Graph convergence, determinantal processes and the sandpile group of random regular graphs

Doctoral Thesis

András Mészáros

Supervisor: Miklós Abért

Department of Mathematics and its Applications
Central European University, Budapest, Hungary

2021

CEU eTD Collection

CEU eTD Collection

Declaration

I, the undersigned András Mészáros, candidate for the degree of Doctor of Philosophy at the Central European University Department of Mathematics and its Applications, declare herewith that the present thesis is based on my research and only such external information as properly credited in notes and bibliography.

I declare that no unidentified and illegitimate use was made of the work of others, and no part of this thesis infringes on any person's or institution's copyright. I also declare that no part of this thesis has been submitted to any other institution of higher education for an academic degree.

Budapest, Hungary, June 2021

András Mészáros

CEU eTD Collection

CEU eTD Collection

Acknowledgements

I would like to thank my supervisor, Miklós Abért for his guidance throughout all of my PhD years.

I am grateful to Ferenc Bencs, Péter Csikvári, Russel Lyons, Samuel Mellick, Gábor Pete, László Tóth, Bálint Virág, Van Vu, Melanie Matchett Wood and the anonymous referees of my papers for the useful comments and discussions.

I would also like to thank all the speakers, organizers and participants of the Kutszem Seminar.

I am thankful to my wife and children for their constant support.

CEU eTD Collection

CEU eTD Collection

Contents

CEU eTD Collection

CEU eTD Collection

1

Introduction

The central topic of this thesis is the *local weak convergence* of sparse graphs, also known as *Benjamini-Schramm convergence*. The general problem is the following. Assume that we have a large sparse graph G and we would like to estimate the value of some graph parameter $\tau(G)$ by the following *local sampling* procedure. Fix an integer r, this will be our radius of sight. Pick a uniform random point of G that we call the root, then look at its r-neighborhood, and repeat this experiment several times. Based on this data, how well can we guess the value $\tau(G)$? What are the parameters $\tau(G)$ that can be estimated this way?

By picking the root of the graph uniformly at random, we turn it to a random rooted graph, that is, a probability measure on the space of rooted graphs. Local weak convergence means weak convergence of these measures. The above testability question translates to the following: what graph parameters are continuous with respect to local weak convergence?

Random graphs provide us natural examples of Benjamini-Schramm convergent graph sequences. *Random d-regular graphs* with a growing number of vertices will converge to a d-regular tree. *Erdős-Rényi graphs* on n vertices and edge probabilities $\frac{c}{n}$ – as n goes to infinity – will converge to a Galton-Watson tree with Poisson offspring distribution. This gives rise to the following particular case of the questions above. What properties of random graphs are already determined by their local structure? Which graph parameters have the property that a sequence of random d-regular graphs can not be distinguished from any other given (essentially) large girth d-regular sequence using that parameter? For example the normalized size of the maximum independent set can be used to distinguish random d-regular graphs from bipartite large girth d-regular graphs, as it was proved by Bollobás [14]. Another special case of this question is given in the next section.

CEU eTD Collection

1 Mod p rank of the Laplacian matrices of random d-regular graphs

Given a graph G, let $A(G)$ be its *adjacency matrix*, and let $L(G)$ be its *Laplace matrix.* Given an integral matrix M and a prime p, we denote by $\dim\ker_p M$ the dimension of the kernel of the matrix M when it is considered as a matrix over the p element field. Let H_{2n} be a random d-regular graph on $2n$ vertices.[1] In Chapter 2, we prove that with probability 1, we have

$$\lim_{n\to\infty}\frac{\dim\ker_p A(H_{2n})}{2n}=0 \text{ and } \lim_{n\to\infty}\frac{\dim\ker_p L(H_{2n})}{2n}=0.$$

In fact, we know much more. It turns out that we can control the limiting distribution of $\dim\ker_p L(H_{2n})$.

Theorem 1.1. *For any $k\ge 0$, and an odd prime p, we have*

$$\lim_{n\to\infty}\mathbb{P}(\dim\ker_p L(H_{2n})=k+1)=p^{-\frac{k(k+1)}{2}}\prod_{i=k+1}^{\infty}(1-p^{-i})\prod_{i=1}^{\infty}(1-p^{-2i})^{-1}.$$

We have a similar formula for $p=2$.

One can also give formulas for the limiting distribution of $\dim\ker_p A(H_{2n})$*, but it is a bit more complicated, because we need a case splitting depending on whether d is divisible by p or not.*

Actually, we prove even more, as we will determine the limiting distribution of the p-Sylow subgroup of the *sandpile group* of H_n, which is defined as the *cokernel of the reduced Laplacian.* The limiting distribution is given by a modified version of the *Cohen-Lenstra heuristics* [18]. This limiting distribution is *universal* in the sense that it does not depend on the choice of d.

The original Cohen-Lenstra distribution is a distribution on the set of finite abelian p-groups where the probability of a group P is proportional to $|\mathrm{Aut}(P)|^{-1}$. It was introduced by Cohen and Lenstra [20] in a conjecture on the distribution of class groups of quadratic number fields. Although this conjecture is still open, several other random groups are known to follow the Cohen-Lenstra distribution. For example, the cokernel of a Haar-uniform square matrix over the p-adic integers has this limiting distribution [27]. In fact this is true even in a more general setting. It is enough to assume that the entries of the matrices are independent and they are not degenerate in a certain sense. This was proved by Wood [60]. Her paper also contains similar results for non-square matrices. Clancy et al [19, 18] introduced a modified version of the Cohen-Lenstra distribution to describe the limiting distribution of the cokernel of a Haar-uniform *symmetric* matrix over the p-adic integers . Later, Wood [58] proved that the sandpile group dense Erdős-Rényi graphs also follows this modified Cohen-Lenstra distribution. Somewhat surprisingly, we have the same limiting distribution even for random d-regular graphs as we will show.

These results also have the following corollary which settles an open question of Frieze [28] and Vu [57].

[1] To be more specific, we use the following model: we take the union of d independent uniform random perfect matchings.

CEU eTD Collection

Theorem 1.2.

$$\lim_{n\to\infty} \mathbb{P}(A(H_{2n}) \text{ is invertible over } \mathbb{R}) = 1.$$

Note that Theorem 1.2 was independently proved by Huang [34, 33].

If we consider an arbitrary large girth d-regular sequence (G_n) instead of random d-regular graphs, then $\dim\ker_p A(H_{2n})$ is less understood. In particular, the following question is still open.

Question 1.3. *Let (G_n) be a large girth d-regular sequence. Is it true that*

$$\lim_{n\to\infty} \frac{\dim\ker_p A(G_n)}{|V(G_n)|} = 0?$$

Note that if we ask the same question over $\mathbb{R}$, then we have an affirmative answer. In fact, over $\mathbb{R}$, the normalized dimension of the kernel of the adjacency matrix is a Benjamini-Schramm continuous graph parameter [1]. The proof uses *spectral methods* which are not available over finite fields.

Chapter 2 is based on the paper [48].

2 Limiting entropy of determinantal processes

Given a finite connected graph G, let $\tau(G)$ be the number of spanning trees of G. The (normalized) *tree entropy* of G is defined as $h(G) = \frac{\log\tau(G)}{|V(G)|}$. McKay [45] proved that if (G_n) is a sequence of random d-regular graphs, then

$$\lim_{n\to\infty} h(G_n) = \log \frac{(d-1)^{d-1}}{(d^2-2d)^{(d/2)-1}}.$$

Lyons proved that this is true for any essentially large girth d-regular graph sequence. In fact, he proved the much stronger statement that that $h(G)$ is Benjamini-Schramm continuous graph parameter [41].

The uniform measure on the spanning trees of a finite connected graph is one of the most important examples of discrete *determinantal measures*. With any orthogonal projection matrix P, we can associate a probability measure η_p on the subsets of its columns in a certain way that we do not specify now. We call η_P the determinatal measure corresponding to P.

In Chapter 3, we extend Lyons's tree entropy theorem to general determinantal measures as follows. Let $P_1, P_2, \dots$ be a sequence of orthogonal projection matrices. Assume that rows and columns of P_n are both indexed with the finite set V_n. Let G_n be a bounded degree graph on the vertex set V_n.

CEU eTD Collection

Theorem 2.1. *Assume that the sequence of pairs (G_n, P_n) is Benjamini-Schramm convergent and tight. Then*

$$\lim_{n\to\infty} \frac{H(\eta_{P_n})}{|V_n|}$$

exists. Here $H(\eta_{P_n})$ is the Shannon entropy of the measure η_{P_n}.

Here the convergence of the pairs (G_n, P_n) is defined along the lines of the convergence of graphs. Tightness is a technical condition that makes sure that large entries of P_n correspond to pairs of vertices that are close to each other in the graph G_n.

It is not difficult to see that this indeed implies Lyons's tree entropy theorem.

