DOI: 10.1214/EJP.v7-108

Electronic Journal of Probability

Vol. 7 (2002) Paper No. 9, pages 1–15.

Journal URL
http://www.math.washington.edu/~ejpecp/
Paper URL
http://www.math.washington.edu/~ejpecp/EjpVol7/paper9.abs.html

EIGENVALUES OF RANDOM WREATH PRODUCTS [1]

Steven N. Evans
Department of Statistics #3860, University of California at Berkeley
367 Evans Hall, Berkeley, CA 94720-3860, U.S.A
evans@stat.Berkeley.EDU

Abstract Consider a uniformly chosen element X_n of the n-fold wreath product $\mathbf{\Gamma_n} = \mathbf{G} \wr \mathbf{G} \wr \cdots \wr \mathbf{G}$, where $\mathbf{G}$ is a finite permutation group acting transitively on some set of size s. The eigenvalues of X_n in the natural s^n-dimensional permutation representation (the *composition* representation) are investigated by considering the random measure Ξ_n on the unit circle that assigns mass 1 to each eigenvalue. It is shown that if f is a trigonometric polynomial, then $\lim_{n\to\infty} \mathbb{P}\{\int f\, d\Xi_n \neq s^n \int f\, d\lambda\} = 0$, where λ is normalised Lebesgue measure on the unit circle. In particular, $s^{-n}\Xi_n$ converges weakly in probability to λ as $n \to \infty$. For a large class of test functions f with non-terminating Fourier expansions, it is shown that there exists a constant c and a non-zero random variable W (both depending on f) such that $c^{-n} \int f\, d\Xi_n$ converges in distribution as $n \to \infty$ to W.

These results have applications to Sylow p-groups of symmetric groups and autmorphism groups of regular rooted trees.

Keywords random permutation, random matrix, Haar measure, regular tree, Sylow, branching process, multiplicative function

AMS subject classification (2000) Primary 15A52, 05C05, 60B15, 60J80

[1] RESEARCH SUPPORTED IN PART BY NSF GRANT DMS-0071468

1 Introduction

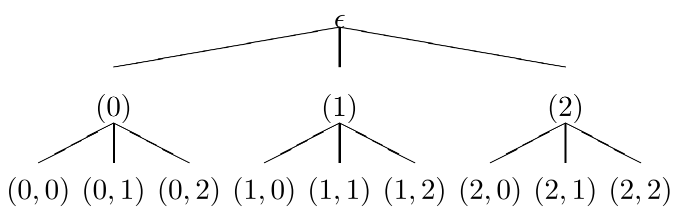
Let $\mathbf{T}$ denote the regular rooted b-ary tree of depth n. That is, $\mathbf{T}$ is a tree with $1+b+b^2+\cdots+b^n$ vertices such that one vertex (the root) has degree b, the b^n leaf vertices have degree 1, and all other vertices have degree $b+1$.

Consider the group $\mathbf{\Gamma}$ of automorphisms of $\mathbf{T}$. An element $\gamma \in \mathbf{\Gamma}$ is a permutation of the vertices of $\mathbf{T}$ such that the images of any two adjacent vertices (that is, two vertices connected by an edge) are again adjacent.

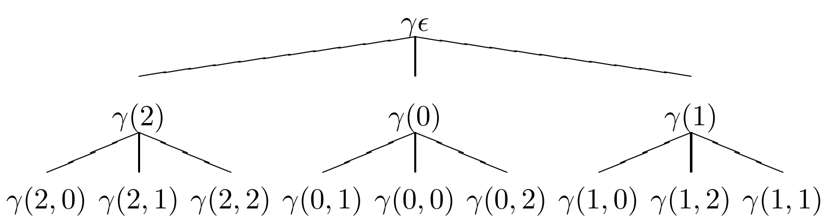
As usual, we may identify the vertices of $\mathbf{T}$ with the set of finite sequences of length at most n drawn from the set $\{0, 1, \ldots, b-1\}$. That is, we may label the vertices with the elements of $\epsilon \cup \{0, 1, \ldots, b-1\} \cup \{0, 1, \ldots, b-1\}^2 \cup \cdots \cup \{0, 1, \ldots, b-1\}^n$, where the empty sequence ϵ corresponds to the root, the length 1 sequences $\{0, 1, \ldots, b-1\}$ correspond to the vertices adjacent to the root, and the length n sequences $\{0, 1, \ldots, b-1\}^n$ correspond to the leaves. With this identification, each $\gamma \in \mathbf{\Gamma}$ maps sequences of length k into sequences of length k for $0 \leq k \leq n$. Moreover, if $\gamma(i_1, i_2, \ldots, i_k) = (j_1, j_2, \ldots, j_k)$, then $\gamma(i_1, i_2, \ldots, i_{k-1}) = (j_1, j_2, \ldots, j_{k-1})$.

plain

Example 1.1 The labelling for the 3-ary tree of depth 2 is:



An example of an element of the group $\mathbf{\Gamma}$ for this tree is:



That is, $\gamma\epsilon = \epsilon$, $\gamma(2) = (0)$, $\gamma(0) = 1$, $\gamma(1) = 2$, $\gamma(2,0) = (0,0)$, $\ldots$, $\gamma(1,1) = (2,2)$.

The group $\mathbf{\Gamma}$ is nothing other than the n-fold *wreath product* of the symmetric group on b letters, $\mathcal{S}_b$, with itself, usually written as $\mathcal{S}_b \wr \mathcal{S}_b \wr \cdots \wr \mathcal{S}_b$. We describe wreath products in general in Section 2. The group $\mathbf{\Gamma}$ can be thought of as a subgroup of the permutation group on the leaves of $\mathbf{T}$. Consequently, each automorphism $\gamma \in \mathbf{\Gamma}$ can be associated with the $b^n \times b^n$ permutation matrix that has a 1 in the (i,j) position if leaf i is mapped to leaf j by γ and has 0s elsewhere in the i^{th} row and j^{th} column. If $\mathbf{G}$ is an arbitrary permutation group acting on a finite set of size $s > 1$, then elements of the n-fold wreath product $\mathbf{G} \wr \mathbf{G} \wr \cdots \wr \mathbf{G}$ can be associated with an $s^n \times s^n$ permutation matrix in a similar manner.

