UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

Random Matrix Theory and L-functions: Numerical Experiments

Francisco Martín Ponce Carrión

Matemáticas

Trabajo de fin de carrera presentado como requisito
para la obtención del título de Matemático.

Quito, 07 de mayo de 2020

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

HOJA DE CALIFICACIÓN
DE TRABAJO DE FIN DE CARRERA

Random Matrix Theory and L-functions: Numerical Experiments

Francisco Martín Ponce Carrión

Nombre del profesor, Título académico Nathan Ryan, PhD

Quito, 07 de mayo de 2020

DERECHOS DE AUTOR

Nombres y apellidos:	Francisco Martín Ponce Carrión
Código:	00136163
Cédula de identidad:	1717271611
Lugar y fecha:	Quito, mayo de 2020

ACLARACIÓN PARA PUBLICACIÓN

UNPLUBLISHED DOCUMENT

RESUMEN

Presentamos experimentos numéricos con matrices aleatorias para modelar ceros de funciones L. Para este fin, desarrollamos e implementamos un algoritmo que genera matrices aleatorias distribuidas con la medida de Haar en 3 grupos compactos: $U(N)$, $SO(N)$ y $USp(N)$. Finalmente comparamos las distribuciones de los argumentos de autovalores de matrices aleatorias con ceros de twists cuadráticos de funciones L asociadas a formas modulares.

Palabras clave: funciones L, matrices aleatorias, ensambles circulares, ensambles de Ginibre, medida de Haar, teoría de matrices aleatorias.

ABSTRACT

We present numerical experiments with random matrices to model zeros of families of L-functions. In order to do so, we develop and implement an algorithm to draw random Haar distributed matrices from 3 classical compact groups: $U(N)$, $SO(N)$ and $USp(N)$. Finally, we compare the distributions of the arguments of the eigenvalues with zeros from quadratic twists of L-functions associated to modular forms.

Keywords: L-functions, random matrices, circular ensembles, ginibre ensembles, Haar measure, random matrix theory.

List of Tables

List of Figures

Contents

1 Introduction and motivation

Random matrix theory has proven to be extremely useful in modeling complex phenomena which involve a degree of randomness. Random matrices are matrices whose entries are random variables; equivalently, they can be understood as matrix-valued random variables in the sense that they are random variables which take values in a space of matrices [17]. Since traditional random variables are used to model a vast variety of phenomena, it should not come as a surprise that random matrices are a powerful tool with applications to various fields, such as: wireless communications, finance, nuclear physics, stochastic differential equations, neural networks and in our case in number theory [11,15,22]. The latter has been developed in the course of the last 30 years. As Keating and Snaith showed [9], studying certain statistical properties of the characteristic polynomial of random matrices allows us to get information on the zeros of L-functions associated with random matrices from different ensembles. (See Section 1.2 for more on L-functions)

Versatility is one of the greatest virtues of random matrices. They are especially useful whenever imprecise matrices occur [15]. In other words, whenever determining exact values from a matrix is not possible. Such problems abound, which is what makes random matrices so powerful in diverse situations. More explicitly, when the dimensions of the matrices are large, some statistical properties of the eigenvalues of ensembles of random matrices are independent of the probability distribution used to define the entries. For example, the GOE conjecture states that the distribution of spacings between eigenvalues is independent of the probability distribution of the entries of the matrix [17]. An important fact to remark is that this independence translates to a notion of universality of the distribution of spacings over the ensemble.

The aim of this work is to model zeros of families of L-functions using ensembles of random matrices. We present implementations of the algorithms used to generate random matrices whose eigenvalues we apply to this aim.

1.1 Nuclear physics

Initially, RMT arose in the context of nuclear physics. Whenever we want to determine the motion of three particles given their initial position and velocities, we cannot obtain a general closed form solution. This yields some intuition into the complexity of the problem when considering nuclei that have hundreds of protons and neutrons, each one interacting with the other. If we could determine the behavior of particles inside the nucleus, then we would be able to compute the energy levels of the nucleus. We know that energy levels of a system are supposed to be modeled by the eigenvalues of a Hermitian operator H. This operator is infinite dimensional and its entries depend on the physical system. Thus, the equation to find its eigenvalues E_i and eigenfunctions Ψ_i [15, 17]

$$H\Psi_i = E_i\Psi_i$$

is unsolvable when the system is a nucleus. In that case H would be impossible to determine exactly, so by imposing statistical restrictions on H and making it finite dimensional, you can model certain characteristics from the nucleus. Even though these finite dimensional approximations of H do not give an exact description of the system, they provide information that would be otherwise unknown. This shows one of the initial applications when random matrices arise naturally.

Analogously, in our models we approximate infinitely many zeros by finite matrices and zeros up to a finite height.

1.2 L-functions

To define an L-function in general is not trivial. A precise definition requires abundant mathematical background which is not essential for the present work. Instead, we choose to present specific cases of L-functions and elaborate further on how deep these mathematical objects are. For our purposes, it will be sufficient to present the Riemann Zeta function, L-functions associated with elliptic curves and twisted elliptic curves. To see more precise and general definitions for L-functions see [6].

1.2.1 The Riemann Zeta function $\zeta(s)$

The Riemann Zeta function is, perhaps, one of the most famous L-functions. It is defined as an infinite sum that can also be expressed as an Euler product as follows [2]:

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}. \tag{1}$$

The series converges absolutely for $\Re s > 1$. Furthermore, it has an analytic continuation such that $\zeta(s)$ extends to a meromorphic function, $\xi(s)$ which has a simple pole at $s = 1$. To this analytic extension we associate a functional equation, which characterizes the L-function.

$$\xi(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \xi(1 - s). \tag{2}$$

Determining zeros of $\zeta(s)$ (or at least their real part) constitutes a deep problem which is far from trivial. The problem in question is one of seven 'Prize Problems' set by the Clay Mathematics Institute at the beginning of the millennium: the Riemann Hypothesis.

The Riemann Hypothesis (RH) states that the non-trivial zeros of the zeta function have real part $\frac{1}{2}$. We discuss one of the implications of RH for number theory. The Prime Number Theorem

(PNT) is a fundamental result which describes the asymptotic behavior of prime numbers:

$$\pi(x) \sim \frac{x}{\log x}$$

where $\pi(x)$ is the prime counting function. It can be stated in terms of the logarithmic integral $Li(x) = \int_2^x \frac{dt}{\log t}$ with its corresponding error term. For $\epsilon > 0$, $\exists C_1, C_2 \in \mathbb{R}$ such that

$$|\pi(x) - Li(x)| \leq C_1 x \exp(-C_2 (\log x)^{3/5-\epsilon})$$

We need not analyze this deeply, we state this only for comparison purposes. Actually RH is equivalent to a better error term in the PNT [10]. In other words, the Riemann Hypothesis is equivalent to the following statement: For $\epsilon > 0$, $\exists\ C_1 > 0$ such that [10]

$$|\pi(x) - Li(x)| \leq C_1 x^{\frac{1}{2}-\epsilon}$$

Remarkably, this assertion connects the zeros of a meromorphic function in the complex plane with the distribution of prime numbers. Additionally, the Riemann Hypothesis has been extended to the Generalized Riemann Hypothesis (GRH) which states that the non trivial zeros of general classes of L-functions (suitably normalized) have real part $\frac{1}{2}$ [2].

