k \prod_{j=0}^{k-1} \frac{j^1}{(k+j)!} (\log T)^{k^2}
\end{equation}

as $T \to \infty$, where $a_k$ is an arithmetic constant that is complicated but well understood, and the other terms come about from modeling the zeta function by the characteristic polynomial of a random unitary matrix. The Keating-Snaith conjecture \cite{keatingsnai} is known to be true only for $k = 1, 2$ but nonetheless a large amount of evidence has accumulated in its favor. Moments of the zeta function are important not only because of their long history, but also because they are connected to important classical conjectures like the Lindelöf Hypothesis.

The left hand side of \cite{keatingsnai}, it was realized over a century ago, is closely related to the distribution of the $k$-fold divisor function $d_k(n) = \# \{(m_1, \ldots, m_k) \in \mathbb{N}^k : n = m_1 \cdots m_k\}$. This function forms the coefficients of the Dirichlet series for $\zeta(s)^k$; for $k = 2$ for instance it counts the number of positive integers that divide $n$. 

2
In [12] coauthored with J. Keating, E. Roditty-Gershon, and Z. Rudnick – motivated by a connection to moments of the zeta function – we studied the probabilistic variance of the sums

\[ D_k(x; H) := \sum_{x \leq n \leq x + H} d_k(n), \]

where \( x \) is a random parameter chosen uniformly from the interval \([X, 2X]\), and where \( H \) is a parameter that grows with \( X \) (e.g. \( H = X^{1/4} \) or \( H = X^{3/4} \)). We make a conjecture about the asymptotic behavior of

\[ \text{Var}_{x \in [X,2X]} D_k(x; H), \]

and likewise provide evidence for this conjecture by proving a function field variant of it. I will elaborate on both these points.

The reason we care about this variance is that the conjecture we make implies [1], and thereby provides an arithmetic interpretation of the Keating-Snaith conjecture.

Prior to our work, it was understood in some sense that the variance of \( D_k(x; H) \) was related to the integral in [1], nonetheless this quantity was not well understood even at a conjectural or heuristic level. A salient feature of our conjecture explains why: we predict that the variance exhibits several phase changes as \( H \) varies. These phase changes are striking and something of a novelty for a problem of this sort. (The form of the phase changes can be explicitly written down and has many interesting combinatorial features.)

The reason we made this conjecture is that we were able to prove a function field variant of it. That is, we replace the ring of integers \( \mathbb{Z} \) with \( \mathbb{F}_q[T] \), the ring of polynomials with coefficients in a finite field. Because \( \mathbb{F}_q[T] \) has much the same arithmetic structure as \( \mathbb{Z} \), analogues of \( k \)-fold divisor functions can be defined on \( \mathbb{F}_q[T] \), and with a bit more thought analogues of the short-interval sums \( D_k(x; H) \) can be defined as well. (For specialists: we work in the large \( q \) limit.) By working in a function field setting, we are able to relate the variance of these sums to a sum over the zeros of \( L \)-functions, and this to a random matrix integral. In turn it is a combinatorial problem to relate this integral to a count of lattice points; these counts can be analyzed and display the phase changes I have mentioned above.

This conjecture has attracted substantial attention, and partial aspects of it have been verified; I mention especially the recent work of S. Lester [13], A. Harper and K. Soundararajan [8], R. de la Bretèche and D. Fiorilli [3] and myself and K. Soundararajan [23]. In the last of these we showed that an analogous conjecture in which random short-intervals are replaced by random sparse-arithmetic-progressions is true in a restricted range. This allows us to see one of the conjectured phase changes (though not all of them).

Decompositions of general arithmetic functions.

We thus now have a much better understanding of how the variance \( \text{Var} D_k(x; H) \) behaves. Despite this, the aforementioned phase changes of this variance remain somewhat mysterious.

One explanation, based on a heuristic method dating back to Hardy and Littlewood but extended in important ways, has been developed in a series of works by B. Conrey and J. Keating (see e.g. [5]). I propose a complementary perspective, that the changes in variance are a result of a changing combinatorial decomposition of the \( k \)-fold divisor function into two parts: one part that behaves in a random (or oscillatory) fashion over a random interval of size \( H \) and another that behaves in a structured (or regular) fashion over the same interval. Decompositions of arithmetic functions, in other contexts, have a long history in analytic number theory. I do not give a technical account here of what I mean by ‘random/oscillatory’ and ‘structured/regular’ – but the points I emphasize are 1) such a decomposition does exist and can be described explicitly in a function field setting,
and 2) changes in the variance as the size of the short interval varies (as we saw above for $d_k(n)$) correspond to changes in this decomposition.

Decompositions like this are not limited to the $k$-fold divisor function. Still working in a function field setting, I show in [17] that they apply to any arithmetic function whose value depends on the size of prime factors. The combinatorial formalism required to produce these decompositions is closely linked with symmetric function theory and provides a pleasant formula for the variance of short-interval sums of any arithmetic function. (The work is featured in a blog post [3] of J. Ellenberg, where he describes an application of it to algebraic geometry in a paper of D. Hast and V. Matei.)