Note that finite approximations of determinantal processes were also considered by Lyons and Thom [43]. Their aim was to find an invariant coupling of certain determinatal processes.

As a byproduct of Theorem 2.1, we also show that the sofic entropy of an invariant determinantal measure does not depend on the chosen sofic approximation. Sofic entropy was first defined by Bowen [16], and it is an invariant for probability measure preserving actions of sofic groups. A group is sofic if it has a Cayley-graph which the Benjamini-Schramm limit of a sequence of finite graphs. The sofic entropy is defined with the help of this finite approximating sequence. In general, it is not known whether the sofic entropy depends on the chosen sofic approximation or not. We prove that for a determinantal measure it does not depend on the chosen approximation.

Another application concerns *matchings of trees.* If we take a finite tree, and consider the vertices that are not covered by a uniform random maximum size matching, then this random subset of the vertices is determinantal. With some additional work, one can combine this observation with Theorem 2.1 to obtain the following theorem.

Theorem 2.2. *Given a finite graph G, let $\mathrm{mm}(G)$ be the number of maximum size matchings of G. Let $G_1, G_2, \dots$ be a Benjamini-Schramm convergent sequence of finite trees with maximum degree at most D. Then*

$$\lim_{n\to\infty} \frac{\log \mathrm{mm}(G_n)}{|V(G_n)|}$$

exists.

Note that without the assumption that the graphs G_i are trees, the limit in Theorem 2.2 might not exist, even if the sequence converges to an amenable graph like $\mathbb{Z}^2$. We can see this by comparing the results of [37, 56, 23]. However, if we restrict our attention to vertex transitive bipartite graphs, the limit above exists for convergent graph sequences, as it was proved by Csikvári [22]. Csikvári's proof based on spectral methods and the notion of the matching measure. In fact, spectral methods allows us to prove that several matching related parameters are Benjamini-Schramm continuous [2], for example: the proportion of vertices that are left uncovered by a maximum size matching of G, the normalized logarithm of the total number of matchings, etc.

Chapter 3 is based on the papers [46, 47].

CEU eTD Collection

2

The distribution of sandpile groups of random regular graphs

We study the distribution of the sandpile group of random d-regular graphs. For the directed model, we prove that it follows the Cohen-Lenstra heuristics, that is, the limiting probability that the p-Sylow subgroup of the sandpile group is a given p-group P, is proportional to $|\operatorname{Aut}(P)|^{-1}$. For finitely many primes, these events get independent in the limit. Similar results hold for undirected random regular graphs, where for odd primes the limiting distributions are the ones given by Clancy, Leake and Payne.

This answers an open question of Frieze and Vu whether the adjacency matrix of a random regular graph is invertible with high probability. Note that for directed graphs this was recently proved by Huang. It also gives an alternate proof of a theorem of Backhausz and Szegedy.

1 Introduction

CEU eTD Collection

We start by defining our random graph models. Let $d \geq 3$. The graph of a permutation π consists of the directed edges $i\pi(i)$. The *random directed graph* D_n is defined by taking the union of the graphs of d independent uniform random permutations of $\{1, 2, \dots, n\}$. Thus, the adjacency matrix A_n of D_n is just obtained as $A_n = P_1 + P_2 + \dots + P_d$, where $P_1, P_2, \dots, P_d$ are independent uniform random $n \times n$ permutation matrices.

For the undirected model, assume that n is even. The *random d-regular graph* H_n is obtained by taking the union of d independent uniform random perfect matchings. The adjacency matrix of H_n is denoted by C_n.

The reduced Laplacian Δ_n of D_n is obtained from $A_n - dI$ by deleting its last row and last column. The subgroup of $\mathbb{Z}^{n-1}$ generated by the rows of Δ_n is denoted by $\operatorname{RowSpace}(\Delta_n)$. The group $\Gamma_n = \mathbb{Z}^{n-1}/\operatorname{RowSpace}(\Delta_n)$ is called the *sandpile group* of D_n. If D_n is strongly connected (which happens with high probability as $n \to \infty$), then Γ_n is a finite abelian group of order $|\det \Delta_n|$. Note that from the Matrix-Tree Theorem, $|\det \Delta_n|$ is the number of spanning trees in D_n oriented towards the vertex n. For general directed graphs the sandpile group may depend on the choice of deleted row and column, but not in our case, because D_n is Eulerian. The sandpile group of H_n is defined the same way. Assuming that H_n is connected, the order of the sandpile group is equal to the number of spanning trees in H_n.

Our main results are the following.

Theorem 1.1. *Let $p_1, p_2, \dots, p_s$ be distinct primes. Let Γ_n be the sandpile group of D_n. Let $\Gamma_{n,i}$ be the p_i-Sylow subgroup of Γ_n. For $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Then*

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i\right) = \prod_{i=1}^{s}\left(|\operatorname{Aut}(G_i)|^{-1}\prod_{j=1}^{\infty}(1-p_i^{-j})\right). \tag{1.1}$$

Theorem 1.2. *Let Γ_n be the sandpile group of H_n. Again let $\Gamma_{n,i}$ be the p_i-Sylow subgroup of Γ_n, and for $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Assuming that d is odd, we have*

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i\right) = \prod_{i=1}^{s}\left(\frac{|\{\phi : G_i \times G_i \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G_i||\operatorname{Aut}(G_i)|}\prod_{j=0}^{\infty}(1-p_i^{-2j-1})\right). \tag{1.2}$$

Assume that d is even and $p_1 = 2$. Then the 2-Sylow subgroup of Γ_n has odd rank[1]*. Furthermore, if we assume that G_1 has odd rank, then*

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i\right) = 2^{\operatorname{Rank}(G_1)}\prod_{i=1}^{s}\left(\frac{|\{\phi : G_i \times G_i \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G_i||\operatorname{Aut}(G_i)|}\prod_{j=0}^{\infty}(1-p_i^{-2j-1})\right).$$

The distribution appearing in (1.1) is the one that appears in the Cohen-Lenstra heuristics. It was introduced by Cohen and Lenstra [20] in a conjecture on the distribution of class groups of quadratic number fields. The distribution appearing in (1.2) is a modified version of the distribution from the Cohen-Lenstra heuristics that was introduced by Clancy et al [19, 18].[2]

A recent breakthrough paper of Wood [58] shows that the sandpile group of dense Erdős-Rényi random graphs satisfies the latter heuristic. That is, Theorem 1.2 says that in terms of the sandpile group, random 3-regular graphs exhibit the same level of randomness as dense Erdős-Rényi graphs. The conceptual explanation is that the random matrices coming from both models mix the space extremely well, as we will see in Theorem 1.6 for our model.

[1]The rank of a group is the minimum number of generators.
[2]See the paragraph after Equation (1.3) for the definition of perfect parings.

CEU eTD Collection

We can gain information about the sandpile group by counting the surjective homomorphisms from it to a fixed finite abelian group V. For a random abelian group Γ and a fixed finite abelian group V, we call the expectation $\mathbb{E}|\operatorname{Sur}(\Gamma, V)|$ the *surjective V-moment* of Γ. Our next theorems determine the limits of the surjective moments of the sandpile groups for our random graph models. The convergence of these moments then implies Theorem 1.1 and Theorem 1.2, using the work of Wood [58].

Theorem 1.3. *Let Γ_n be the sandpile group of D_n. For any finite abelian group V, we have*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\Gamma_n, V)| = 1.$$

Recall that the exterior power $\wedge^2 V$ is defined to be the quotient of $V \otimes V$ by the subgroup generated by elements of the form $v \otimes v$.

Theorem 1.4. *Let Γ_n be the sandpile group of H_n. Let V be a finite abelian group. If d is odd, then*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\Gamma_n, V)| = |\wedge^2 V|,$$

if d is even, then

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\Gamma_n, V)| = 2^{\operatorname{Rank}_2(V)}|\wedge^2 V|,$$

where $\operatorname{Rank}_2(V)$ is the rank of the 2-Sylow subgroup of V.

These theorems are proved by using the fact that, when they are acting on V^n, the adjacency matrices A_n and C_n both exhibit strong mixing properties, described as follows: For $q = (q_1, q_2, \dots, q_n) \in V^n$, the minimal coset in V containing $q_1, q_2, \dots, q_n$ is denoted by MinC_q. Note that MinC_q is the coset $q_n + V_0$ where V_0 is the subgroup of V generated by $q_1 - q_n, q_2 - q_n, \dots, q_{n-1} - q_n$. The sum of the components of q is denoted by $s(q) = \sum_{i=1}^n q_i$, and we define

$$R(q,d) = \{r \in (d \cdot \operatorname{MinC}_q)^n \quad | \quad s(r) = ds(q)\}.$$[3]

It is straightforward to check that $A_n q \in R(q,d)$. Let $U_{q,d}$ be a uniform random element of $R(q,d)$. Given two random variables X and Y taking values of the finite set $\mathcal{R}$, we define $d_\infty(X,Y) = \max_{r\in\mathcal{R}} |\mathbb{P}(X = r) - \mathbb{P}(Y = r)|$. We prove that the distribution of $A_n q$ is close to that of $U_{q,d}$ in the following sense.