Furthermore, assuming the Riemann Hypothesis we can study spacings of roots on the line $\Re s = \frac{1}{2}$. The n**-level correlations** are statistics that describe behavior of spacings of zeros over the critical line $\Re s = \frac{1}{2}$. These statistics rely on the infinity of zeros that lie on the critical line. However, these are invariant under removing finitely many zeros [17]. We did not define this object rigorously since it is beyond the scope of this work, but it is important to know that they provide information on the spacing of zeros and they can be modeled by matrix ensembles.

For L-functions which have infinitely many zeros on the critical line, we can study distribution of spaces of zeros very far away from the central point using ensembles of matrices. However, the aforementioned invariance of the n level correlation implies that this quantity is not very useful for providing information of zeros near the central point.

Rather than studying zeros of L-functions along the critical line ($\Re s = \frac{1}{2}$) we can think of the implications of studying zeros near the central point of the critical line. This leads naturally to another relevant open problem in number theory and also another Clay Prize Problem: the Birch and Swinnerton-Dyer conjecture (BSD). This conjecture relates the amount of zeros at the central point of an L-function with the rank of a finitely generated group. We elaborate on this in the following subsection.

1.2.2 L-functions and Elliptic curves

An elliptic curve E over $\mathbb{Q}$ is the curve defined by the following equation:

$$E : y^2 = x^3 + ax + b \tag{3}$$

where $a, b \in \mathbb{Q}$ and $-16(4a^3 + 27b^2) \neq 0$ (this last condition guarantees there are no singularities on the curve). We also know there is a group structure that can be defined on the rational solutions for the elliptic curve, i.e. $E(\mathbb{Q})$.

Mordell showed that this group is finitely generated and abelian [21]. This means there is a **finite** basis for all rational solutions to an elliptic curve defined over $\mathbb{Q}$. Finitely generated abelian groups are isomorphic to a direct sum of copies of $\mathbb{Z}$ the torsion subgroup which is the finite part. The arithmetic rank $r \geq 0$ of $E(\mathbb{Q})$ is defined as:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{torsion}$$

We can also associate an L-function to this elliptic curve in the following way [4]:

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_n^*}{n^s}$$

With an analytical continuation Φ_E meropmorphic in the complex plane and its associated functional equation:

$$\left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s) L(s, E) = \Phi_E(s) = w_E \Phi_E(1 - s)$$

Where N is the conductor of E (See [6]) and $w_E = \pm 1$ is known as the sign of the functional equation. We need a_n^* to be normalized coefficients so that the critical strip for this L-function is also $0 < \Re s < 1$. These are defined so that $|a_n^*| \leq d(n)$ where $d(n)$ is the number of positive divisors of n. Finally, we require that $a_n = \sqrt{n} a_n^*$ is an integer dependent on the number of solutions mod p of (3) for p prime divisors of n [4].

Thus we know there exists an L-function $L(s, E)$ associated to an elliptic curve. BSD conjecture states that the arithmetic rank r is equal to the the analytic rank, the order of vanishing of $L(s, E)$ at the central point (normalized to be at $s = \frac{1}{2}$) [23].

Consequently, we could study this conjecture by understanding zeros near the central point. As opposed to the case of $\zeta(s)$, we do not have an infinity of different zeros from which we can rescue relevant statistical behavior. We need to get data from zeros near the central point. Thus, instead of getting an infinite number of zeros of a given L-function over a line, we can get a finite number of zeros near a point of infinitely many similar L-functions. This is an intuitive way to introduce families of L-functions and leads us to our last example:

1.2.3 Quadratic twists

For an elliptic curve E over a field K and square-free d, a quadratic twist E^d is a curve isomorphic to E over $K(\sqrt{d})$ mapped in the following way [12]:

$$\begin{aligned} E &\to E^d \\ y^2 = x^3 + ax + b &\to dy^2 = x^3 + ax + b \qquad \text{or equivalently,} \\ y^2 = x^3 + ax + b &\to y^2 = x^3 + ad^2x + d^3b \qquad \text{i.e.,} \\ (x, y) &\mapsto \left(\frac{x}{d}, \frac{y}{d^{3/2}}\right) \end{aligned}$$

If $d \equiv 1 \mod 4$ or $d = 4k$ where $k \equiv 2, 3 \mod 4$ (with k square free) then we say d is a fundamental discriminant [18].

For a fundamental discriminant d, we can define a quadratic character $\chi_d(n)$ using the Kronecker symbol, i.e. $\chi_d(n) = \left(\frac{d}{n}\right)$. The Kronecker symbol is an extension of the Legendre symbol $\left(\frac{q}{p}\right)$ for quadratic residues mod p to n not necessarily prime (See [7]). Thus we consider the following twisted L-function:

$$L(s, E, \chi_d) = \sum_{n=1}^{\infty} \frac{a_n^* \chi_d(n)}{n^s}$$

Which is the associated L-function for the twisted elliptic curve E^d [4]. Additionally it admits the following functional equation:

$$\left(\frac{2\pi}{\sqrt{|d|N}}\right)^{-s}\Gamma(s)L(s,E,\chi_d(n))=\Phi_E(s,\chi_d(n))=w_E\chi_d(-N)\Phi_E(1-s,\chi_d(n))$$

Observe that since d can be made arbitrarily large, we thus obtain a family of L-functions associated to an elliptic curve. We now have an infinite set of L-functions from which we can obtain information about their zeros near the central point. This statistic is called the **1-level density** and we will discuss it more explicitly because it yields an analogy between L-functions and physics. The following deduction of the 1 - level density can be found in [17].

We begin by assuming the GRH, so that the non trivial zeros of $L(s,f)$ are of the form $\frac{1}{2}+i\gamma_f^{(j)}$ where $\gamma_f^{(j)}\in\mathbb{R}$. Consider a (test) function h that vanishes rapidly, so let

$$D_f(h)=\sum_j h(c_f\gamma_f^{(j)}). \tag{4}$$

The analytic conductor (c_f) of a given L-function is not going to be addressed but its definition and further information about this object can be found in [**?**]. For our purposes, it is important to know it rescales zeros near $s=\frac{1}{2}$. Observe that since h vanishes rapidly then most of the contribution of $D_f(h)$ comes from zeros near the central point. We take the average over all of the family of functions $\mathcal{F}$ and that is the 1-level density:

$$D_{\mathcal{F}}(h)=\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}D_f(h) \tag{5}$$

Note that this statistic depends on the choice of h. The analogy which we seek to point out is that physicists bombard heavy nuclei with neutrons to study their energy levels in an analogous fashion in which we use test functions to study zeros of L-functions. On top of this, both energy levels and zeros of L-functions behave as eigenvalues of random matrices belonging to some ensemble.