In this paper we investigate the random permutation matrix associated with a uniformly chosen element of $\mathbf{G} \wr \mathbf{G} \wr \cdots \wr \mathbf{G}$ for $\mathbf{G}$ an arbitrary transitive permutation group. More specifically, we consider the random probability measure Ξ_n on the unit circle $\mathbb{T} \subset \mathbb{C}$ that assigns mass 1 to each of the eigenvalues (with their multiplicities) of this matrix and investigate the asymptotic behaviour as $n \to \infty$ of the integrals $\int_{\mathbb{T}} f \, d\Xi_n$ for suitable test functions f.

The outline of the rest of the paper is as follows. We define wreath products and list some of their elementary properties in Section 2. In Section 3, we observe some connections between the cycle counts of a uniform random pick from an iterated wreath product, the traces of powers of the associated permutation matrix, and the random measure Ξ_n. We establish the following result in Section 4: here λ is Lebesgue measure on the unit circle normalised to have total mass 1.

Theorem 1.2 *For a trigonometric polynomial $f(z) = \sum_{k=-m}^{m} c_k z^k$, $z \in \mathbb{T}$,*

$$\lim_{n\to\infty} \mathbb{P}\left\{ \int_{\mathbb{T}} f \, d\Xi_n \neq s^n c_0 \right\} = 0$$

In particular, the random probability measure $s^{-n}\Xi_n$ converges weakly in probability to λ as $n \to \infty$.

Theorem 1.2 leaves open the possibility of interesting behaviour for $\int_{\mathbb{T}} f \, d\Xi_n$ for certain functions f having non-terminating Fourier expansion $f(z) = \sum_{k=-\infty}^{\infty} c_k z^k$ with $c_0 = 0$. In Section 5, we show for certain such f that there exists a constant c and a non-zero random variable W (both depending on f) such that $c^{-n} \int f \, d\Xi_n$ converges in distribution as $n \to \infty$ to W.

We end this introduction with some bibliographic comments on the substantial recent interest in eigenvalues of random matrices in general and eigenvalues of Haar distributed random matrices from various compact groups in particular.

A general reference to the history of random matrix theory and its applications is [Meh91]. Asymptotics for the traces of powers of unitary, orthogonal and symplectic matrices (equivalently, integrals of powers against the analogue of the measure Ξ_n) are investigated in [DS94] (see also [Rai97]). Integrals of more general well-behaved functions against the analogue of Ξ_n for these groups are studied in [Joh97]. The number of eigenvalues in an interval for the unitary group (that is, the integral of an indicator function against the analogue of Ξ_n) is investigated in [Wie98]. The logarithm of the characteristic polynomial of a random unitary matrix is also the integral of a suitable function against the analogue of Ξ_n, and this object is the subject of [HKO01, KS00a, KS00b]. A general theory for the unitary, orthogonal and symplectic groups that subsumes much of this work is presented in [DE01].

Random permutations give rise to random permutation matrices. Given the connection between cycle counts of permutations and traces of the corresponding matrices that we recall in Section 3, some of the huge literature on the cycle structure of uniform random permutations can be translated into statements about eigenvalues of random permutation matrices. More in the spirit of this paper, the number of eigenvalues in an interval and the logarithm of the characteristic polynomial are investigated in [Wie00] and [HKOS00], respectively. The former paper treats not only the symmetric group, but also the wreath product of a cyclic group with a symmetric group.

There is a limited literature on other probabilistic aspects of wreath products. Various connections between automorphism groups of infinite regular trees and probability are explored in [AV02]. As we recall in Section 2, the Sylow p-group of $\mathcal{S}_{p^r}$ is a wreath product. The distribution of the order of a random element of this group is studied in [PS83b], while the distribution of the degree of a randomly chosen irreducible character is studied in [PS83a, PS89]. The probability that a randomly chosen element of $\mathcal{S}_n \wr \mathcal{S}_p$ has no fixed points as $n \to \infty$ is given in [DS95]. Mixing times of Markov chains on wreath products are considered in [FS01]. Finally, infinite wreath products are a fruitful source of examples of interesting behaviour and counterexamples in the study of random walks on infinite groups (see, for example, [KV83, LPP96, PSC99, Dyu99b, Dyu99a]).

2 Wreath products

We recall the general definition of a wreath product as follows. Let $\mathbf{G}$ and $\mathbf{H}$ be two permutation groups acting on sets of size s and t, respectively, which we will identify with $\{0, 1, \ldots, s-1\}$ and $\{0, 1, \ldots, t-1\}$. As a set, the wreath product $\mathbf{G} \wr \mathbf{H}$ of $\mathbf{G}$ and $\mathbf{H}$ is the Cartesian product $\mathbf{G}^t \times \mathbf{H}$; that is, an element of $\mathbf{G} \wr \mathbf{H}$ is a pair (f, π), where f is function from $\{0, 1, \ldots, t-1\}$ into $\mathbf{G}$ and $\pi \in \mathbf{H}$. Setting $f_\pi := f \circ \pi^{-1}$ for $f \in \mathbf{G}^t$ and $\pi \in \mathbf{H}$, the group operation on $\mathbf{G} \wr \mathbf{H}$ is given by $(f, \pi)(f', \pi') := (f f'_\pi, \pi\pi')$, where multiplication is coordinatewise in $\mathbf{G}^t$. It is not hard to see that for three permutation groups $\mathbf{G}, \mathbf{H}, \mathbf{K}$ the group $(\mathbf{G} \wr \mathbf{H}) \wr \mathbf{K}$ is isomorphic to the group $\mathbf{G} \wr (\mathbf{H} \wr \mathbf{K})$, and so it makes sense to refer to these isomorphic groups as $\mathbf{G} \wr \mathbf{H} \wr \mathbf{K}$. More generally, it makes sense to speak of the wreath product $\mathbf{G}_1 \wr \mathbf{G}_2 \wr \cdots \wr \mathbf{G}_n$ of n permutation groups $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_n$.