Theorem 1.5. *For $d \geq 3$, we have*

$$\lim_{n\to\infty} \sum_{q \in V^n} d_\infty(A_n q, U_{q,d}) = 0.$$

We have a similar theorem for C_n. For $q, w \in V^n$, we define

$$< q \otimes w >= \sum_{i=1}^n q_i \otimes w_i.$$

[3]By definition $d \cdot \operatorname{MinC}_q = \{g_1 + g_2 + \cdots + g_d | g_1, g_2, \dots, g_d \in \operatorname{MinC}_q\}$.

CEU eTD Collection

Furthermore, let $I_2 = I_2(V)$ be the subgroup of $V \otimes V$ generated by the set $\{a \otimes b + b \otimes a| \quad a, b \in V\}$. Let $\mathrm{Rank}_2(V)$ be the rank of the 2-Sylow of V, and let $I = I(V)$ be the subgroup of $V \otimes V$ generated by all elements of the form $a \otimes a$ for $a \in V$. Note that I_2 is a subgroup of I of index $2^{\mathrm{Rank}_2(V)}$. Since the random matrix C_n is symmetric and the diagonal entries are all equal to 0, for any $q \in V^n$, we have $< q \otimes C_n q > \in I_2$. Let us define $R^S(q, d)$ as

$$R^S(q, d) = \{r \in (d \cdot \mathrm{MinC}_q)^n \quad | \quad s(r) = ds(q) \text{ and } < q \otimes r > \in I_2\}.$$

It is clear from what is written above that $C_n q \in R^S(q, d)$. Similarly as before, let $U^S_{q,d}$ be a uniform random element of $R^S(q, d)$. Then, we have

Theorem 1.6. *For $d \geq 3$, we have*

$$\lim_{n \to \infty} \sum_{q \in V^n} d_\infty(C_n q, U^S_{q,d}) = 0.$$

Note that the limits in Theorems 1.3, 1.4, 1.5 and 1.6 are uniform in d. See Section 6 for further discussion. However, until Section 6, we never claim any uniformity over the choice of V and d.

Recently, Huang [34] considered a slightly different random d-regular directed graph model on n vertices, the configuration model introduced by Bollobás [13]. Let F_n be the adjacency matrix of this random graph. Huang proves that for a prime p such that $\gcd(p, d) = 1$, we have

$$\mathbb{E}|\{0 \neq x \in \mathbb{F}_p^n| \quad F_n x = 0\}| = 1 + o(1),$$

as n goes to infinity, where F_n is considered as a matrix over $\mathbb{F}_p$. Then he combines this with Markov's inequality to obtain that

$$\mathbb{P}(F_n \text{ is singular in } \mathbb{F}_p) \leq \frac{1 + o(1)}{p - 1}.$$

Consequently, as a random matrix in $\mathbb{R}$,

$$\mathbb{P}(F_n \text{ is singular in } \mathbb{R}) = o(1).$$

This solves an open problem of Frieze [28] and Vu [57] for random regular bipartite graphs.

Using Theorem 1.6, we can answer this question in its original form.

Theorem 1.7. *For the adjacency matrix C_n of H_n, we have*

$$\mathbb{P}(C_n \textit{ is singular in } \mathbb{R}) = o(1).$$

Indeed, from Theorem 1.6 with the choice of $V = \mathbb{F}_p$, it is straightforward to prove that for an odd prime p such that $\gcd(p, d) = 1$, we have

CEU eTD Collection

$$\mathbb{E}|\{0 \neq x \in \mathbb{F}_p^n | \quad C_n x = 0\}| = 1 + o(1).$$

Therefore, the statement follows as above.

There are contiguity results [35, 49] which allow us to pass from one random d-regular graph model to another. In particular, Theorem 1.7 also true for uniform random d-regular graphs with even number of vertices. See also the work of Nguyen and Wood [50]. After the first version of this paper appeared online, Huang [33] also extended his results to the undirected configuration model, giving credit to this paper.

Theorem 1.2 describes the local behavior of the sandpile group Γ_n of H_n. Now we try to gain some global information on these groups. The next statement gives the asymptotic order of Γ_n. This was first proved by McKay [45], but it also follows from the more general theorem of Lyons [41]. Let us choose $H_2, H_4, \dots$ independently. The torsion part of Γ_n is denoted by $\mathrm{tors}(\Gamma_n)$.

Theorem 1.8 (McKay, Lyons)**.** *With probability* 1*, we have*[4]

$$\lim_{n\to\infty} \frac{\log|\mathrm{tors}(\Gamma_n)|}{n} = \log \frac{(d-1)^{d-1}}{[d(d-2)]^{d/2-1}}.$$

Theorem 1.4 leads to the following statement on the rank of Γ_n.

Theorem 1.9. *With probability* 1*, we have*

$$\lim_{n\to\infty} \frac{\mathrm{Rank}(\Gamma_n)}{n} = 0.$$

Observe that $\mathrm{Rank}(\mathrm{tors}(\Gamma_n)) = \max_{p \text{ is a prime}} \mathrm{Rank}_p(\mathrm{tors}(\Gamma_n))$, where $\mathrm{Rank}_p(\mathrm{tors}(\Gamma_n))$ is the rank of the p-Sylow subgroup of $\mathrm{tors}(\Gamma_n)$. Thus, this theorem suggests that many primes should contribute to reach the growth described in Theorem 1.8, but we do not have a definite result in this direction.

A conjecture of Abért and Szegedy states that if $G_1, G_2, \dots$ is a Benjamini-Schramm convergent sequence of finite graphs, then for any prime p the limit

$$\lim_{n\to\infty} \frac{\text{co-rank}_p\, G_n}{|V(G_n)|}$$

exists, here $\text{co-rank}_p\, G_n = \dim\ker \mathrm{Adj}(G_n)$, where $\mathrm{Adj}(G_n)$ is the adjacency matrix of G_n considered as a matrix over the finite field $\mathbb{F}_p$. One of the most common examples of a Benjamini-Scramm convergent sequence is the sequence of random d-regular graphs H_n. This means that if we choose H_n independently, then with probability 1, the sequence converges. Following along the lines of the proof of Theorem 1.9, one can prove that

$$\lim_{n\to\infty} \frac{\max_{p \text{ is a prime}} \text{co-rank}_p(H_n)}{n} = 0$$

[4]If H_n is connected, which happens with high probability, then $\mathrm{tors}(\Gamma_n) = \Gamma_n$. The only reason for using $\mathrm{tors}(\Gamma_n)$ is to handle disconnected graphs too.

CEU eTD Collection

with probability 1, which settles this special case of the conjecture, and we even get a uniform convergence in p. Note that this has been proved by Backhausz and Szegedy [7] using a different method.

Theorem 1.1 follows from Theorem 1.3 using the results of Wood [58] on the *moment problem*. The general question is the following. Given a random finite abelian p-group X, is it true that the surjective V-moments of X uniquely determine the distribution of X? Note that we can restrict our attention to the surjective V-moments, where V is a p-group, because any other moment is 0. Furthermore, is it true that if $X_1, X_2, \dots$ is a sequence of random abelian p-groups such that the surjective V-moments of X_n converge to those of X, then the distribution of X_n converge weakly to the distribution of X? Ellenberg, Venkatesh and Westerland [24] proved that the answer is affirmative for both questions in the special case when each surjective moment of X is 1. In this case X has the distribution from the Cohen-Lenstra heuristic. Later, it was proved by Wood [58] that the answer is yes for both questions if the moments do not grow too fast, namely, if $\mathbb{E}|\operatorname{Sur}(X,V)| \le |\wedge^2 V|$ for any finite abelian p-group V. The proof generalizes the ideas of Heath-Brown [30]. In [58] this is stated only in the special case, when the limiting surjective V-moments of X are exactly $|\wedge^2 V|$, but in a later paper of Wood [60] it is stated in its full generality above. In fact, Wood proved this theorem in a slightly more general setting. Instead of abelian p-groups, one can consider groups which are direct sums of finite abelian p_i-groups for a fixed finite set of primes. See Section 5 for details. Note that for even d, the moments of the sandpile groups of H_n are larger than the bounds above. But using the extra information that the 2-Sylow subgroups have odd rank in this case, we can modify the arguments of Wood to obtain the convergence of probabilities. See Section 8.