Now we have arrived to the result that motivates the numerical experiment this thesis: since Katz and Sarnak conjectured [17] that near the central point $s = \frac{1}{2}$ the distributions of zeros of families of L-functions behave like the distributions of eigenvalues near 1 of circular ensembles. In this work we develop an algorithm to draw random Haar distributed matrices from these groups. We conclude by comparing the results obtained for matrix ensembles to those obtained from zeros of L-functions associated to modular forms (these L-functions are very similar to those of elliptic curves).

2 Mathematical background

To understand the core of the present work, the reader should be familiar with some technical concepts which will be addressed in this section. In the main section, we discuss Haar measure over compact groups of matrices, so we provide a short introduction to said objects.

2.1 Quaternions $\mathbb{H}$

We denote the quaternion algebra with $\mathbb{H}$, this ring is different from $\mathbb{R}$ and $\mathbb{C}$ because multiplication is not commutative, thus it is not a field. However, inverses do exist, so the quaternions are a skew field. Now, we begin by defining quaternion units as

$$i_1^2 = i_2^2 = i_3^2 = i_1 i_2 i_3 = -1$$

This implies that

$$i_1 i_2 = -i_2 i_1 = i_3$$

$$i_2 i_3 = -i_3 i_2 = i_1$$

$$i_3 i_1 = -i_1 i_3 = i_2$$

Since these form a basis for the quaternions over $\mathbb{R}$, we can express any number $q \in \mathbb{H}$ as $q = a + bi_1 + ci_2 + di_3$ with $a, b, c, d \in \mathbb{R}$. Its conjugate $\overline{q} = a - bi_1 - ci_2 - di_3$. And its norm $||q||^2 = q\overline{q} = a^2 + b^2 + c^2 + d^2$. This in turn justifies the existence of the multiplicative inverse, namely, $q^{-1} = \frac{\overline{q}}{||q||^2}$ for any quaternion $q \neq 0$.

2.2 Classical compact groups

A **topological group** is a topological space (G, τ) equipped with a continuous multiplication and inverse [1].

$$G \times G \to G \qquad (x, y) \mapsto xy$$

$$G \to G \qquad g^{-1} \mapsto g$$

We make use of 3 compact groups, $U(N)$, $O(N)$ and $USp(2N)$ which will be defined in general and further discussed in the context of RMT.

2.2.1 $U(N)$

We first define the complex general inear group:

$$GL(N, \mathbb{C}) = \left\{ X \in \mathcal{M}_{n \times n}(\mathbb{C}) \;\middle|\; det(X) \neq 0 \right\}.$$

Equipped with the subspace topology from $\mathcal{M}_{n\times n}(\mathbb{C})$. It is a group under matrix multiplication since every matrix is invertible. Now we define the **unitary group** as subgroup of $GL(N,\mathbb{C})$:

$$U(N) = \left\{ X \in GL(N,\mathbb{C}) \;\middle|\; XX^* = X^*X = I \right\}$$

where X^* is the conjugate transpose of X. Important remarks are that $|\det(X)| = 1$ and that both $GL(N,\mathbb{C})$ and $U(N)$ are compact [1].

2.2.2 $SO(N)$

Similarly we define the general linear group:

$$GL(N,\mathbb{R}) = \left\{ X \in \mathcal{M}_{n\times n}(\mathbb{R}) \;\middle|\; det(X) \neq 0 \right\}$$

The invertibility of matrices guarantees $GL(N,\mathbb{R})$ is a group under multiplication. It is equipped with the subspace topology from $\mathcal{M}_{n\times n}(\mathbb{R})$. Now we define the **orthogonal group** as a subgroup of $GL(N,\mathbb{R})$:

$$O(N) = \left\{ X \in GL(N,\mathbb{R}) \;\middle|\; XX^T = X^TX = I \right\}$$

However, in the real case, we will focus on the **special orthogonal group** $SO(N)$ defined as a subgroup of $O(N)$:

$$SO(N) = \left\{ X \in O(N) \;\middle|\; \det(X) = 1 \right\}$$

We make the following observations:

$$GL(N,\mathbb{R}) \subset GL(N,\mathbb{C})$$

$$SO(N) \subset O(N) \subset \ U(N)$$

2.2.3 $USp(2N)$

Analogously we define the general linear group for quaternions:

$$GL(N,\mathbb{H}) = \left\{ X \in \mathcal{M}_{n\times n}(\mathbb{H}) \;\middle|\; det(X) \neq 0 \right\}$$

We proceed as in $U(N)$ and $O(N)$ to define the subgroup of $GL(N,\mathbb{H})$ analogue to the unitary and orthogonal groups. The **symplectic group** $Sp(N)$ can be defined as:

$$Sp(N) = \left\{ X \in GL(N,\mathbb{H}) \;\middle|\; X^*X = XX^* = I \right\}$$

Where X^* is the quaternionic conjugate transpose. And we define the **unitary symplectic group** $USp(2N)$ to be:

$$USp(2N) = \left\{ X \in U(2N) \;\middle|\; XJX^T = J \right\}$$

where

$$J = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}$$

and I_N denotes the identity matrix of order N.

There exists an isomorphism between $Sp(N)$ and $USp(2N)$ given by identifying quaternionic units as follows [16]:

$$1 \to I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i_1 \to e_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; i_2 \to e_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; i_3 \to e_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Observe that any matrix $\mathcal{Q} \in Sp(N) \subset GL(N, \mathbb{H})$ can be written as $\mathcal{Q} = Q_0 + i_1 Q_1 + i_2 Q_2 + i_3 Q_3$ where $Q_0,\ Q_1,\ Q_2,\ Q_3$ are $N \times N$ matrices with real entries. We can map $\mathcal{Q}$ to $Q \in USp(2N)$ isomorphically with the tensor product [16]:

$$Q = Q_0 \otimes I_2 + Q_1 \otimes e_1 + Q_2 \otimes e_2 + Q_3 \otimes e_3 \tag{6}$$

2.3 Haar measure

A Haar measure over a topological group is a measure that is invariant under group operation. Let $(X, \mathcal{F}, \mu)$ be a measure space, where X is a locally compact topological group, $\mathcal{F}$ is the σ-algebra of Borel sets of X and μ a Borel measure.

We say that μ is a (left) Haar measure provided:

$$\mu(xE) = \mu(E) \qquad \forall x \in X \text{ and } E \in \mathcal{F} \tag{7}$$

$$\mu(U) > 0 \qquad \forall U \text{ open, } U \neq \emptyset \tag{8}$$

$$\mu(K) < \infty \qquad \forall K \text{ compact} \tag{9}$$

Observe that condition (7) means that μ is translation invariant. For compact groups, left and right Haar measures are equivalent. Furthermore, Von Neumann proved Haar measure's uniqueness (up to constant) and existence for locally compact topological groups [8].