Excellent references for wreath products with extensive bibliographies are [Ker71, Ker75, JK81]. A reference that deals specifically with the automorphism groups of regular rooted trees and their representation theory is [AD02]. A connection between automorphism groups of regular trees and dynamical systems is explored in [BOERT96]. Besides their appearance as the automorphism groups of regular rooted trees, wreath products are important in the representation theory of the symmetric group and in various problems arising in the Polya–Redfield theory of enumeration under group action. Classically, they appeared in the work of Cauchy on Sylow p-groups of the symmetric group. For example, the Sylow p-group of $\mathcal{S}_{p^r}$, the symmetric group on p^r letters, is the r-fold wreath product $\mathcal{C}_p \wr \mathcal{C}_p \wr \cdots \wr \mathcal{C}_p$, where $\mathcal{C}_p$ is the cyclic group of order p (see 4.1.22 of [JK81]). A review of the uses of wreath products in experimental design and the analysis of variance is given in [BPRS83]. An intriguing application to spectroscopy can be found in [LH63].

For $\mathbf{G}$ and $\mathbf{H}$ as above, there is a natural representation of $\mathbf{G} \wr \mathbf{H}$ as a group of permutations of the set $\{0, 1, \ldots, t-1\} \times \{0, 1, \ldots, s-1\}$. In this permutation representation, the group element $(f, \pi) \in \mathbf{G} \wr \mathbf{H}$ is associated with the the permutation that sends the pair (i', i'') to the pair (j', j'') where $j' = \pi(i')$ and $j'' = f(\pi(i'))(i'')$. Consequently, $\mathbf{G} \wr \mathbf{H}$ has a linear representation in terms of $(ts) \times (ts)$ permutation matrices with rows and columns both indexed by $\{0, 1, \ldots, t-1\} \times \{0, 1, \ldots, s-1\}$. In this linear representation, the group element $(f, \pi) \in \mathbf{G} \wr \mathbf{H}$ is associated with the matrix M given by

$$M((i', i''), (j', j'')) = \begin{cases} 1, & \text{if } j' = \pi(i') \text{ and } j'' = f(\pi(i'))(i''), \\ 0, & \text{otherwise.} \end{cases}$$

Either of these representations is called the *composition* representation.

plain

Example 2.1 The automorphism group of the rooted 3-ary tree of depth 2 considered in Example 1.1 is $\mathcal{S}_3 \wr \mathcal{S}_3$, and so the resulting (linear) composition representation is 9-dimensional. The particular group element γ exhibited in Example 1.1 is given by the pair (f, π), where, in cycle notation,

$$\pi = (012),$$
$$f(0) = (01)(2),\ f(1) = (0)(12),\ f(2) = (0)(1)(2).$$

The corresponding matrix is

$$\begin{array}{c} \\ (0,0) \\ (0,1) \\ (0,2) \\ (1,0) \\ (1,1) \\ (1,2) \\ (2,0) \\ (2,1) \\ (2,2) \end{array}
\begin{array}{c} \begin{array}{ccccccccc} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) & (2,0) & (2,1) & (2,2) \end{array} \\
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix} \end{array}$$

plain

Definition 2.2 Suppose that $\mathbf{G}$ and $\mathbf{H}$ are two permutation groups acting on sets of size s and t. Consider $(f, \pi) \in \mathbf{G} \wr \mathbf{H}$. Suppose that $\pi \in \mathbf{H}$ has the cycle decomposition

$$\pi = \prod_{\nu=1}^{c(\pi)} \left(j_\nu \pi(j_\nu) \cdots \pi^{\ell_\nu - 1}(j_\nu) \right);$$

that is, π can be decomposed into $c(\pi)$ cycles, with the ν^{th} cycle of length ℓ_ν. The elements of $\mathbf{G}$ defined by

$$g_\nu(f, \pi) := f(j_\nu) f(\pi^{-1}(j_\nu)) \cdots f(\pi^{-(\ell_\nu - 1)}(j_\nu)) = f f_\pi \cdots f_{\pi^{\ell_n u - 1}}(j_\nu)$$

are called the *cycle products* of (f, π). Note that the definition of $g_\nu(f, \pi)$ depends on the choice of the cycle representative j_ν, so to give an unambigious definition we would need to specify how j_ν is chosen (for example, as the smallest element of the cycle). However, different choices of cycle representative lead to conjugate cycle products (see 4.2.5 of [JK81]).

The following result is 4.2.19 in [JK81].

Lemma 2.3 *Suppose that* $\mathbf{G}$ *and* $\mathbf{H}$ *are two permutation groups acting on sets of size* s *and* t*. Consider* $(f, \pi) \in \mathbf{G} \wr \mathbf{H}$*. Suppose that* $\pi \in \mathbf{H}$ *has the cycle decomposition*

$$\pi = \prod_{\nu=1}^{c(\pi)} \left(j_\nu \pi(j_\nu) \cdots \pi^{\ell_\nu - 1}(j_\nu) \right)$$

and that the ν^{th} cycle product $g_\nu(f,\pi)$ has a cycle decomposition into cycles of lengths $m_{\nu,1}, m_{\nu,2}, \ldots, m_{\nu,d(\pi,\nu)}$. Then the cycle decomposition of the composition representation of (f,π) consists of cycles of lengths $\ell_\nu m_{\nu,\eta}$, $1 \le \eta \le d(\pi,\nu)$, $1 \le \nu \le c(\pi)$.

The following is obvious and we leave the proof to the reader.

Lemma 2.4 *Suppose that $\mathbf{G}$ and $\mathbf{H}$ are two permutation groups acting on sets of size s and t, respectively. A $\mathbf{G} \wr \mathbf{H}$-valued random variable (F,Π) is uniformly distributed if and only if*

- *The $\mathbf{H}$-valued random variable Π is uniformly distributed.*
- *The coordinates of the $\mathbf{G}^t$-valued random variable F are uniformly distributed on $\mathbf{G}$ and independent.*
- *The random variables F and Π are independent.*

3 Random elements of iterated wreath products

Suppose from now on that we fix a permutation group $\mathbf{G}$ acting on a finite set of size $s > 1$. For simplicity, we will suppose that $\mathbf{G}$ acts transitively.