Now we discuss the Cohen-Lenstra heuristic in terms of random matrices over the p-adic integers. Let $\mathbb{Z}_p$ be the ring of p-adic integers. Given an $n \times m$ matrix M over $\mathbb{Z}_p$, we define $\operatorname{RowSpace}(M) = \{xM | x \in \mathbb{Z}_p^n\}$. The *cokernel* of M is defined as $\operatorname{cok}(M) = \mathbb{Z}_p^m / \operatorname{RowSpace}(M)$. Freidman and Washington [27] proved that if M_n is an $n \times n$ random matrix over $\mathbb{Z}_p$, with respect to the Haar-measure, then $\operatorname{cok}(M_n)$ asymptotically follows the distribution from the Cohen-Lenstra heuristic, that is, for any finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(M_n) \simeq G) = |\operatorname{Aut}(G)|^{-1} \prod_{j=1}^{\infty} (1 - p^{-j}).$$

In fact this is true even in a more general setting. It is enough to assume that the entries of M_n are independent and they are not degenerate in a certain sense. This was proved by Wood [60]. Her paper also contains similar results for non-square matrices.

Bhargava, Kane, Lenstra, Poonen and Rains [11] proved that the cokernels of Haar-uniform skew-symmetric random matrices over $\mathbb{Z}_p$ are asymptotically distributed according to Delaunay's heuristics. The following somewhat analogous result was obtained by Clancy, Leake, Kaplan, Payne and Wood [18]. Let M_n be a Haar-uniform symmetric random matrix over $\mathbb{Z}_p$. Then, for

CEU eTD Collection

any finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(M_n) \simeq G) = \frac{|\{\phi : G \times G \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G||\operatorname{Aut}(G)|} \prod_{j=0}^{\infty}(1 - p^{-2j-1}). \tag{1.3}$$

This is exactly the distribution appearing in Theorem 1.2. Note that this is not the original formula given in [18], but it can be easily deduced from it, see [58]. Here, a map $\phi : G \times G \to \mathbb{C}^*$ is called a symmetric, bilinear, perfect pairing if (i) $\phi(x,y) = \phi(y,x)$, (ii) $\phi(x, y+z) = \phi(x,y)\phi(x,z)$, and (iii) for $\phi_x(y) = \phi(x,y)$, we have $\phi_x \equiv 1$ if and only if $x = 0$. We can give a more explicit formula for the limiting probability above by using the following fact from [58]. If $G = \bigoplus_i \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$ with $\lambda_1 \geq \lambda_2 \geq \cdots$ and μ is the transpose of the partition λ, then

$$\frac{|\{\phi : G \times G \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G||\operatorname{Aut}(G)|} = p^{-\sum_i \frac{\mu_i(\mu_i+1)}{2}} \prod_{i=1}^{\lambda_1} \prod_{j=1}^{\lfloor \frac{\mu_i - \mu_{i+1}}{2} \rfloor} (1 - p^{-2j})^{-1}. \tag{1.4}$$

Now we give a brief summary of results on distribution of sandpile groups. We already defined the Laplacian and the sandpile group of a d-regular graph, now we give the general definitions. We start by directed graphs. Let D be a strongly connected directed graph on the n element vertex set V. The Laplacian Δ of D is an $n \times n$ matrix, where the rows and the columns are both indexed by V, and for $i, j \in V$, we have

$$\Delta_{ij} = \begin{cases} d(i,j) & \text{for } i \neq j, \\ d(i,i) - d_{\text{out}}(i) & \text{for } i = j. \end{cases}$$

Here $d(i,j)$ is the multiplicity of the directed edge ij, $d_{\text{out}}(i)$ is the out-degree of i, that is, $d_{\text{out}}(i) = \sum_{j\in V} d(i,j)$. For $s \in V$, the reduced Laplacian Δ_s is obtained from Δ by deleting the row and column corresponding to s. The group $\Gamma_s = \mathbb{Z}^{n-1}/\operatorname{RowSpace}(\Delta_s)$ is called the *sandpile group at vertex s*. The order of Γ_s is the number of spanning trees in D oriented towards s. Let us define
$\mathbb{Z}_0^n = \{x \in \mathbb{Z}^n | \sum_{i=1}^n x_i = 0\}$. Note that every row of Δ is in $\mathbb{Z}_0^n$. Thus the following definition makes sense. The group $\Gamma = \mathbb{Z}_0^n/\operatorname{RowSpace}(\Delta)$ is called the *total sandpile group.* If D is Eulerian, then all of these definitions of sandpile groups coincide, so it is justified to speak about the sandpile group of D. In fact, the converse of the above statement about Eulerian graphs is also true, see Farrel and Levine [25].

For an undirected graph G, let D be the directed graph obtained from G by replacing each edge $\{i,j\}$ of G by the directed edges ij and ji. Then D is Eulerian. The sandpile group of G is defined as the sandpile group of D. See [36, 39, 51, 32] for more information on sandpile groups.

We already mentioned the result of Wood [58] on Erdős-Rényi random graphs. Here we give more details. For $0 \leq \varrho \leq 1$, the Erdős-Rényi random graph $G(n, \varrho)$ is a graph on the vertex set $\{1, 2, \dots, n\}$, such that for each pair of vertices, there is an edge connecting them with probability

CEU eTD Collection

ϱ independently. Let $p_1, p_2, \dots, p_s$ be distinct primes. Fix $0 < \varrho < 1$. Let Γ_n be the sandpile group of $G(n, \varrho)$. Let $\Gamma_{n,i}$ be the p_i-Sylow subgroup of Γ_n, and for $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Then

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i\right)$$
$$= \prod_{i=1}^{s}\left(\frac{|\{\phi : G_i \times G_i \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G_i||\operatorname{Aut}(G_i)|}\prod_{j=0}^{\infty}(1-p_i^{-2j-1})\right).$$

See Equation (1.4) for an even more explicit formula.

Koplewitz [38] proved the analogous result for directed graphs. For $0 \le \varrho \le 1$, the random directed graph $D(n, \varrho)$ is a graph on the vertex set $\{1, 2, \dots, n\}$, such that for each ordered pair of vertices, there is a directed edge connecting them with probability ϱ independently. Let $p_1, p_2, \dots, p_s$ be distinct primes. Fix $0 < \varrho < 1$. Let Γ_n be the total sandpile group of $D(n, \varrho)$. Let $\Gamma_{n,i}$ be the p_i-Sylow subgroup of Γ_n, and for $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Then

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i\right) = \prod_{i=1}^{s} \frac{\prod_{j=2}^{\infty}(1-p_i^{-j})}{|G||\operatorname{Aut}(G)|}.$$

Note that, unlike what we would expect knowing the undirected case, this distribution is not the same as the one given in Theorem 1.1 for the random directed d-regular graph D_n. A quick explanation is that D_n is Eulerian, while $D(n, \varrho)$ is not. Indeed, the total sandpile group is defined as $\mathbb{Z}_0^n \simeq \mathbb{Z}^{n-1}$ factored out by n relations, so for a general directed graph, we expect that it behaves like the cokernel of a random $n \times (n-1)$ matrix. However, for an Eulerian graph these n relations are linearly dependent, because their sum is zero, so we expect that the total sandpile group behaves like the cokernel of a random $(n-1) \times (n-1)$ matrix. The results above indeed support these intuitions.

The structure of the chapter

Section 2 contains the basic definitions that we need, including the notion of typical vectors. In Section 3, we investigate the distribution of $A_n q$, where q is a typical vector. The results in this section allow us to handle the contribution of the typical vectors to the sum $\sum_{q\in V^n} d_\infty(A_n^{(d)} q, U_{q,d})$ in Theorem 1.5, but we still need to control the contribution of the non-typical vectors. This is done in Section 4. The connection between the mixing property of the adjacency matrix and the sandpile group is explained in Section 5. In Section 6, we prove that several results hold uniformly in d. Most of the chapter deals with the directed random graph model, the necessary modifications for the undirected model are given in Section 7 and Section 8. In Section 9, we prove Theorem 1.9. At many points of the chapter we need to estimate the probabilities of certain non-typical events, the proofs of these lemmas are collected in Section 10.

CEU eTD Collection

2 Preliminaries

In most of the chapter we will consider the directed model, and then later give the modifications of the arguments that are needed to be done for the undirected model.

Consider a vector $q = (q_1, q_2, ..., q_n) \in V^n$. For a permutation π of the set $\{1, 2, \dots, n\}$, the vector $q_\pi = (q_{\pi(1)}, q_{\pi(2)}, \dots, q_{\pi(n)})$ is called a permutation of q. We write $q_1 \sim q_2$ if q_1 and q_2 are permutations of each other. The relation $\sim$ is an equivalence relation, the equivalence class of q, i.e., the set of permutations of q is denoted by $S(q)$. A random permutation of q is defined as the random variable q_π, where π is chosen uniformly from the set of all permutations, or equivalently, as a uniform random element of $S(q)$.

Note that for $q \in V^n$, the equivalence class $S(q)$ can be described by $|V|$ non-negative integers summing up to n. Namely, for $c \in V$, we define

$$m_q(c) = |\{i \quad | \quad q_i = c\}|,$$

so m_q can be considered as a vector in $\mathbb{R}^V$.