Consider the case when $X = \mathbb{R}$ under addition equipped with the Lebesgue measure. An interval $I = [a, b]$ is clearly measurable. So consider

$$\mu(I) = b - a$$

But note that we could translate this interval anywhere on the real line and its measure is unchanged, i.e. for $x \in \mathbb{R}$

$$\mu(x + I) = \mu([x + a, x + b]) = b - a = \mu(I)$$

More generally, for measurable $E \subset \mathbb{R}$,

$$\mu(E) = \int_E dx$$

Heine Borel guarantees that every compact subset of $\mathbb{R}$ has finite Lebesgue measure. And condition (8) is satisfied for any open set. Thus in $\mathbb{R}$ the Lebesgue measure is a Haar measure.

Now let us consider $X = \mathbb{R}^+$ equipped with multiplication. We want to find a measure μ such that it is invariant under scaling of a set, i.e. $\mu(xE) = \mu(E)$ for measurable $E \subset \mathbb{R}^+$. Let us first consider an interval $I = [a, b]$, $0 < a < b$ and observe that if we let

$$\mu(I) = \log(b) - \log(a)$$

Thus, for $x \in \mathbb{R}^+$

$$\mu(xI) = \mu([xa, xb]) = \log(xb) - \log(xa) = \log(x) + \log(b) - (\log(x) - \log(a)) = \mu(I)$$

Then we can state this more generally for measurable E and consider

$$\mu(E) = \int_E \frac{dx}{x}$$

Note that for $c \in \mathbb{R}^+$,

$$d\mu = \frac{dx}{x} = \frac{cdx}{cx} = \frac{d(cx)}{cx}$$

Shows that μ is invariant under scaling by c. Thus showing it is an invariant measure under scaling. An important remark is that these groups are locally compact, however, commutativity shows that left and right Haar measure are equal. An example for one of the compact groups, $U(N)$ is explained next:

If we consider, say, $U(1)$ then the elements we get are of the form $e^{i\theta}$ so we obtain elements on the unit circle S^1 and multiplication of such elements are rotations. Now, let μ be a Haar measure and we state its invariance property:

$$d\mu(U) = d\mu(UU_0) \tag{10}$$

Observe that if $U = e^{i\theta}$, $0 \leq \theta < 2\pi$ then $\mu(U)$ measures the perimeter of the circle (i.e. it is the Lebesgue measure on S^1). And if $U_0 = e^{i\theta_0}$, then it is obvious that $\mu(UU_0)$ only experiences a rotation by θ_0 and that does not affect what it measures. This notion of uniformity can be generalized for greater values of N following the same idea and intuition. And in similar ways to $SO(N)$ and $USp(N)$.

3 Random Matrix Groups

In this section we will discuss three ensembles of random matrices from which we seek to draw matrices to ultimately model zeros of L-functions. An ensemble is a group of matrices equipped with a probability measure. We aim to obtain Haar distributed random matrices from 3 different ensembles: Circular Unitary Ensemble (CUE), Circular Orthogonal Ensemble (COE) (to be later transformed into matrices of positive determinant) and Circular Symplectic Ensemble (CSE).
However, this cannot be done directly. We derive a way to draw these matrices from other ensembles, which are easier to compute and whose probability measure is more intuitive. The Ginibre ensembles, which are matrices whose entries are normal standard independent identically distributed random variables. We have these ensembles for real, complex and quaternion entries. Furthermore, observe that the matrix spaces for each ensemble are their respective general linear groups. Next we describe the process in which we can obtain random matrices from the circular ensembles starting with matrices from the Ginibre ensembles.
We describe the process very thoroughly for the CUE, the other two circular ensembles follow a similar process which is described more generally.

3.1 U(N)

Let Z be an N by N complex matrix with standard normal i.i.d. entries. Then its joint probability density function can be written as [16]:

$$P(Z) = \frac{1}{\pi^{N^2}} \exp(-Tr(Z^* Z)) \tag{11}$$

Which leads naturally to a measure:

$$d\mu_G(Z) = P(Z)dZ \tag{12}$$

if we denote the entries of Z as $z_{jk} = x_{jk} + iy_{jk}$, then $dZ = \prod_{j,k=1}^{N} x_{jk}y_{jk}$.

Observe that if $U \in U(N)$,

$$\begin{aligned} P(UZ) =& \frac{1}{\pi^{N^2}} \exp(-Tr(Z^*U^*UZ)) \\ =& \frac{1}{\pi^{N^2}} \exp(-Tr(Z^*Z)) \\ =& P(Z) \end{aligned}$$

Thus

$$d\mu_G(Z) = d\mu_G(UZ) \tag{13}$$

and we conclude that the measure in the Ginibre ensemble is invariant under left multiplication by unitary matrices. Right multiplication follows analogously.

An explicit measure for $U(N)$ cannot be established as easily as in the Ginibre ensemble because entries of the matrices are not independent. However, compactness of $U(N)$ guarantees there exists a unique (up to a constant) Haar measure in $U(N)$. Thus if we find a way to induce property (13) to a measure in $U(N)$, this must be the Haar measure.

We aim to induce such a measure by using QR factorization. We need to be careful in doing this. Observe that

$$QR : GL(N, \mathbb{C}) \longrightarrow U(N) \times T(N)$$

(where $T(N) \subset GL(N, \mathbb{C})$ is the set of upper triangular matrices) is a multi-valued map. Consider

$$Z = QR$$

Let $\Lambda \in T(N)$ be diagonal unitary and not the identity. Observe that:

$$Q' = Q\Lambda \qquad R' = \Lambda^{-1}R \tag{14}$$

Thus

$$Z = QR = Q'R' \tag{15}$$

So Z admits many representations under this map. The main idea is to choose an appropriate subset of $U(N) \times T(N)$ so that this map can be made into a uniquely valued one to one mapping. We know (14) implies (15), we claim the converse is also true. Note that (14) is equivalent to showing

$$Q^{-1}Q' = RR'^{-1} \quad \in \Lambda(N) \tag{16}$$

Where $\Lambda(N)$ is the set of diagonal matrices from $U(N)$. Furthermore if we assume (15) then

$$Q^{-1}Q' = RR'^{-1} \tag{17}$$

Observe that the LHS of the equality implies the matrix is unitary and RHS implies it is upper triangular, thus showing it is diagonal. This characterizes equivalent representations of Z under the multivalued map. Therefore, we consider the group of right cosets $\Gamma(N) = T(N)/\Lambda(N)$. And define QR factorization as a map

$$QR : GL(N, \mathbb{C}) \longrightarrow U(N) \times \Gamma(N)$$

This is now defined on classes of representatives of $\Gamma(N)$. If we choose the class of representatives R such that its diagonal is real and positive, then QR is uniquely valued and one to one in this class [14].