**Local distribution of zeros of the zeta function**

The projects above have made use of a function field analogy, but now I return to the Riemann zeta function itself. Recall that a main conjecture in this area is that statistically the spacings between zeros wrapped around the circle in Figure 2 resemble the spacings between eigenvalues in Figure 1. Evidence that this is the case has been developed in papers of H. Montgomery [15], D. Hejhal [9], and Z. Rudnick and P. Sarnak [24]. Formally what these authors show is that the $n$-point correlation functions of zeros and eigenvalues agree against a collection of band-limited functions; informally this means that we can verify the resemblance as long as we squint. This resemblance between zeros and eigenvalues at the level of individual spacings is said to be a resemblance *at a microscopic scale*.

In a series of papers I have developed similar themes:

In [16, 14], I, with K. Maples in the second, show at a mesoscopic scale (that is, a scale larger than microscopic, involving collections of a growing number of zeros/eigenvalues, but a scale which does not take up the entire unit circle) the distribution of zeros continues to resemble that of the eigenvalues of a random matrix. This was done by proving for the zeros an analogue of the strong Szegő theorem from random matrix theory (cf. the independent work [2]). This is a central limit theorem for generalized counts of zeros; its analogue in random matrix theory has a long and important history (see e.g. [26], [27]). In the unconditional form of [14], it was the first time a ‘form factor’ term of $|x|$, characteristic here of Gaussian pink noise, has been unconditionally seen among counts of ordinates of zeros.

In [18], I show that this resemblance does not quite extend to a macroscopic scale (that is, a scale which includes the entire unit circle), by confirming on the Riemann Hypothesis a resurgence phenomenon in the pair correlation function for zeros which was first conjectured heuristically by Bogomolny and Keating [1].

In [20], I derive tail bounds for the likelihood that a large number of zeros fall in a microscopic interval and use this to show that GUE universality can be used to control averages of ratios of the zeta function. In [4], coauthored with R. Chhaibi, E. Hovhannisyan, J. Najnudel, and A. Nikeghbali, ideas in part from this paper were used to analyze the limiting behavior of characteristic polynomials from classical random matrix ensembles.

**New directions**

There are a number of projects which arise especially from the combinatorial decomposition of arithmetic functions described above, and I highlight these here. In the next few years I intend in particular to

- Investigate an analogue of this decomposition process in the setting of the integers. Because this decomposition is closely related to the appearance of random matrix statistics in a function field setting, I hope especially to illuminate a concrete mechanism by which GUE universality could heuristically be seen to arise from arithmetic considerations, and in the process develop an illuminating combinatorial framework.
• Develop random models for the sequence of characters \( \{1^t, 2^t, 3^t, \ldots \} \) where \( t \) is a random variable uniformly distributed in the interval \([T, 2T] \). The sum of this sequence of characters against certain arithmetic functions is closely connected to the conjectured statistical appearance of random matrix theory among the zeros of the Riemann zeta function. In particular I hope to find a computationally tractable sequence of random variables \( \{U_1(T), U_2(T), \ldots \} \) that may be proven to exhibit the same behavior against such arithmetic functions as random matrix theory predicts the sequence \( \{n^t\} \) will.

• Develop similar models for other (symplectic/orthogonal) families of characters.

A fuller and more technical account of these projects especially may be found in my NSF grant description.

Other related ongoing projects include:

• Work with E. Roditty-Gershon analyzing the distribution of primes in short intervals in algebraic number fields. Part of our work has been to decide upon the ‘right’ notion of a short interval in this context. We provide support for the view that the primes are not distributed in a completely random fashion over large enough short-intervals by analyzing sums of singular series. Our work generalizes a result of H. Montgomery for the integers, but its proof depends on very different ideas.

• Work with J. Lagarias, showing that the so-called ‘Alternative Hypothesis’ about the zeta function’s zeros cannot be ruled out using just the Rudnick-Sarnak information about higher-level correlation, by explicit construction of a counterexample point process.

• Ongoing work on a central limit theorem for quasicrystals: take an aperiodic tiling of the plane, and count the number of vertices to land in a thin annulus with growing radius but diminishing thickness. This count becomes gaussian for the radius chosen randomly.

• Ongoing work related to a model for \( \{1^t, 2^t, \ldots\} \) in a function field setting. More exactly, take a Dirichlet L-function over \( \mathbb{F}_q[T] \), and replace the characters with random multiplicative functions (i.i.d. on the unit circle say). Then condition the resulting analytic function on (i) having only \( N \) zeros, and (ii) having all zeros satisfying a Riemann Hypothesis. Then in the large \( q \) limit the zeros will be distributed according to the circular symplectic ensemble (with no random matrix present!).