Fix $\frac{1}{2} < \alpha < \beta < \gamma < \frac{2}{3}$. We keep these choices fixed throughout the whole chapter. All the (explicit or implicit) constants are allowed to depend on the choice of α, β and γ. However, since we view α, β and γ as fixed, we will never emphasize this.

Note that if we choose a uniform random element q of V^n, then the expectation of $m_q(c)$ is $\frac{n}{|V|}$ for any $c \in V$. This makes the following definition quite natural.

Definition 2.1. A vector $q \in V^n$ is called α-typical if $\left\| m_q - \frac{n}{|V|}\mathbb{1} \right\|_\infty < n^\alpha$. Here $\mathbb{1}$ is the all 1 vector and $\|.\|_\infty$ is the maximum norm.

Similarly, we can can define β-typical vectors. Note that, since $\alpha > \frac{1}{2}$, a uniform element of V^n will be α-typical with probability $1 - o(1)$.

We write $A_n^{(d)}$ in place of A_n to emphasize the value of d.

One of the key steps towards Theorem 1.5 is the following theorem.

Theorem 2.2. *For any fixed finite abelian group V and $d \geq 3$, we have*

$$\lim_{n\to\infty} |V|^n \sup_{q \in V^n \quad \alpha-typical} d_\infty(A_n^{(d)} q, U_{q,d}) = 0.$$

This will be an easy consequence of the following theorem.

Theorem 2.3. *For any fixed finite abelian group V and $h \geq 2$, we have*

$$\lim_{n\to\infty} \sup_{\substack{q\in V^n \quad \alpha-typical \\ r\in R(q,h) \quad \beta-typical}} \left| \mathbb{P}(A_n^{(h)} q = r)|V|^{n-1} - 1 \right| = 0.$$

CEU eTD Collection

In the proofs we often need to consider h-tuples $Q = (q^{(1)}, q^{(2)}, \dots, q^{(h)})$ where each $q^{(i)}$ is a permutation of a fixed $q \in V^n$. Such h-tuples will be called (q,h)-tuples. Let $\mathcal{Q}_{q,h}$ be the set of (q,h)-tuples. A random (q,h)-tuple is a tuple $\bar{Q} = (\bar{q}^{(1)}, \bar{q}^{(2)}, \dots, \bar{q}^{(h)})$, where $\bar{q}^{(1)}, \bar{q}^{(2)}, ..., \bar{q}^{(h)}$ are independent random permutations of q.

Whenever we use the symbols Q and $\bar{Q}$, they stand for a (q,h)-tuple, and a random (q,h)-tuple respectively, even if this is not mentioned explicitly. The value of q should be clear from the context.

Sometimes, it will be convenient to view a (q,h)-tuple Q as a vector $Q = (Q_1, Q_2, \dots, Q_n)$ in $\left(V^h\right)^n$, where $Q_i = (q_i^{(1)}, q_i^{(2)}, \dots, q_i^{(h)})$. The vector m_q was used to extract the important information from a vector $q \in V^n$, we do the same for (q,h)-tuples, that is, for $t \in V^h$, we define

$$m_Q(t) = |\{i \quad | \quad Q_i = t\}|.$$

For a subset S of V^h, the sum $\sum_{t \in S} m_Q(t)$ is denoted by $m_Q(S)$. Instead of S, we usually just write the property that defines the subset S. For example, $m_Q(\tau_1 = c)$ stands for $m_Q(\{\tau \in V^h | \quad \tau_1 = c\})$.

Definition 2.4. A (q,h)-tuple Q or m_Q itself will be called γ-typical if

$$\left\| m_Q - \frac{n}{|V|^h} \mathbb{1} \right\|_\infty < n^\gamma.$$

The sum $\Sigma(Q)$ of a (q,h)-tuple Q is defined as $\Sigma(Q) = \sum_{i=1}^h q^{(i)}$.

Note that for a random (q,h)-tuple $\bar{Q}$, the distribution of $\Sigma(\bar{Q})$ is the same as that of $A_n^{(h)} q$.

Later in the chapter, we will give asymptotic formulas that will be true uniformly in the following sense.

Definition 2.5. Let $X_1, X_2, ...$ and $Y_1, Y_2, ...$ be two sequences of finite sets, $P_n \subset X_n \times Y_n$, $f : \cup_{n=1}^\infty X_n \to \mathbb{R}$ and $g : \cup_{n=1}^\infty Y_n \to \mathbb{R}$.

The term $f(x_n) \sim g(y_n)$ *uniformly* for $(x_n, y_n) \in P_n$ means that

$$\lim_{n\to\infty} \sup_{(x_n,y_n)\in P_n} \left| \frac{f(x_n)}{g(y_n)} - 1 \right| = 0.$$

The statement of Theorem 2.3 then can be reformulated as

$$\mathbb{P}(\Sigma(\bar{Q}) = r) \sim \frac{1}{|V|^{n-1}}$$

uniformly for any α-typical $q \in V^n$ and β-typical $r \in R(q,h)$.

CEU eTD Collection

3 Behavior of typical vectors

In this section and the next section, we keep V and h fixed. All the (explicit or implicit) constants are allowed to depend on V and h. Moreover, whenever we claim the convergence of any quantity, it is meant that the convergence is only true for fixed V and h. We never claim any uniformity over the choice of V and h. Note that we deal with the question of uniformity in d in Section 6 separately.

We assume that $h \geq 2$ throughout this section.

3.1 The proof of Theorem 2.3

We express the event $\Sigma(\bar{Q}) = r$ as the disjoint union of smaller events, which can be handled more easily. Let

$$\mathcal{M}(q,r) = \{m_Q \quad | \quad Q \in \mathcal{Q}_{q,h}, \Sigma(Q) = r\}.^5$$

Then the event $\Sigma(\bar{Q}) = r$ can be written as the disjoint union of the events $(\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)$ where m runs through $\mathcal{M}(q,r)$, so

$$\mathbb{P}(\Sigma(\bar{Q}) = r) = \sum_{m \in \mathcal{M}(q,r)} \mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)).$$

Observe that $\mathcal{M}(q,r)$ consists of the non-negative integral points of a certain affine subspace $A(q,r)$ of $\mathbb{R}^{V^h}$. This affine subspace $A(q,r)$ is determined by linear equations expressing that whenever $\Sigma(Q) = r$ for a (q,h)-tuple $Q = (q^{(1)}, q^{(2)}, \dots, q^{(h)})$, we have $m_{q^{(i)}} = m_q$ for every $i = 1, 2, \dots, h$ and $m_{\Sigma(Q)} = m_r$, as the following lemma shows.

For $t = (t_1, t_2, \dots, t_h) \in V^h$, we define t_Σ as $t_\Sigma = \sum_{i=1}^h t_i$.

Lemma 3.1. *Consider $q, r \in V^n$. If $m \in \mathcal{M}(q,r)$, then m is a non-negative integral vector satisfying the following linear equations:*

$$m(\tau_i = c) = m_q(c) \qquad \forall i \in \{1, 2, \dots, h\}, c \in V, \tag{3.1}$$
$$m(\tau_\Sigma = c) = m_r(c) \qquad \forall c \in V. \tag{3.2}$$

Now assume that m is a nonnegative integral vector satisfying the equations above, then

[5] Here we omitted from the notation the dependence on h, later we will do this several times without mentioning it.

CEU eTD Collection

$$\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)) = \frac{\prod_{c\in V} m_r(c)!}{\prod_{t\in V^h} m(t)!} \Bigg/ \left(\frac{n!}{\prod_{c\in V} m_q(c)!}\right)^h \tag{3.3}$$
$$= \frac{\prod_{c\in V} m(\tau_\Sigma = c)!}{\prod_{t\in V^h} m(t)!} \Bigg/ \left(\frac{n!}{\prod_{c\in V} m_q(c)!}\right)^h.$$

In particular, $\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)) > 0$ *so* $m \in \mathcal{M}(q,r)$*. Thus,* $\mathcal{M}(q,r)$ *is the set of non-negative integral points of the affine subspace* $A(q,r)$ *given by the linear equations above.*

Proof. We only give the proof of Equation (3.3), since all the other statements of the lemma are straightforward to prove. For $c \in V$, let

$$I_c = \{i \in \{1,2,\dots,n\} | \quad r_i = c\},$$

and let $W_c = \{t \in V^h | t_\Sigma = c\}$. Let $Q = (Q_1, Q_2, \dots, Q_n) \in \left(V^h\right)^n$. Assume that m is a nonnegative integral vector satisfying Equation (3.1) and Equation (3.2) above. Observe that $Q \in \mathcal{Q}_{q,h}$, $m_Q = m$ and $\Sigma(Q) = r$ if and only if for every $c \in V$, the sets

$$(\{i \in \{1,2,\dots,n\} \quad | \quad Q_i = t\})_{t\in W_c}$$

give us a partition of I_c, such that for every $t \in W_c$, the size of the corresponding part is $m(t)$.