Thus, $Z = QR$ can be made unique using (14) with Λ chosen so that R' has positive real diagonal. Unique factorization implies that for $Z \in GL(N, \mathbb{C})$ and $U \in U(N)$ then

$$Z = QR \implies UZ = UQR. \tag{18}$$

It follows from this result that the invariance of the measure in the Ginibre ensemble shown in (13) is induced on $U(N)$. Since $U(N)$ is compact then it must be the Haar measure.

An important result from Haar measure on the CUE is that eigenvalues of unitary Haar distributed matrices are uniformly distributed in S^1 which further justifies the notion of Haar measure as an analogue for the uniform distribution. There are, however, other relevant eigenvalue statistics from this ensemble.(See [5]).

3.2 $SO(N)$

Let X be a real matrix with standard normal i.i.d. entries, i.e. from the real Ginibre ensemble. We proceed exactly as with the complex case. We define the probability measure with the joint probability density function as follows:

Let

$$P(X) = \frac{1}{\pi^{N^2}} \exp(-Tr(X^T X)) \tag{19}$$

If we define the measure as

$$d\mu_G(X) = P(X)dX \tag{20}$$

where x_{jk} are the entries of X and $dX = \prod_{j,k=1}^{N} x_{jk}$.

Furthermore, it is invariant under left and right multiplication by orthogonal matrices. We proceed in a similar fashion as in the complex case and factorize X using QR. So we take the multi-valued map:

$$QR : GL(N, \mathbb{R}) \longrightarrow O(N) \times T(N)$$

(where $T(N) \subset GL(N, \mathbb{R})$ is the set of upper triangular matrices). We modify this map as we did with the map for complex matrices, since $O(N)$ is also compact then Haar measure is also induced by this factorization.

This yields an algorithm to get Haar distributed matrices in $O(N)$. However, our final aim is to obtain matrices in $SO(N)$. We do this by subjecting output matrices in $O(N)$ to a map that changes the sign of the first column of a matrix if it has negative determinant and does nothing if it has positive determinant. This does not affect the previously induced Haar measure.

The intuition behind understanding this proof can be explained with an analogy: assume we have a subset of the integers, say $[-N, N] \cap \mathbb{Z}$ for some $N > 0$. Additionally, assume we have a uniform probability associated to each integer. Now, if we were to translate our map to this context, it would mean that if we draw from our subset of integers and we get a negative integer, we multiply by negative one and count the positive result. The important observation is that this does nothing more than to double the chances of getting positive numbers, leaving the uniformity of the distribution unaffected.

Let $J \in O(N)$ such that:

$$J = \begin{pmatrix} -1 & 0 \\ 0 & I_{N-1} \end{pmatrix}$$

Then we observe that we can write $O(N) = SO(N) \cup SO(N)J$. Now, say we have a matrix $X \in O(N)$, we define a function

$$f : O(N) \to SO(N)$$

such that

$$f(X) = \begin{cases} X, & \text{if } X \in SO(N) \\ XJ, & \text{if } X \in SO(N)J \end{cases}$$

We know we have a measure space $(O(N), \mathcal{F}, \mu)$ where μ is the Haar measure. We want to show that the measure space of $SO(N)$ induced by f has the same measure (up to scalar multiplication and translation). Let $(SO(N), \mathcal{F}', \mu')$ be the measure space induced by f, where $\mathcal{F}' = \{f(E) | E \in \mathcal{F}\}$. Observe that for measurable $E \in \mathcal{F}'$

$$\mu'(E) = \mu(f^{-1}(E)) = \mu(E \cup EJ)$$

Since μ is invariant under group multiplication and $J \in O(N)$, then $\mu(EJ) = \mu(E)$. Additionally, since $E \cap EJ = \emptyset$,

$$\mu'(E) = \mu(E \cup EJ) = \mu(E) + \mu(EJ)$$

$$= 2\mu(E)$$

So it holds that the measure is not affected under the algorithm used to obtain matrices in $SO(N)$.

3.3 $USp(2N)$

We proceed as in the two previous cases but change the matrix entries to quaternions. Note that for the quaternionic Ginibre ensemble we get an invariant measure under multiplication by symplectic matrices. Furthermore, QR decomposition is a multi-valued mapping

$$QR : GL(N, \mathbb{H}) \longrightarrow Sp(N) \times T(N)$$

where $T(N) \subset GL(N, \mathbb{H})$ is the set of upper triangular matrices. This mapping can be made into a one to one mapping that induces Haar measure on $Sp(N)$ [16]. At this point we use the isomorphism given by the tensor product described in (6). Thus getting Haar distributed matrices from $USp(2N)$.

The algorithm in question requires QR factorization which is available in mathematical packages for both $\mathbb{R}$ and $\mathbb{C}$. However, we stumbled upon the lack of such routines implemented for matrices with quaternionic entries. This problem is solved by implementing QR decomposition using Householder reflections.

4 Algorithms

We aim to model low lying zeros of L-functions with ensembles of random matrices. So we need an algorithm that returns eigenvalues of Haar distributed random matrices from each of the classical compact groups.

Next, we present the general algorithm, `myhaar_measure(N)` to generate these matrices

Algorithm 1 Calculate eigenvalues from a matrix in one of the circular ensembles. *myhaar_measure*(N, F)

```
Require: $N \in \mathbb{N}$ and $F$ is $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$
  Create an $N \times N$ random matrix $Z$ with i.i.d. entries over $F$
  Decompose $Z$ with Householder reflections so that $Z = QR$.
  Create the following matrix:
      $\Lambda = \begin{pmatrix} \frac{r_{11}}{||r_{11}||} & & \\ & \ddots & \\ & & \frac{r_{NN}}{||r_{NN}||} \end{pmatrix}$
  where the $r_{jj}$ are the diagonal elements of $R$.
  Calculate $Q' = Q\Lambda$ which is Haar distributed.
  if $F = \mathbb{R}$ then
    if $\det(Q') = -1$ then
      $Q_{Final} = Q'J$ where $J$ is the matrix that changes the sign of the first column of $Q'$
    end if
  end if
  if $F = \mathbb{H}$ then
    Map $Q'$ to a matrix $Q_{Final} \in USp(2N)$ using the tensor product in (6).
  end if
  if $F = \mathbb{C}$ then
    $Q_{Final} = Q'$
  end if
  return Eigenvalues of $Q_{Final}$
```

Since QR is required, we used the Householder reflections:

The algorithm takes an invertible $N \times N$ matrix A with entries in $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

A Householder matrix H_n works depending on an n dimensional vector v. Such a matrix can be constructed so that v is projected onto $e_1 = (1, 0, \ldots, 0)$:

$$H_n(v)v = ||v||e_1$$

This is done by reflecting v over an appropriate vector. Since there are well defined norms in each of the rings we aim to discuss, we can state the Householder algorithm in general for matrices with entries in $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. Additionally, we have conjugate transposes in each ring (for the real case it is the same as just transposition). So we use norms $||\cdot||$ and conjugate transposes * without specifying which of the rings we are using. We can find the Householder reflection for a vector $v = (v_1, v_2, ..., v_n)$ in the following way:

Let $\hat{v} = \frac{v}{||v||}$ and let $c = \frac{v_1}{||v_1||}$ then

$$H_n(\hat{v}) = -\overline{c}(I - 2\hat{u}\hat{u}^*)$$

where

$$\hat{u} = \frac{\hat{v} + ce_1}{||\hat{v} + ce_1||}$$

Given a matrix $A_{N\times N}$, we find a Householder matrix depending on its first column vector a_1 so that the product $H_N A$ is a matrix where the first column is projected onto e_1, i.e. every entry after the first row in the first column vector of $H_N A$ is 0. We repeat this by now taking a Householder matrix H_{N-1} which depends on the second column vector of $H_N A$ starting at the second row so it is $N-1$ dimensional. We want to be able to multiply this result by $H_N A$ and not affect its structure in the first column. So set up another matrix in the following way:

$$\tilde{H}_{N-1} = \begin{pmatrix} 1 & 0 \\ 0 & H_{N-1} \end{pmatrix}$$

Thus $\tilde{H}_{N-1} H_N A$ has second column vector also 0 after the second row and this repeats until we get to H_1 so the product

$$\tilde{H}_1 \dots \tilde{H}_{N-1} H_N A = R$$

is upper triangular and

$$A = H_N^* \tilde{H}_{N-1}^* \dots \tilde{H}_1^* R$$

So

$$Q = H_N^* \tilde{H}_{N-1}^* \dots \tilde{H}_1^*$$

We present implementations for all of the algorithms discussed in the following section along with their respective timings.

4.1 Implementations

Implementations in Sage 8.7 can be found in the online repository (See [19]). Next we show timings from running the functions `myhaar_measureSO(N)`, `myhaar_measureU(N)` and `myhaar_measureUSp(N)` 1000 times each for different values of N on a 1.4 GHz Quad-Core Intel Core i5 processor.

Table 1: Timings for implementations in Sage.

N	$SO(N)$	$U(N)$	$USp(2N)$
6	2.97s	7.52 s	30.2 s
12	8.08 s	32.1 s	3min 34s
25	33.5 s	3min 10s	36min 35s
50	2min 59s	23min 17s	6h 46min 14s

4.2 Preliminary results

To test the algorithms we ran the implementations over 100000 50 × 50 matrices with randomly distributed entries over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. See Figures 1 2 3 for our results:

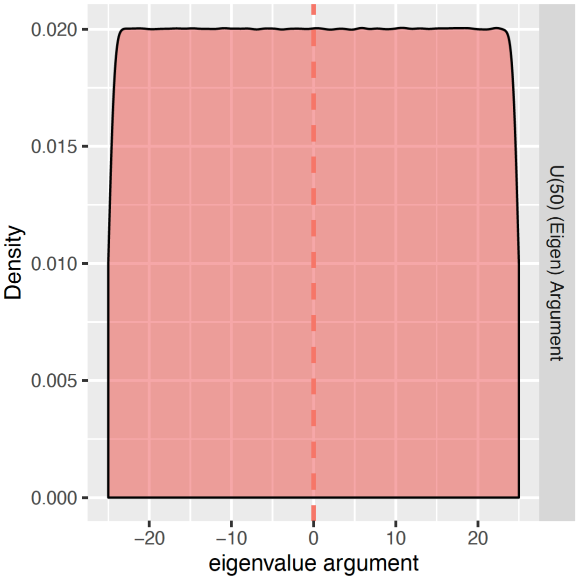

Figure 1: Results from running `myhaar_measureU(50)` 100000 times. We obtain a uniform distribution of the argument of the eigenvalues as expected.

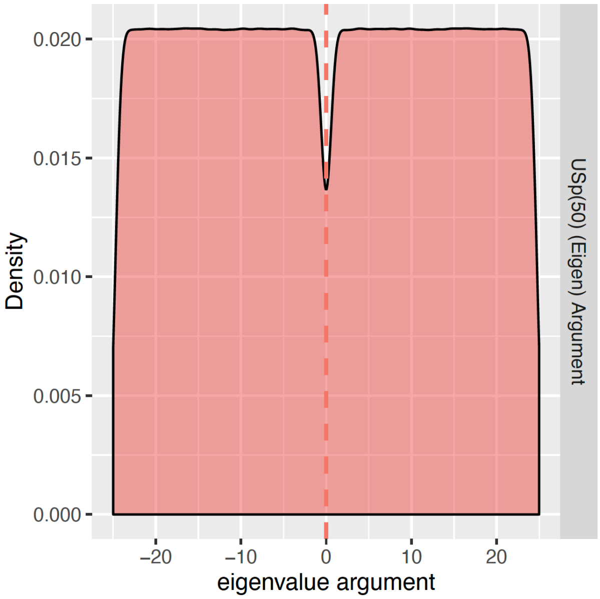

Figure 2: Results from running `myhaar_measureUSp(50)` 100000 times. In this case we see a lower density near 0. That shows there are less real eigenvalues in $USp(2N)$. The distribution shows that the frequency of eigenvalues with a non-zero argument is higher for the unitary symplectic group than the other compact groups.

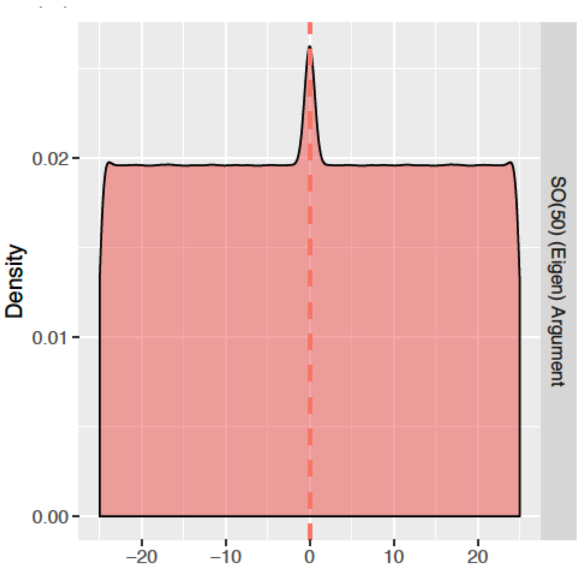

Figure 3: Results from running `myhaar_measureSO(50)` 100000 times. In this case there is a higher density in 0. That shows there are more real eigenvalues in $SO(N)$. The distribution shows that a real eigenvalue is more frequent for the special orthogonal group than the other compact groups.

5 Modeling families of L-functions

In this section we present experimental results comparing the low lying zeros of modular form L-functions and eigenvalues of random matrices. See [3,13,20] for more information on modular forms. We compare the minimum positive argument from eigenvalues of matrices in the three groups with the minimum positive zero from twists of L-functions.

The zeros of L-functions were computed using PARI/GP, Python, Slurm for parallel computing and Bucknell University's cluster BisonNet[1]. The algorithms in PARI/GP were implemented by Pascal Molin and Henri Cohen based on this article [3].