Let X_n be a uniform random pick from the n-fold wreath product

$$\mathbf{\Gamma_n} := \mathbf{G} \wr \mathbf{G} \wr \cdots \wr \mathbf{G}.$$

The random group element X_n will have a corresponding composition representation M_n. If we wished to describe the distribution of the $s^n \times s^n$ random matrix M_n, we would need to specify the order in which the successive "wreathings" were performed. However, two different orders produce matrices that are similar (with the similarity effected by a permutation matrix), and so the eigenvalues of the composition representation of X_n (and their multiplicities) are well-defined without the need for specifying such an order. As in the Introduction, let Ξ_n denote the random discrete measure of total mass s^n on the unit circle $\mathbb{T} \subset \mathbb{C}$ that is supported on this set of eigenvalues and assigns a mass to each eigenvalue equal to its multiplicity.

Note that

$$\begin{aligned}
&\int_{\mathbb{T}} z^k \, \Xi_n(dz) \\
&\quad = \operatorname{Tr}(M_n^k) = \overline{\operatorname{Tr}(M_n^k)} = \operatorname{Tr}(\overline{M_n}^k) \\
&\quad = \int_{\mathbb{T}} \bar{z}^k \, \Xi_n(dz) = \int_{\mathbb{T}} z^{-k} \, \Xi_n(dz),
\end{aligned} \tag{3.1}$$

and so the behaviour of $\int_{\mathbb{T}} f \, d\Xi_n$ for a function f with Fourier expansion $f(z) = \sum_{k=-\infty}^{\infty} c_k z^k$ is determined by the behaviour of the random variables $T_{n,k} := \operatorname{Tr}(M_n^k)$, $k \ge 1$.

Let $S_{n,k}$ denote the number of k-cycles in the composition representation of X_n. By a standard fact about permutation characters (see, for example, 6.13 of [Ker75]),

$$T_{n,k} = \sum_{\ell | k} \ell S_{n,\ell}, \tag{3.2}$$

and hence, by Möbius inversion,

$$S_{n,k} = \frac{1}{k} \sum_{\ell | k} \mu\left(\frac{k}{\ell}\right) T_{n,\ell}, \tag{3.3}$$

where μ is the usual Möbius function

$$\mu(i) := \begin{cases} (-1)^j, & \text{if } i \text{ is the product of } j \text{ distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, it is equally useful to study the random variables $S_{n,k}$, $k \geq 1$.

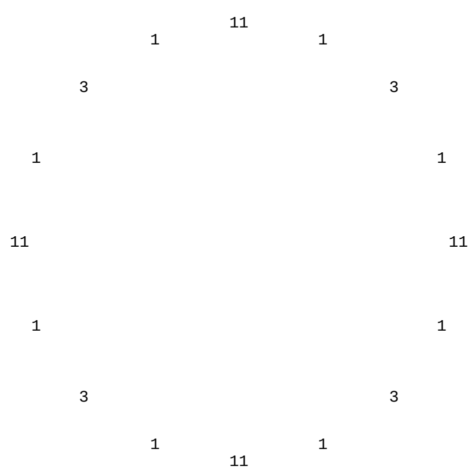
plain

Example 3.1 Consider the n-fold wreath product $\mathcal{S}_2 \wr \mathcal{S}_2 \wr \cdots \wr \mathcal{S}_2$, that is, the group of automorphisms of the regular rooted binary tree of depth n (so that the composition representation has dimension 2^n). It follows from Lemma 2.3 that the cycle count $S_{n,k}$ is 0 unless k is of the form 2^j, $0 \leq j \leq n$. Observe from (3.2) that if $k = 2^h r$ where $2 \nmid r$, then

$$T_{n,k} = \sum_{2^j | k,\, j \leq n} 2^j S_{n,2^j} = \sum_{2^j | 2^h,\, j \leq n} 2^j S_{n,2^j} = T_{n,2^{h \wedge n}}.$$

It thus suffices to understand the random variables $T_{n,2^h}$, $0 \leq h \leq n$.

A simulated realisation of the random group element X_6 resulted in the eigenvalues shown (with multiplicities) in (3.4).



(3.4)

The corresponding realisations of the traces are

$$T_{6,1} = 0,\, T_{6,2} = 0,\, T_{6,4} = 32,\, T_{6,8} = 48,\, T_{6,16} = 64,\, T_{6,32} = 64,\, T_{6,64} = 64,$$

and, by (3.3), the corresponding realisations of the cycle counts are

$$S_{6,1} = 0,\, S_{6,2} = 0,\, S_{6,4} = 8,\, S_{6,8} = 2,\, S_{6,16} = 1,\, S_{6,32} = 0,\, S_{6,64} = 0.$$

We note that the eigenvalues in (3.4) can be computed from the cycle counts (and hence the traces) as follows. Observe from the cycle counts that, by a suitable common permutation of the rows and columns, the composition representation matrix becomes block diagonal with 8 4×4 blocks, 2 8×8 blocks, and 1 16×16 block – each block of the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Such a $2^k \times 2^k$ block has the $(2^k)^{\text{th}}$ roots of unity as its eigenvalues. Thus each 4^{th} root of unity appears as an eigenvalue of the composition representation matrix with multiplicity $11 = 8+2+1$, each 8^{th} root of unity that is not a 4^{th} root appears with multiplicity $3 = 2 + 1$, and each 16^{th} root of unity that is not an 8^{th} root appears with multiplicity 1.