Note that for any $c \in V$, we have

$$\frac{|I_c|!}{\prod_{t\in W_c} m(t)!} = \frac{m_r(c)!}{\prod_{t\in W_c} m(t)!}$$

such partitions of I_c.

Clearly, the total number (q,h)-tuples is

$$\left(\frac{n!}{\prod_{c\in V} m_q(c)!}\right)^h.$$

Putting everything together the statement follows. □

The left hand sides of Equation (3.1) and Equation (3.2) in Lemma 3.1 do not depend on q or r, therefore the affine subspaces $A(q,r)$ are all parallel for any choice of q and r. Hence, for every $q, r_1, r_2 \in V^n$, there is a translation that moves $A(q,r_1)$ to $A(q,r_2)$. There are many such translations, and we will use the one given in the next lemma.

Lemma 3.2. *For any* $r_1, r_2 \in V^n$*, we define the vector* $v = v_{r_1,r_2} \in \mathbb{R}^{V^h}$ *by*

$$v(t) = \frac{m_{r_2}(t_\Sigma) - m_{r_1}(t_\Sigma)}{|V|^{h-1}}$$

CEU eTD Collection

for every $t \in V^h$. Then, for any $q \in V^h$, we have

$$A(q, r_1) + v_{r_1,r_2} = A(q, r_2).$$

Proof. It is enough to prove that $A(q, r_1) + v_{r_1,r_2} \subset A(q, r_2)$ or equivalently if m satisfies Equation (3.1) and Equation (3.2) in Lemma 3.1 above for $r = r_1$, then $m' = m + v_{r_1,r_2}$ satisfies Equation (3.1) and Equation (3.2) for $r = r_2$. Observe that for any $i = 1, 2, \dots, h$ and $c, s \in V$, we have

$$|\{t \in V^h| \quad t_i = c, t_\Sigma = s\}| = |V|^{h-2}.$$

(Here we need to use that $h \geq 2$.) So we have

$$\begin{aligned}
\sum_{\substack{t \in V^h \\ t_i = c}} m'(t) &= \sum_{\substack{t \in V^h \\ t_i = c}} m(t) + \sum_{\substack{t \in V^h \\ t_i = c}} v_{r_1,r_2}(t) \\
&= m_q(c) + \sum_{s \in V} |\{t \in V^h| \quad t_i = c, t_\Sigma = s\}| \frac{m_{r_2}(s) - m_{r_1}(s)}{|V|^{h-1}} \\
&= m_q(c) + \frac{1}{|V|} \left(\sum_{s \in V} m_{r_2}(s) - \sum_{s \in V} m_{r_1}(s) \right) \\
&= m_q(c) + \frac{1}{|V|}(n - n) = m_q(c),
\end{aligned}$$

that is, Equation (3.1) is satisfied. Furthermore, for any $c \in V$, we have

$$\begin{aligned}
\sum_{\substack{t \in V^h \\ t_\Sigma = c}} m'(t) &= \sum_{\substack{t \in V^h \\ t_\Sigma = c}} m(t) + \sum_{\substack{t \in V^h \\ t_\Sigma = c}} v_{r_1,r_2}(t) \\
&= m_{r_1}(c) + |V|^{h-1} \frac{m_{r_2}(c) - m_{r_1}(c)}{|V|^{h-1}} = m_{r_2}(c),
\end{aligned}$$

that is, Equation (3.2) is satisfied. □

Whenever $A(q, r)$ contains integral points, the integral points of $A(q, r)$ are placed densely, in the sense that there is a D, depending only on h and V, such that for any point $x \in A(q, r)$, there is an integral point $y \in A(q, r)$ with $\|x - y\|_\infty < D$. Actually, this is a general fact as the following lemma shows.

Lemma 3.3. *Let A be an affine subspace of $\mathbb{R}^k$ which is given by a set of equations with rational coefficients. Assume that A contains an integral point p. Then there is a D such that for any point $x \in A$, there is an integral point $y \in A$ with $\|x - y\|_\infty < D$. For parallel subspaces, we can choose the same D.*

Proof. Observe that we can write A as $A = p + A_0$, where A_0 is a linear subspace generated by a set of rational vectors $\{a_1, a_2, \dots, a_\ell\}$. Multiplying these vectors with an appropriate scalar,

CEU eTD Collection

we may assume that they are all integral vectors. Let

$$D = \sum_{i=1}^{\ell} \|a_i\|_\infty.$$

Note that $x - p \in A_0$, so $x - p = \sum_{i=1}^{\ell} \alpha_i a_i$ for some constants α_i. Then

$$y = p + \sum_{i=1}^{\ell} \lfloor \alpha_i \rfloor a_i$$

is an integral vector such that $\|x - y\|_\infty < D$. $\square$

For $c \in V$, let $w_c \in \mathbb{R}^{V^h}$ be such that $w_c(t) = 1$ if $t_\Sigma = c$ and $w_c(t) = 0$ otherwise. For $i = 1, 2, \dots, h$ and $c \in V$, let $u_{i,c} \in \mathbb{R}^{V^h}$ be such that $u_{i,c}(t) = 1$ if $t_i = c$ and $u_{i,c}(t) = 0$ otherwise.

Lemma 3.4. *If $r \in R(q, h)$, then $A(q, r)$ contains an integral point.*

Proof. We need to show that the system of linear equations given by Equation (3.1) and Equation (3.2) admits an integral solution. Using the integral analogue of Farkas' lemma [54, Corollary 4.1a.], we obtain that there exists an integral solution if and only if for every choice of rational numbers
$0 \le \gamma(i, c) < 1$ $(i = 1, 2, \dots, h, \quad c \in V)$ and $0 \le \delta(c) < 1$ $(c \in V)$ such that

$$\sum_{i=1}^{h} \sum_{c \in V} \gamma(i, c) u_{i,c} + \sum_{c \in V} \delta(c) w_c \text{ is an integral vector} \tag{3.4}$$

the number $\sum_{i=1}^{h} \sum_{c \in V} \gamma(i, c) m_q(c) + \sum_{c \in V} \delta(c) m_r(c)$ is an integer. We project the rational numbers $\gamma(i, c)$ and $\delta(c)$ to the group $S^1 = \mathbb{Q}/\mathbb{Z}$. From now on we work in the group S^1. The condition given in (3.4) translates as follows. For every $t \in V^h$,

$$\sum_{i=1}^{h} \gamma(i, t_i) + \delta(t_\Sigma) = 0 \tag{3.5}$$

in the group S^1. We define $\gamma'(i, c) = \gamma(i, c) - \gamma(i, 0)$ and $\delta'(c) = \delta(c) + \sum_{i=1}^{h} \gamma(i, 0)$. Clearly $\gamma'(i, 0) = 0$. Moreover, from Equation (3.5) with $t = 0$, we get that $\delta'(0) = 0$. Equation (3.5) can be rewritten as

$$\sum_{i=1}^{h} \gamma'(i, t_i) + \delta'(t_\Sigma) = 0.$$

CEU eTD Collection

For every i and c, if $t \in V^h$ is such that $t_i = c$ and $t_j = 0$ for $i \neq j$, then we obtain that $\gamma'(i,c) = -\delta'(c)$. Therefore, Equation (3.5) can be once again rewritten as

$$\sum_{i=1}^{h} \delta'(t_i) = \delta'(t_\Sigma) = \delta'\left(\sum_{i=1}^{h} t_i\right),$$

which means that δ' is a group homomorphism between V and $\mathbb{Q}/\mathbb{Z}$. Thus, we get that

$$\begin{aligned}
&\sum_{i=1}^{h}\sum_{c\in V}\gamma(i,c)m_q(c) + \sum_{c\in V}\delta(c)m_r(c) \\
&\quad= \sum_{i=1}^{h}\sum_{c\in V}\big(\gamma'(i,c)+\gamma(i,0)\big)\,m_q(c) + \sum_{c\in V}\left(\delta'(c) - \sum_{i=1}^{h}\gamma(i,0)\right)m_r(c) \\
&\quad= \sum_{i=1}^{h}\sum_{c\in V} -\delta'(c)m_q(c) + \sum_{c\in V}\delta'(c)m_r(c) \\
&\quad= -h\sum_{c\in V}\delta'(c)m_q(c) + \sum_{c\in V}\delta'(c)m_r(c) \\
&\quad= -h\sum_{i=1}^{n}\delta'(q_i) + \sum_{i=1}^{n}\delta'(r_i) = \delta'\left(-h\cdot s(q)+s(r)\right) = \delta'(0) = 0
\end{aligned}$$

using that $r \in R(q,h)$. That is, $\sum_{i=1}^{h}\sum_{c\in V}\gamma(i,c)m_q(c) + \sum_{c\in V}\delta(c)m_r(c)$ is indeed an integer. □

Suppose that $r_1, r_2 \in R(q,h)$. Let $v = v_{r_1,r_2}$. Then there is an integral point m_1 in $A(q,r_1)$. Since $m_1 + v \in A(q,r_2)$, there is an integral point m_2 in $A(q,r_2)$ such that $\|m_1+v-m_2\|_\infty < D$. Set $\hat{v} = \hat{v}_{r_1,r_2} = m_2 - m_1$, then $\|\hat{v}-v\|_\infty < D$ and the map $m \mapsto m+\hat{v}$ gives a bijection between the integral points of $A(q,r_1)$ and the integral points of $A(q,r_2)$.