First we consider a particular example of modular form of weight 8 and level 3 (see [13, Modular Form 3.8.a.a])

[1] This material is based upon work supported by the National Science Foundation under Grant No. 1659397.

Its Fourier expansion begins with:

$$f(q) = q + 6q^2 - 27q^3 - 92q^4 + 390q^5 - 162q^6 - 64q^7 - 1320q^8 + 729q^9 + O(q^{10})$$

We study low lying zeros of quadratic twists $L(f, s, \chi_d)$ for this f.

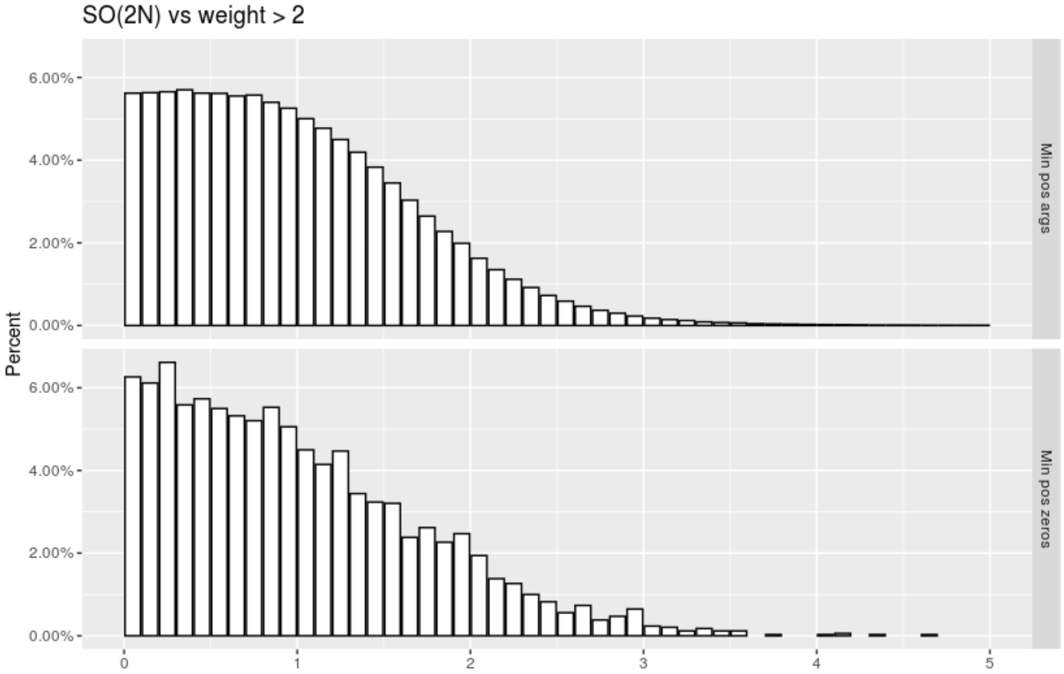

Figure 4: Minimum positive argument of eigenvalues from matrices in $SO(2N)$ vs minimum positive zeros from $L(f, s, \chi_d)$

See Figure 4 for our results; note that we scaled the distributions so that both have mean 1. Further, the similarity between the graph of the minimum positive argument for matrices in $SO(2N)$ and the minimum positive zeros for $L(f, s, \chi_d)$ shows that the distributions are very close together.

Now we consider another example of a modular form of weight 3 and level 7 (see [13, Modular Form 7.3.b.a]).

Its Fourier expansion begins with:

$$f(q) = q - 3q^2 + 5q^4 - 7q^7 - 3q^8 + 9q^9 + O(q^{10})$$

We study low lying zeros of quadratic twists $L(f, s, \chi_d)$ for this f.

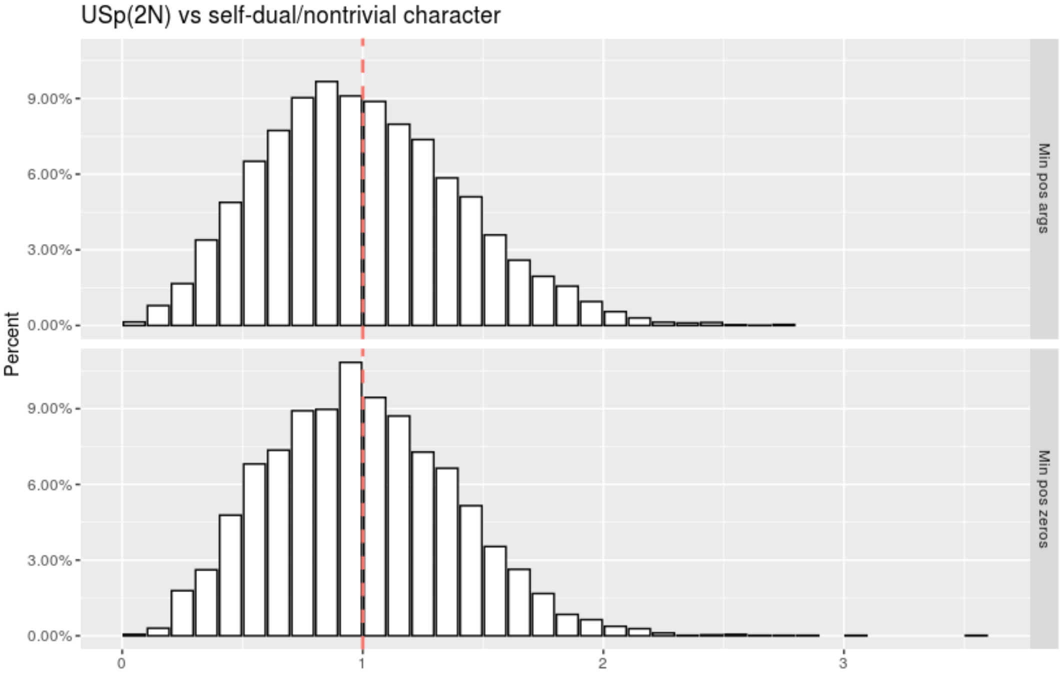

Figure 5: Minimum positive argument of eigenvalues from matrices in $USp(2N)$ vs minimum positive zeros from $L(f, s, \chi_d)$

For this case we also scaled the data so that the mean is 1 for both distributions. This shows similarity between distribution of low lying zeros of $L(s, f, \chi_d)$ and the least positive argument of eigenvalues from matrices in $USp(2N)$.

Finally we consider a modular form of weight 2 and level 12 (see [13, Modular Form 13.2.e.a]).

The coefficients of the Fourier expansion for this modular form are expressed in terms of a primitive root of unity ζ_6.

$$f(q) = q + (-1-\zeta_6)q^2 + (-2+2\zeta_6)q^3 + \zeta_6 q^4 + (1-2\zeta_6)q^5 + (4-2\zeta_6)q^6 + (-1+2\zeta_6)q^8 - \zeta_6 q^9 + O(q^{10})$$

We study low lying zeros of quadratic twists $L(f, s, \chi_d)$ for this f.