Here are 10 more simulated realisations of the traces $T_{6,2^h}$, $0 \le h \le 6$.

$$\begin{array}{c} \begin{array}{ccccccc} T_{6,1} & T_{6,2} & T_{6,4} & T_{6,8} & T_{6,16} & T_{6,32} & T_{6,64} \end{array} \\ \begin{pmatrix} 2 & 20 & 40 & 64 & 64 & 64 & 64 \\ 0 & 0 & 16 & 48 & 64 & 64 & 64 \\ 0 & 0 & 0 & 0 & 0 & 64 & 64 \\ 0 & 0 & 24 & 64 & 64 & 64 & 64 \\ 2 & 16 & 32 & 64 & 64 & 64 & 64 \\ 10 & 36 & 56 & 64 & 64 & 64 & 64 \\ 8 & 20 & 56 & 64 & 64 & 64 & 64 \\ 0 & 0 & 0 & 16 & 64 & 64 & 64 \\ 14 & 44 & 56 & 64 & 64 & 64 & 64 \end{pmatrix} \end{array}.$$

The corresponding realisations of the cycle counts are

$$\begin{array}{c} \begin{array}{ccccccc} S_{6,1} & S_{6,2} & S_{6,4} & S_{6,8} & S_{6,16} & S_{6,32} & S_{6,64} \end{array} \\ \begin{pmatrix} 2 & 9 & 5 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 6 & 5 & 0 & 0 & 0 \\ 2 & 7 & 4 & 4 & 0 & 0 & 0 \\ 10 & 13 & 5 & 1 & 0 & 0 & 0 \\ 0 & 4 & 8 & 3 & 0 & 0 & 0 \\ 8 & 6 & 9 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 3 & 0 & 0 \\ 14 & 15 & 3 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Using the facts we develop below in Section 4, it is not difficult to show in this example that $\mathbb{E}[T_{n,1}] = 1$ and $\mathbb{E}[T_{n,2}] = n+1$. (In general, $\mathbb{E}[S_{n,p}] = n\mu_p$ and $\mathbb{E}[T_{n,p}] = 1+np\mu_p$ for a prime p, where μ_k denotes the expected number of k-cycles in the cycle decomposition of a permutation chosen uniformly at random from $\mathbf{G}$.) However, 5 realisations out of 11 resulted in the value 0 for both $T_{6,1}$ and $T_{6,2}$. This suggests that for large n the random variables $T_{n,1}$ and $T_{n,2}$ take the value 0 with probability close to 1, while the expectation is maintained by large values being taken with probability close to 0. Theorem 1.2 shows that this is indeed the case.

4 Proof of Theorem 1.2

In order to prove the theorem, it suffices by (3.1) to show that

$$\lim_n \mathbb{P}\{T_{n,k} \neq 0\} = 0 \text{ for all } k \geq 1.$$

By (3.2), it suffices in turn to show that

$$\lim_n \mathbb{P}\{S_{n,k} \neq 0\} = 0 \text{ for all } k \geq 1. \tag{4.1}$$

We will now choose a specific order of the successive "wreathings" in the construction of $\mathbf{\Gamma_n} = \mathbf{G} \wr \mathbf{G} \wr \cdots \wr \mathbf{G}$ that leads to a useful inductive way of constructing $X_1, X_2, \ldots$ on the one probability space. Take $\mathbf{\Gamma_n} = \mathbf{G} \wr (\mathbf{G} \wr (\mathbf{G} \wr (\cdots \wr \mathbf{G}) \ldots))$. In other words, think of $\mathbf{\Gamma_n}$ as a permutation group on a set of size s^n and build $\mathbf{\Gamma_{n+1}}$ as $\mathbf{G} \wr \mathbf{\Gamma_n}$. Start with X_1 as a uniform random pick from $\mathbf{G}$. Suppose that $X_1, X_2, \ldots, X_n$ have already been constructed. Take X_{n+1} to be the pair (F, X_n), where F is a $\mathbf{G}^{s^n}$-valued random variable with coordinates that are independent uniform random picks from $\mathbf{G}$ which are also independent of X_n. It follows inductively from Lemma 2.4 that X_{n+1} is a uniform random pick from $\mathbf{\Gamma_{n+1}}$.

It is immediate from Lemma 2.4 that the cycle products of (F, X_n) consist of products of disjoint collections of the independent uniformly distributed $\mathbf{G}$-valued random variables $F(j)$. The segregation of the $F(j)$ into the various cycle products is dictated by the independent $\mathbf{\Gamma_n}$-valued random variable X_n. Therefore, conditional on X_n, the cycle products of (F, X_n) form a sequence of independent, uniformly distributed $\mathbf{G}$-valued random variables.

Put $S_{01} := 1$ and $S_{0k} := 0$, $k > 1$. By Lemma 2.3, the stochastic process $((S_{n,k})_{k=1}^\infty)_{n=0}^\infty$ taking values in the collection of infinite-length integer-valued sequences is thus a Galton–Watson branching process with infinitely many types (the types labelled by $\{1, 2, 3, \ldots\}$). An individual of type k can only give birth to individuals of types $k, 2k, 3k, \ldots$. Moreover, the joint distribution of the sequence of integer-valued random variables recording the number of offspring of types $k, 2k, 3k, \ldots$ produced by an individual of type k does not depend on k and is the same as that of the sequence recording the number of cycles of lengths $1, 2, 3, \ldots$ for a uniformly chosen element of $\mathbf{G}$.

Recall our standing assumption that $\mathbf{G}$ acts transitively. It follows from this and Burnside's Lemma (see, for example, Lemma 4.1 of [Ker75]) that the number of 1-cycles (that is, fixed points) of a uniformly chosen element of $\mathbf{G}$ is a non-trivial random variable with expectation $\mu_1 = 1$. By the observations above, the process $(S_{n,1})_{n=0}^\infty$ is a critical (single-type) Galton–Watson branching process and hence this process becomes extinct almost surely. That is, if we set $\tau_1 := \inf\{n : S_{n,1} = 0\}$, then $\mathbb{P}\{\tau_1 < \infty\} = 1$ and $0 = S_{\tau_1,1} = S_{\tau_1+1,1} = \ldots$.

By the observations above and the strong Markov property, $(S_{\tau_1+n,2})_{n=0}^\infty$ is also a critical (single-type) Galton–Watson branching process (with the same offspring distribution as $(S_{n,1})_{n=0}^\infty$) and so this process also becomes extinct almost surely. Hence, if we set $\tau_2 := \inf\{n : S_{n,1} = S_{n,2} = 0\}$, then $\mathbb{P}\{\tau_2 < \infty\} = 1$ and $0 = S_{\tau_2,1} = S_{\tau_2,2} = S_{\tau_2+1,1} = S_{\tau_2+1,2} = \ldots$. Continuing in this way establishes (4.1), as required.

plain

Remark 4.1 Much of the work on eigenvalues of Haar distributed random matrices described in the Introduction is based on moment calculations. As noted in the Introduction, $\mathbb{E}[T_{n,1}] = 1$ for all n, and so a result such as Theorem 1.2 could not be proved using such methods.