For each α-typical $q \in V^n$, fix an arbitrary β-typical $r_0 = r_0(q) \in R(q,h)$, that is, let r_0 be any β-typical $r_0 \in V^n$ such that $s(r_0) = h \cdot s(q)$. Set

$$\mathcal{M}^*(q,r_0) = \left\{ m \in \mathcal{M}(q,r_0) \quad \middle| \quad \left\| m - \frac{n}{|V|^h}\mathbb{1} \right\|_\infty < 2n^\gamma \right\}.$$

For any other β-typical $r \in R(q,h)$, we define

$$\mathcal{M}^*(q,r) = \{ m + \hat{v}_{r_0,r} \quad | \quad m \in \mathcal{M}^*(q,r_0) \} \subset \mathcal{M}(q,r).$$

Observe that for large enough n, if both r_0 and r are β-typical, then

$$\|\hat{v}_{r_0,r}\|_\infty < D + \frac{2n^\beta}{|V|^{h-1}} < n^\gamma.$$

CEU eTD Collection

Thus, using that the map $m \mapsto m + \hat{v}_{r_0,r}$ is a bijection between the integral points of $A(q, r_0)$ and the integral points of $A(q, r)$, we obtain that if n is large enough, then for every α-typical $q \in V^n$ and β-typical $r \in R(q,h)$, we have

$$\left\{ m \in \mathcal{M}(q,r) \quad \middle| \quad \left\| m - \frac{n}{|V|^h}\mathbb{1} \right\|_\infty < n^\gamma \right\} \subset \mathcal{M}^*(q,r). \tag{3.6}$$

Here the set on the left is just the set of the γ-typical elements of $\mathcal{M}(q,r)$.

The crucial point of our argument is the next lemma.

Lemma 3.5. *For an α-typical $q \in V^n$, a β-typical $r \in R(q,h)$, $r_0 = r_0(q)$ and $m \in \mathcal{M}^*(q, r_0)$, we have that*

$$\mathbb{P}((\Sigma(\bar{Q}) = r_0) \wedge (m_{\bar{Q}} = m)) \sim \mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m + \hat{v}_{r_0,r}))$$

uniformly in the sense of Definition 2.5.

Remark 3.6. For clarity, we write out the definition of the uniform convergence above. That is, Lemma 3.5 is equivalent with the statement that for any fixed V and h, we have

$$\lim_{n\to\infty} \sup_{\substack{q\in V^n \quad \alpha\text{-typical} \\ m\in\mathcal{M}^*(q,r_0(q)) \\ r\in R(q,h) \quad \beta\text{-typical}}} \left| \frac{\mathbb{P}((\Sigma(\bar{Q}) = r_0(q)) \wedge (m_{\bar{Q}} = m))}{\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m + \hat{v}_{r_0(q),r}))} - 1 \right| = 0.$$

To prove Lemma 3.5, we need a few lemmas.

The following approximation will be useful for Lemma 3.8.

Lemma 3.7. *Fix $K(n)$ such that $K(n) = o\left(n^{\frac{2}{3}}\right)$. Then for $|k| < K(n)$, we have*

$$(n+k)! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \exp\left(k\log n + \frac{k^2}{2n}\right)$$

uniformly. In other words, we have

$$\lim_{n\to\infty} \sup_{|k|<K(n)} \left| \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \exp\left(k\log n + \frac{k^2}{2n}\right)}{(n+k)!} - 1 \right| = 0.$$

Proof. Using Taylor's theorem with the Lagrange form of the remainder [53, Theorem 5.15] for the function $f(x) = x\log x$, we get that

$$\left|(n+k)\log(n+k) - \left(n\log n + (\log n + 1)k + \frac{k^2}{2n}\right)\right| = \left|\frac{f^{(3)}(c)}{6}k^3\right| = \frac{|k|^3}{6c^2}$$

CEU eTD Collection

for some $c \in (n, n+k)$. This implies that

$$\lim_{n\to\infty} \sup_{|k|<K(n)} \left| (n+k)\log(n+k) - \left(n\log n + (\log n + 1)k + \frac{k^2}{2n} \right) \right| = 0.$$

It is also clear that

$$\frac{\sqrt{n+k}}{\sqrt{n}} \sim 1$$

uniformly for $|k| \leq K(n)$.

Recall that Stirling's formula [53, (8.22)] states that

$$n! \sim \sqrt{2\pi n} \exp(n\log n - n).$$

If we put everything together, then we get that

$$\begin{aligned}
(n+k)! &\sim \sqrt{2\pi(n+k)} \exp\left((n+k)\log(n+k) - (n+k)\right) \\
&\sim \sqrt{2\pi n} \exp\left(\left(n\log n + (\log n + 1)k + \frac{k^2}{2n} \right) - (n+k) \right) \\
&= \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \exp\left(k\log n + \frac{k^2}{2n} \right)
\end{aligned}$$

uniformly for $|k| \leq K(n)$. □

Note that in the lemma above, we do not need to assume that n is an integer, as long as $n+k$ is an integer.

In the next lemma, we use the notation $a(n) = \sqrt{2\pi n}(\frac{n}{e})^n$.

Lemma 3.8. *For $q, r \in V^n$ and $m \in \mathcal{M}(q,r)$ such that $\left\| m - \frac{n}{|V|^h}\mathbb{1} \right\|_\infty < 3n^\gamma$, we have*

$$\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)) \sim f(q) \exp\left(\frac{1}{2n} B\left(m - \frac{n}{|V|^h}\mathbb{1}, m - \frac{n}{|V|^h}\mathbb{1} \right) \right)$$

uniformly, where

$$f(q) = \left(\frac{n!}{\prod_{c\in V} m_q(c)!} \right)^{-h} \frac{\left(a\left(\frac{n}{|V|}\right)\right)^{|V|}}{\left(a\left(\frac{n}{|V|^h}\right)\right)^{|V|^h}},$$

and $B : \mathbb{R}^{V^h} \times \mathbb{R}^{V^h} \to \mathbb{R}$ is a bilinear form defined as

$$B(x,y) = |V| \sum_{c\in V} \left(\sum_{\substack{t\in V^h \\ t_\Sigma = c}} x(t) \right) \left(\sum_{\substack{t\in V^h \\ t_\Sigma = c}} y(t) \right) - |V|^h \sum_{t\in V^h} x(t)y(t).$$

Note that $f(q)$ does not depend on r and m.

CEU eTD Collection

Proof. Recall that $\gamma < \frac{2}{3}$, so for any $t \in V^h$, Lemma 3.7 can be applied to expand $m(t)!$ at the point $\frac{n}{|V|^h}$. Thus, we obtain the approximation

$$m(t)! \sim a\left(\frac{n}{|V|^h}\right) \cdot \exp\left(\left(m(t) - \frac{n}{|V|^h}\right)\log\frac{n}{|V|^h} + \frac{|V|^h\left(m(t) - \frac{n}{|V|^h}\right)^2}{2n}\right).$$

Similarly, for every $c \in V$, by expanding $m(\tau_\Sigma = c)!$ at the point $\frac{n}{|V|}$, we obtain the approximation

$$m(\tau_\Sigma = c)! \sim a\left(\frac{n}{|V|}\right) \cdot \exp\left(\left(\sum_{\substack{t\in V^h\\ t_\Sigma = c}} m(t) - \frac{n}{|V|}\right)\log\frac{n}{|V|} + \frac{|V|\left(\sum_{\substack{t\in V^h\\ t_\Sigma = c}}\left(m(t) - \frac{n}{|V|^h}\right)\right)^2}{2n}\right).$$

Substituting these approximations in Equation (3.3), we obtain the statement. □

We made all the necessary preparations to prove Lemma 3.5.