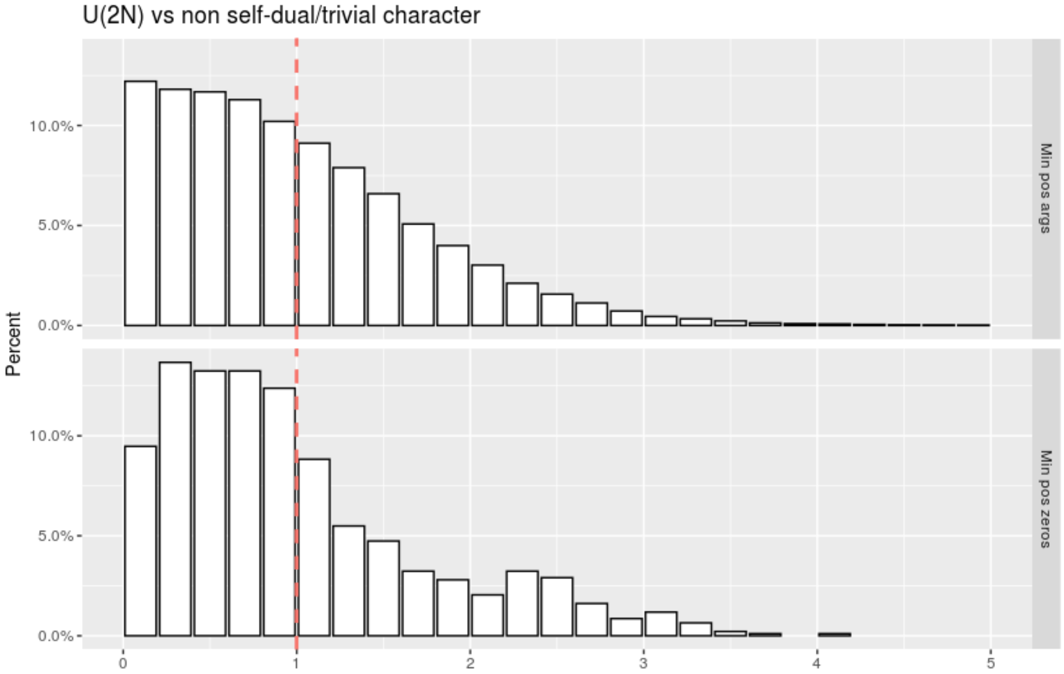

Figure 6: Minimum positive argument of eigenvalues from matrices in $U(2N)$ vs minimum positive zeros from $L(f, s, \chi_d)$

Means were also scaled to 1 for this case. Observe that the distributions are not as similar as those seen in Figure 4 and Figure 5. Finding zeros from this particular family of L-functions is computationally intensive, which limited this sample size to one tenth of the sample taken for the previous cases. This emphasizes the fact that these are **finite** approximations, which depend strongly on the sample size.

6 Conclusions

To summarize, this thesis displayed a connection between random matrices and L-functions. We developed an algorithm to draw matrices from the circular ensembles starting with an ensemble which is simpler to compute. Additionally, we showed the distribution of the arguments of eigenvalues our algorithm produces. Finally we compared results obtained from our algorithm with zeros from L-functions which further justify the correspondence between eigenvalues from random matrices and zeros from L-functions.

Understanding zeros from L-functions is an unsolved issue with important consequences. Of course, computing these numerically could yield some intuition on their nature. However, this process can be computationally complex. Thus, modeling these with random matices can be advantageous since their computing times are fairly short (See Table 1).

The correspondence of families of L-functions and groups of random matrices allows us to assign symmetry types to such families, which can help provide new insights into understanding families of L-functions. Additionally, this connection further suggests a spectral interpretation of zeros.

References

[1] Andrew Baker. *Matrix groups: An introduction to Lie group theory.* Springer Science & Business Media, 2012.

[2] Enrico Bombieri. Problems of the millennium: The riemann hypothesis, 2000.

[3] Henri Cohen. Computational number theory in relation with L-functions. In *Notes from the International Autumn School on Computational Number Theory*, pages 171–266. Springer, 2019.

[4] J Brian Conrey, Jonathan Keating, Michael Rubinstein, and Nina Snaith. On the frequency of vanishing of quadratic twists of modular l-functions. *arXiv preprint math/0012043*, 2000.

[5] Persi Diaconis and Mehrdad Shahshahani. On the Eigenvalues of Random Matrices. *Journal of Applied Probability*, 31:49–62, 1994.

[6] David Farmer, Ameya Pitale, Nathan Ryan, and Ralf Schmidt. Analytic L-functions: Definitions, theorems, and connections. *Bulletin of the American Mathematical Society*, 56(2):261–280, 2019.

[7] Leo Goldmakher. Legendre, Jacobi, and Kronecker symbols.

[8] Angela Spalsbury Joe Diestel. *The Joys of Haar Measure*, volume 150 of *Graduate Studies in Mathematics*. American Mathematical Society, 2014.

[9] J P Keating and N C Snaith. Random matrices andL-functions. *Journal of Physics A: Mathematical and General*, 36(12):2859–2881, mar 2003.

[10] Jeffrey C. Lagarias. An Elementary Problem Equivalent to the Riemann Hypothesis. *The American Mathematical Monthly*, 109(6):534–543, 2002.

[11] Laurent Laloux, Pierre Cizeau, Marc Potters, and Jean-Philippe Bouchaud. Random matrix theory and financial correlations. *International Journal of Theoretical and Applied Finance*, 03(03):391–397, 2000.

[12] Chao Li. Recent developments on quadratic twists of elliptic curves. 2018.

[13] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 2 May 2020].

[14] Tom Lyche. *Numerical Linear Algebra and Matrix Factorizations*. Springer Nature, 2020.

[15] Madan Lal Mehta. *Random matrices*. Elsevier, 2004.

[16] Francesco Mezzadri. How to generate random matrices from the classical compact groups, 2006.

[17] Steven J Miller, Steven J Miller, and Ramin Takloo-Bighash. *An invitation to modern number theory*. Princeton University Press, 2006.

[18] Ken Ono and Christopher Skinner. Non-vanishing of quadratic twists of modular l-functions. *Inventiones mathematicae*, 134:651–660, 11 1998.

[19] Nathan Ryan. Vanishings. `https://github.com/nathancryan/vanishings`, 2019.

[20] W. A. Stein and P. E. Gunnells. *Modular forms, a computational approach*, volume 79. American Mathematical Society Providence, RI, 2007.

[21] William Stein. *Elementary number theory: primes, congruences, and secrets: a computational approach*. Springer Science & Business Media, 2008.

[22] Antonia M. Tulino and Sergio Verdú. Random Matrix Theory and Wireless Communications. *Foundations and Trends in Communications and Information Theory*, 1(1):1–182, 2004.

[23] Andrew Wiles. The Birch and Swinnerton-Dyer Conjecture, 2006.