5 Asymptotics for other test functions

In this section we consider the asymptotic behaviour of $\int_{\mathbb{T}} f\, d\Xi_n$ for test functions other than trigonometric polynomials. Because of (3.1), it suffices to consider functions of the form $f(z) = \sum_{k=1}^{\infty} c_k z^k$.

plain

Definition 5.1 A complex sequence $(d_k)_{k=1}^{\infty}$ is *multiplicative* if $d_{k\cdot\ell} = d_k d_\ell$. Obvious examples of multiplicative sequence are $d_k = k^\beta$ for $\beta \in \mathbb{C}$. In general, a multiplicative function is specified by assigning arbitrary values of d_p to each prime p. The value of d_k for an integer k with prime decomposition $k = p_1^{h_1} p_2^{h_2} \cdots p_m^{h_m}$ is then $d_{p_1}^{h_1} d_{p_2}^{h_2} \cdots d_{p_m}^{h_m}$.

plain

Notation 5.2 As in Section 3, let μ_k denote the expected number of k-cycles in the cycle decomposition of a permutation chosen uniformly at random from $\mathbf{G}$. Write $\mathcal{M}$ for the smallest subset of $\mathbb{N}$ that contains $\{1 \le k \le s : \mu_k > 0\}$ and is closed under multiplication.

plain

Example 5.3 For the reader's benefit, we record the expected cycle counts μ_k in some examples (see 5.16 of [Ker75]).

i) If $\mathbf{G} = \mathcal{S}_s$, the symmetric group of order $s!$ acting on a set of size s, then $\mu_k = k^{-1}$, $1 \le k \le s$.

ii) If $\mathbf{G} = \mathcal{C}_s$, the cyclic group of order s acting on a set of size s, then

$$\mu_k = \begin{cases} \Phi(k)/k, & \text{if } k|s, \\ 0, & \text{otherwise,} \end{cases}$$

where $\Phi(k) := \#\{1 \le \ell \le k : (\ell, k) = 1\}$ is the Euler function.

iii) If $\mathbf{G} = \mathcal{D}_s$, the dihedral group of symmetries of a regular s-gon, then $\mu_1 = 1$,

$$\mu_2 = \begin{cases} (s-1)/4, & \text{if } n \text{ is odd,} \\ s/4, & \text{if } n \text{ is even,} \end{cases}$$

and $\mu_k = \Phi(k)/k$, $3 \le s \le k$, $k|s$.

iv) If $\mathbf{G}$ is an arbitrary finite group of order s acting on itself via the regular representation, then $\mu_k = \omega_k/k$, $k|s$, where ω_k is the number of elements in $\mathbf{G}$ of order k.

Theorem 5.4 *Consider two sequences $(c_k)_{k=1}^\infty$ and $(d_k)_{k=1}^\infty$ that satisfy the following conditions:*

a) $(d_k)_{k=1}^\infty$ *is multiplicative,*

b) $d_k > 0$ *for all* k *such that* $\mu_k > 0$,

c) $\sum_{k=1}^\infty d_k < \infty$,

d) $(\sum_{k=1}^s k d_k \mu_k)^2 > \sum_{k=1}^s k^2 d_k^2 \mu_k$,

e) $\lim_{k\to\infty, k\in\mathcal{M}} c_k/d_k = c$ *exists.*

Then the sequence of random variables

$$(\sum_{k=1}^s k d_k \mu_k)^{-n} \int_{\mathbb{T}} \sum_{k=1}^\infty c_k z^k \, \Xi_n(dz)$$

converges in distribution as $n \to \infty$ to a random variable $cW \sum_{k=1}^\infty d_k$, where $0 < W < \infty$ almost surely.

Proof By Theorem 1.2, we may suppose that $c_k = d_k$ for all k. From equations (3.1) and (3.2) we have, in the notation of Section 4, that

$$\begin{aligned}
\int_{\mathbb{T}} f \, d\Xi_n &= \sum_{k=1}^\infty d_k T_{n,k} \\
&= \sum_{k=1}^\infty d_k \left(\sum_{\ell | k} \ell S_{n,\ell} \right) \\
&= \sum_{\ell=1}^\infty \ell \left(\sum_{j=1}^\infty d_{j\cdot\ell} \right) S_{n,\ell} \\
&= \left(\sum_{j=1}^\infty d_j \right) \left(\sum_{\ell=1}^\infty \ell d_\ell S_{n,\ell} \right).
\end{aligned}$$

Setting $\delta := \sum_{j=1}^s j d_j \mu_j$ and $(W_n)_{n=0}^\infty := (\delta^{-n} \sum_{k=1}^\infty k d_k S_{n,k})_{n=0}^\infty$, it thus suffices to establish that W_n converges in distribution as $n \to \infty$ to a random variable W with $\mathbb{P}\{0 < W < \infty\} = 1$.

Construct $X_1, X_2, \ldots$ in the manner described in Section 4, so that $((S_{n,k})_{k=1}^\infty)_{n=0}^\infty$ is an infinitely–many–types Galton–Watson branching process. Let $\mathcal{F}_n := \sigma\{X_1, X_2, \ldots, X_n\}$ and observe that

$$\begin{aligned}
\mathbb{E}\left[\sum_{k=1}^\infty k d_k S_{n+1,k} \,\middle|\, \mathcal{F}_n\right] &= \sum_{k=1}^\infty k d_k \left(\sum_{\ell | k} S_{n,\ell}\mu_{k/\ell}\right) \\
&= \sum_{\ell=1}^\infty \left(\sum_{j=1}^s j \cdot \ell d_{j\cdot\ell}\mu_j\right) S_{n,\ell} \\
&= \left(\sum_{j=1}^s j d_j \mu_j\right)\left(\sum_{\ell=1}^\infty \ell d_\ell S_{n,\ell}\right).
\end{aligned}$$

Thus, $(W_n)_{n=0}^\infty$ is a nonnegative martingale with respect to the filtration $(\mathcal{F}_n)_{n=0}^\infty$, and hence W_n converges almost surely as $n \to \infty$ to an almost surely finite nonnegative random variable W.