• Ongoing work with K. Soundararajan, and separate ongoing work with O. Gorodetsky, on correlations of other arithmetic functions and their behavior in short intervals, both over \( \mathbb{Z} \) and over \( \mathbb{F}_q[T] \).

• Ongoing work with T. Tao on a heat flow evolution of the Riemann Xi function, and the de Bruijn-Newman constant.

Rudin-Shapiro polynomials and products of random matrices

Background

I come now to very different type of problem, but one whose resolution was still influenced by random matrices.

Littlewood polynomials are the class of single-variable polynomials from with all coefficients \( \pm 1 \). It is a longstanding open problem to determine whether there are constants \( c_1 \) and \( c_2 \) such that there exist Littlewood polynomials \( L \) of arbitrarily high degree \( N \) satisfying \( c_1 \sqrt{N} \leq |L(z)| \leq c_2 \sqrt{N} \) for all \( |z| = 1 \). (A computation of the \( L^2 \)-norm on the unit circle shows that if a degree \( N \) Littlewood polynomial takes nearly a constant value for all \( |z| = 1 \), that value must be \( \sqrt{N} \).)

The Rudin-Shapiro polynomials \( P_k(z) \) are a special sequence of Littlewood polynomials of degree \( N = 2^k - 1 \) satisfying an upper bound of this sort: \( P_k(z) = O(\sqrt{N}) \). The Rudin-Shapiro polynomials do not satisfy a corresponding lower-bound, and it is natural to ask how far they deviate from doing so.
Questions of this sort can be made precise by letting \( \omega \) be a random variable uniformly distributed on the unit circle and investigating the distribution of \( P_k(\omega) \). In [19], I proved that as \( k \to \infty \), the random variable \( \frac{P_k(\omega)}{\sqrt{N}} \) tends to uniform distribution in the disc \( D := \{ z \in \mathbb{C} : |z| \leq \sqrt{2} \} \).

This result resolved a conjecture of H. Montgomery and as a corollary a 1980 conjecture of B. Saffari.

**A relation to products of pseudo-random matrices**

The method of proving their conjecture was quite different from other techniques that have been used in this area in the past; its starting point was to relate the distribution of the polynomial \( P_k(\omega) \) to the distribution of the product of matrices

\[
G(\omega^{2^{k-1}})G(\omega^{2^{k-2}}) \cdots G(\omega),
\]

where

\[
G(\omega) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \omega \\ 1 & -\omega \end{pmatrix}.
\]

It is easy to see that \( G(\omega) \) is a random element of \( U(2) \), and in [19], I showed the product above equidistributes in \( U(2) \) with respect to Haar measure as \( k \to \infty \). From this fact, the limiting distribution of \( P_k(\omega) \) can be derived.

An intuitive interpretation of this last result is as follows: the sequence of random variables \( \omega^{2^{k-1}}, \omega^{2^{k-2}}, \cdots, \omega \) can be seen to behave in many instances like a sequence of independent random variables \( \omega_{k-1}, \omega_{k-2}, \cdots, \omega_0 \), with each uniformly distributed on the unit circle (a well known example of this phenomenon is the Salem-Zygmund central limit theorem [25]). For this reason one might expect that the pseudo-random walk in [2] on the group \( U(2) \) behaves rather like an actual random walk:

\[
G(\omega_{k-1})G(\omega_{k-2}) \cdots G(\omega_0).
\]

Such random walks in compact groups are known to equidistribute unless certain obvious obstructions arise, and in this case they do not.

Nonetheless, despite the heuristic analogy between the products \( G(\omega^{2^{k-1}})G(\omega^{2^{k-2}}) \cdots G(\omega) \) and \( G(\omega_{k-1})G(\omega_{k-2}) \cdots G(\omega_0) \), it is not from a comparison between these two that one proves the former product equidistributes. Instead, one must make use of the representation theory of \( U(2) \) and a combinatorial analysis that is seemingly very special to the problem at hand.

This result has recently found application in the work of T. Erdélyi, who has made use of it to resolve another old conjecture about the Mahler measure of Rudin-Shapiro polynomials [7].

**New directions**

The pseudo-random walks considered here are really a nascent topic, and several natural problems suggest themselves immediately. For example:

- There exist other ergodic sequences \( g_1, g_2, \ldots \) of random elements of compact groups (even groups as simple as \( \mathbb{Z}/2\mathbb{Z} \)) such that \( g_kg_{k-1} \cdots g_1 \) does not equidistribute, while a product of independent elements would. I hope to find general criteria characterizing equidistribution.
In a different direction, it seems likely that the product $2^k$ equidistributes whenever $2^k$ is replaced by any sufficiently quickly growing sequence. I hope to show that this is the case when $2^k$ is replaced by any lacunary sequence $n_k$ (that is, so that $n_{k+1}/n_k \geq C > 1$, for some constant $C$). The matrices $G(\omega)$ considered here can be replaced by polynomial maps into compact algebraic linear groups, and the same question can be sensibly asked.

References