We will next show that $\mathbb{E}[W] = 1$ by showing that the martingale $(W_n)_{n=0}^\infty$ is bounded in $\mathcal{L}^2(\mathbb{P})$ (and hence converges in $\mathcal{L}^2(\mathbb{P})$ as well as almost surely). By orthogonality of martingale increments,

$$\mathbb{E}[W_{n+1}^2] = \mathbb{E}[(W_{n+1} - W_n)^2] + \mathbb{E}[W_n^2].$$

Let $\sigma_{j',j''}$ denote the covariance between the number of j'-cycles and the number of j''-cycles in a uniform random pick from $\mathbf{G}$. By the branching process property,

$$\begin{aligned}
\mathbb{E}[(W_{n+1} - W_n)^2 \,\big|\, \mathcal{F}_n] &= \delta^{-2(n+1)} \sum_{\ell=1}^\infty S_{n,\ell} \sum_{j',j''} \ell \cdot j' d_{\ell\cdot j'}\, \ell \cdot j'' d_{\ell\cdot j''}\, \sigma_{j',j''} \\
&= \delta^{-2(n+1)} \left(\sum_{\ell=1}^\infty \ell^2 d_\ell^2 S_{n,\ell}\right)\left(\sum_{j',j''} j' d_{j'} j'' d_{j''} \sigma_{j',j''}\right).
\end{aligned}$$

Note that the sequence $(\ell^2 d_\ell^2)_{\ell=1}^\infty$ is multiplicative. Thus, setting $\varepsilon := \sum_{j=1}^s j^2 d_j^2 \mu_j$, the sequence $(\varepsilon^{-n} \sum_{k=1}^\infty k^2 d_k^2 S_{n,k})_{n=0}^\infty$ is a martingale by the same argument that established $(W_n)_{n=0}^\infty$ was a martingale. Consequently,

$$\mathbb{E}[(W_{n+1} - W_n)^2] = \delta^{-2(n+1)} \varepsilon^n \sum_{j',j''} j' d_{j'}\, j'' d_{j''}\, \sigma_{j',j''}.$$

By assumption, $\delta^2 > \varepsilon$, and hence $\sup_n \mathbb{E}[W_n^2] < \infty$, as required.

For a partition $a = (1^{a_1}, 2^{a_2}, \ldots, s^{a_s})$ of s (that is, a has a_1 parts of size 1, a_2 parts of size 2, *et cetera* and, in particular, $\sum_i i a_i = s$) let $p(a_1, a_2, \ldots, a_s)$ denote the probability that a uniformly chosen element of $\mathbf{G}$ has a_1 1-cycles, a_2 2-cycles *et cetera*. Write

$$g(u_1, u_2, \ldots, u_s) := \sum_{a \vdash s} p(a_1, a_2, \ldots, a_s) \prod_{i=1}^s u_i^{a_i}$$

for the multivariate probability generating function corresponding to the probability distribution p (thus g is just the cycle index polynomial of the group $\mathbf{G}$ - see 5.14 of [Ker75]).

Set $\varphi_n(x) := \mathbb{E}[\exp(-xW_n)]$ and $\varphi(x) := \mathbb{E}[\exp(-xW)]$, $x \geq 0$. Conditioning on $\mathcal{F}_1$ gives

$$\varphi_{n+1}(x) = g(\varphi_n(1d_1x/\delta), \varphi_n(2d_2x/\delta), \ldots, \varphi_n(sd_sx/\delta)),$$

and hence

$$\varphi(x) = g(\varphi(1d_1x/\delta), \varphi(2d_2x/\delta), \ldots, \varphi(sd_sx/\delta)).$$

Thus, from assumption (b),

$$\begin{aligned} \rho &:= \mathbb{P}\{W = 0\} \\ &= \lim_{x\to\infty} \varphi(x) \\ &= h(\rho), \end{aligned} \tag{5.1}$$

where $h(u) := g(u, \ldots, u)$ is the probability generating function of the total number of cycles in a random uniform pick from $\mathbf{G}$. The equation (5.1) has two solutions in the interval $[0, 1]$: namely, 1 and the probability of eventual extinction for a (single-type) Galton–Watson branching process with the distribution of the total number of cycles as its offspring distribution. Because $\mathbb{E}[W] = 1$, ρ cannot be 1. The other root of (5.1) is clearly 0, because the total number of cycles is always at least 1.

□

plain

Remark 5.5 Suppose that $(d_k)_{k=1}^\infty$ is an arbitrary positive multiplicative sequence. Note that $d_1 = 1$ (by the multiplicative assumption), $\mu_1 = 1$ (by Burnside's Lemma and the assumption that $\mathbf{G}$ acts transitively – see Section 4), and $\mu_k > 0$ for some $k \geq 2$ (again by transitivity). Thus $\sum_{k=1}^s kd_k\mu_k > 1$ and $(\sum_{k=1}^s kd_k\mu_k)^2 > \sum_{k=1}^s kd_k\mu_k$. For any group $\mathbf{G}$ the condition (d) of Theorem 5.4 is therefore implied by the condition $kd_k \leq 1$ for all k.

In light of Remark 5.5, the following result is immediate from Theorem 5.4.

Corollary 5.6 *Suppose that $(c_k)_{k=1}^\infty$ is a sequence such that for some $\alpha < -1$ $\lim_{k\to\infty} c_k/k^\alpha = c$ exists. Then the sequence of random variables*

$$(\sum_{k=1}^s k^{\alpha+1}\mu_k)^{-n} \int_{\mathbb{T}} \sum_{k=1}^\infty c_k z^k \, \Xi_n(dz)$$

converges in distribution as $n \to \infty$ to a random variable $cW \sum_{k=1}^\infty k^\alpha$, where $0 < W < \infty$ almost surely.

plain

Remark 5.7 Theorem 5.4 was proved under the hypothesis (b) that $d_k > 0$ for all $k \in \mathcal{M}$. If this is weakened to the hypothesis that $d_k \geq 0$ for all $k \in \mathcal{M}$, then a similar result holds. Hypothesis (e) needs to be modified to an assumption that $\lim_{k\to\infty, d_k>0} c_k/d_k = c$ exists and $d_k = 0$ implies $c_k = 0$ for all k sufficiently large. The conclusion then becomes that the stated limit holds with $0 \leq W < \infty$ almost surely. The probability $\mathbb{P}\{W = 0\}$ is the probability of eventual extinction for a Galton-Watson branching process with offspring distribution the total number of cycles in a random uniform pick from $\mathbf{G}$ having lengths in the set $\{k : d_k > 0\}$.

Acknowledgement: We thank Persi Diaconis and Dan Rockmore for helpful conversations and an anonymous referee for several helpful suggestions.

References

[AD02] M. Abért and P. Diaconis. One–two–tree(s) and Sylow subgroups of $\mathcal{S}_n$. Technical report, Department of Mathematics, Stanford University, 2002.

[AV02] M. Abért and B. Virág. Groups acting on regular trees: probability and Hausdorff dimension. Technical report, Department of Mathematics, M.I.T., 2002.

[BOERT96] Hyman Bass, Maria Victoria Otero-Espinar, Daniel Rockmore, and Charles Tresser. *Cyclic renormalization and automorphism groups of rooted trees.* Springer-Verlag, Berlin, 1996.

[BPRS83] R. A. Bailey, Cheryl E. Praeger, C. A. Rowley, and T. P. Speed. Generalized wreath products of permutation groups. *Proc. London Math. Soc. (3)*, 47(1):69–82, 1983.

[DE01] Persi Diaconis and Steven N. Evans. Linear functionals of eigenvalues of random matrices. *Trans. Amer. Math. Soc.*, 353(7):2615–2633 (electronic), 2001.

[DS94] P. Diaconis and M. Shahshahani. On the eigenvalues of random matrices. *J. Appl. Probab.*, 31A:49–62, 1994.

[DS95] Knut Dale and Ivar Skau. The (generalized) secretary's packet problem and the Bell numbers. *Discrete Math.*, 137(1-3):357–360, 1995.

[Dyu99a] A. Dyubina. Characteristics of random walks on the wreath products of groups. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 256(Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 3):31–37, 264, 1999.

[Dyu99b] A. G. Dyubina. An example of the rate of departure to infinity for a random walk on a group. *Uspekhi Mat. Nauk*, 54(5(329)):159–160, 1999.

[FS01] James Allen Fill and Clyde H. Schoolfield, Jr. Mixing times for Markov chains on wreath products and related homogeneous spaces. *Electron. J. Probab.*, 6:no. 11, 22 pp. (electronic), 2001.

[HKO01] C. P. Hughes, J. P. Keating, and Neil O'Connell. On the characteristic polynomial of a random unitary matrix. *Comm. Math. Phys.*, 220(2):429–451, 2001.

[HKOS00] B. M. Hambly, P. Keevash, N. O'Connell, and D. Stark. The characteristic polynomial of a random permutation matrix. *Stochastic Process. Appl.*, 90(2):335–346, 2000.

[JK81] Gordon James and Adalbert Kerber. *The representation theory of the symmetric group.* Addison-Wesley Publishing Co., Reading, Mass., 1981. With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson.

[Joh97] K. Johansson. On random matrices from the compact classical groups. *Ann. of Math. (2)*, 145:519–545, 1997.

[Ker71] Adalbert Kerber. *Representations of permutation groups. I.* Springer-Verlag, Berlin, 1971. Lecture Notes in Mathematics, Vol. 240.

[Ker75] Adalbert Kerber. *Representations of permutation groups. II.* Springer-Verlag, Berlin, 1975. Lecture Notes in Mathematics, Vol. 495.

[KS00a] J. P. Keating and N. C. Snaith. Random matrix theory and L-functions at $s = 1/2$. *Comm. Math. Phys.*, 214(1):91–110, 2000.

[KS00b] J. P. Keating and N. C. Snaith. Random matrix theory and $\zeta(1/2 + it)$. *Comm. Math. Phys.*, 214(1):57–89, 2000.

[KV83] V. A. Kaĭmanovich and A. M. Vershik. Random walks on discrete groups: boundary and entropy. *Ann. Probab.*, 11(3):457–490, 1983.

[LH63] H.C. Longuet-Higgins. The symmetry groups of non-rigid molecules. *Molecular Physics*, 6:445–460, 1963.

[LPP96] Russell Lyons, Robin Pemantle, and Yuval Peres. Random walks on the lamplighter group. *Ann. Probab.*, 24(4):1993–2006, 1996.

[Meh91] Madan Lal Mehta. *Random matrices*. Academic Press Inc., Boston, MA, second edition, 1991.

[PS83a] P. P. Pálfy and M. Szalay. The distribution of the character degrees of the symmetric p-groups. *Acta Math. Hungar.*, 41(1-2):137–150, 1983.

[PS83b] P. P. Pálfy and M. Szalay. On a problem of P. Turán concerning Sylow subgroups. In *Studies in pure mathematics*, pages 531–542. Birkhäuser, Basel, 1983.

[PS89] P. P. Pálfy and M. Szalay. Further probabilistic results on the symmetric p-groups. *Acta Math. Hungar.*, 53(1-2):173–195, 1989.

[PSC99] Christophe Pittet and Laurent Saloff-Coste. Amenable groups, isoperimetric profiles and random walks. In *Geometric group theory down under (Canberra, 1996)*, pages 293–316. de Gruyter, Berlin, 1999.

[Rai97] E.M. Rains. High powers of random elements of compact Lie groups. *Probab. Theory Related Fields*, 107:219–241, 1997.

[Wie98] K.L. Wieand. *Eigenvalue distributions of random matrices in the permutation group and compact Lie groups*. PhD thesis, Harvard University, 1998.

[Wie00] Kelly Wieand. Eigenvalue distributions of random permutation matrices. *Ann. Probab.*, 28(4):1563–1587, 2000.