Proof. (Lemma 3.5) It is easy to check that w_c is in the radical of the bilinear form B, that is, $B(.,w_c) = B(w_c,.) = 0$. (w_c was defined before Lemma 3.4.) Since $v_{r_0,r} \in \mathrm{Span}_{c\in V} w_c$, we get that $v_{r_0,r}$ is also in the radical. Observe that if n is large enough, then $\|\hat{v}_{r_0,r}\|_\infty < D + \frac{2n^\beta}{|V|^{h-1}} < n^\gamma$, so both m and $m + \hat{v}_{r_0,r}$ satisfies the conditions of Lemma 3.8. It is also clear that $B(x,y) = O(\|x\|_\infty \|y\|_\infty)$. Thus,

$$\begin{aligned}
&\frac{1}{2n}B\left(m + \hat{v}_{r_0,r} - \frac{n}{|V|^h}\mathbb{1}, m + \hat{v}_{r_0,r} - \frac{n}{|V|^h}\mathbb{1}\right)\\
&= \frac{1}{2n}B\left(m + (\hat{v}_{r_0,r} - v_{r_0,r}) + v_{r_0,r} - \frac{n}{|V|^h}\mathbb{1}, m + (\hat{v}_{r_0,r} - v_{r_0,r}) + v_{r_0,r} - \frac{n}{|V|^h}\mathbb{1}\right)\\
&= \frac{1}{2n}\Bigg(B\left(m - \frac{n}{|V|^h}\mathbb{1}, m - \frac{n}{|V|^h}\mathbb{1}\right) + 2B\left(m - \frac{n}{|V|^h}\mathbb{1}, \hat{v}_{r_0,r} - v_{r_0,r}\right)\\
&\qquad\qquad + B\left(\hat{v}_{r_0,r} - v_{r_0,r}, \hat{v}_{r_0,r} - v_{r_0,r}\right)\Bigg)\\
&= \frac{1}{2n}\left(B(m - \frac{n}{|V|^h}\mathbb{1}, m - \frac{n}{|V|^h}\mathbb{1}) + O(4Dn^\gamma + D^2)\right)\\
&= \frac{1}{2n}B\left(m - \frac{n}{|V|^h}\mathbb{1}, m - \frac{n}{|V|^h}\mathbb{1}\right) + O(n^{\gamma-1}).
\end{aligned}$$

Then, the statement follows from Lemma 3.8. □

CEU eTD Collection

From Lemma 3.5, it follows immediately that for an α-typical q and β-typical $r_1, r_2 \in R(q,h)$, we have

$$\sum_{m \in \mathcal{M}^*(q,r_1)} \mathbb{P}((\Sigma(\bar{Q}) = r_1) \wedge (m_{\bar{Q}} = m)) \sim \sum_{m \in \mathcal{M}^*(q,r_2)} \mathbb{P}((\Sigma(\bar{Q}) = r_2) \wedge (m_{\bar{Q}} = m))$$

uniformly, or equivalently

$$\mathbb{P}((\Sigma(\bar{Q}) = r_1) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r_1))) \sim \mathbb{P}((\Sigma(\bar{Q}) = r_2) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r_2))) \tag{3.7}$$

uniformly.

The content of the next lemma can be summarized as "only the typical events matter".

Lemma 3.9. *We have*

(i) A uniformly chosen element of V^n is β-typical with probability $1 - o(1)$.

(ii) There is a C_1 such that for any α-typical $q \in V^n$, we have

$$\mathbb{P}(\bar{Q} \textit{ is not } \gamma - \textit{typical}) \leq C_1 \exp(-n^{2\gamma-1}/C_1).$$

In particular, for an α-typical $q \in V^n$, we have $\mathbb{P}(\bar{Q}$ is $\gamma -$ typical$) \sim 1$ uniformly in the sense of Definition 2.5.

(iii) There is a C_2 such that for any α-typical $q \in V^n$, we have

$$\mathbb{P}(\Sigma(\bar{Q}) \textit{ is not } \beta - \textit{typical}) \leq C_2 \exp(-n^{2\beta-1}/C_2).$$

In particular, for an α-typical $q \in V^n$, we have $\mathbb{P}(\Sigma(\bar{Q})$ is $\beta -$ typical$) \sim 1$ uniformly in the sense of Definition 2.5.

(iv) The following holds

$$\lim_{n\to\infty} \sup_{\substack{q \in V^n \quad \alpha-\textit{typical} \\ r \in R(q,h) \quad \beta-\textit{typical}}} \mathbb{P}\left((\Sigma(\bar{Q}) = r) \wedge (\bar{Q} \textit{ is not } \gamma - \textit{typical})\right) |V|^{n-1} = 0.$$

Proof. Part (i) can be proved using standard concentration results. We omit the details. To prove the other statements of Lemma 3.9, we need the following result.

Lemma 3.10. *Fix $K(n)$ such that $n^\alpha = o(K(n))$. There is a C such that for any α-typical $q \in V^n$ and a random (q,h)-tuple $\bar{Q}$, we have*

$$\mathbb{P}\left(\left\| m_{\bar{Q}} - \frac{n}{|V|^h}\mathbb{1}\right\|_\infty \geq K(n)\right) \leq C \exp\left(-\frac{K(n)^2}{Cn}\right).$$

CEU eTD Collection

Proof. Observe that for any α-typical $q \in V^n$ and $t \in V^h$, we have

$$\left| n \prod_{i=1}^{h} \frac{m_q(t_i)}{n} - \frac{n}{|V|^h} \right| = O(n^\alpha) = o(K(n)),$$

where the hidden constant does not depend on q or t. Thus, for an α-typical $q \in V^n$ and a (q,h)-tuple Q, if we have

$$\left| m_Q(t) - \frac{n}{|V|^h} \right| \geq K(n)$$

for some $t \in V^h$, then

$$\left| m_Q(t) - n \prod_{i=1}^{h} \frac{m_q(t_i)}{n} \right| \geq (1 - o(1))K(n).$$

The lemma follows from Lemma 10.2 and the union bound. ☐

With the choice of $K(n) = n^\gamma$ Lemma 3.10 implies part (ii).

To prove part (iii), choose $K(n) = |V|^{-(h-1)} n^\beta$, and observe the following. For (q,h)-tuple Q, if we have

$$\left\| m_Q - \frac{n}{|V|^h} \mathbb{1} \right\|_\infty < K(n),$$

then $\Sigma(Q)$ is β-typical.

To prove part (iv), we need the following lemma.

Lemma 3.11. *There is a $C_3 > 0$ such that for every β-typical $r \in V^n$, if we consider the number of permutations of r, i. e., the cardinality of the set $S(r) = \{r'$ is a permutation of $r\}$, then we have*

$$|S(r)| \geq |V|^n \exp\left(-C_3 n^{2\beta-1}\right).$$

Proof. This can be proved using Lemma 3.7. ☐

Part (iv) follows from the next lemma.

Lemma 3.12. *We will use the constants C_1 and C_3 provided by Lemma 3.11 and part (ii). For every α-typical $q \in V^n$, β-typical $r \in V^n$ and a random (q,h)-tuple $\bar{Q}$, we have*

$$\mathbb{P}(\Sigma(\bar{Q}) = r \text{ and } \bar{Q} \text{ is not } \gamma\text{-typical}) < \frac{C_1 \exp\left(-n^{2\gamma-1}/C_1 + C_3 n^{2\beta-1}\right)}{|V|^n}.$$

Here the numerator $C_1 \exp\left(-n^{2\gamma-1}/C_1 + C_3 n^{2\beta-1}\right)$ on the right hand side goes to 0 as n goes to infinity.

Proof. For every $r' \in S(r)$, consider the event that $\Sigma(\bar{Q}) = r'$ and $\bar{Q}$ is not γ-typical. These events are disjoint, and by symmetry, they have the same probability. Moreover,

CEU eTD Collection

they are all contained by the event that Q is not γ-typical. Thus,

$$\mathbb{P}(\Sigma(\bar{Q}) = r \text{ and } \bar{Q} \text{ is not } \gamma\text{-typical}) \leq \frac{\mathbb{P}(\bar{Q} \text{ is not } \gamma\text{-typical})}{|S(r)|}.$$

The statement then follows from part (ii) and Lemma 3.11. $\square$

This concludes the proof of Lemma 3.9. $\square$

Fix an α-typical $q \in V^n$. For every β-typical $r \in R(q,h)$, consider the events $(\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r))$. These events are pairwise disjoint. Moreover, from (3.6) above, we see that their union contains the event $(\Sigma(\bar{Q}) \text{ is } \beta-\text{typical}) \wedge (\bar{Q} \text{ is } \gamma - \text{typical})$ for large enough n. So for large enough n, we have

$$\begin{aligned}&\mathbb{P}((\Sigma(\bar{Q}) \text{ is } \beta - \text{typical}) \wedge (\bar{Q} \text{ is } \gamma - \text{typical})) \\ &\qquad \leq \sum_{r\in R(q,h) \quad \beta-\text{typical}} \mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r))) \leq 1. \quad (3.8)\end{aligned}$$

From part (ii) and (iii) of Lemma 3.9, we get that

$$\mathbb{P}((\Sigma(\bar{Q}) \text{ is } \beta - \text{typical}) \wedge (\bar{Q} \text{ is } \gamma - \text{typical})) \sim 1$$

uniformly for all α-typical $q \in V^n$. Thus

$$\sum_{r\in R(q,h) \quad \beta-\text{typical}} \mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r))) \sim 1$$

uniformly for every α-typical $q \in V^n$. Combining this with Equation (3.7), we obtain that

$$\begin{aligned}&\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} \in \mathcal{M}^*(q,r))) \sim \\ &\qquad |\{r \in R(q,h)| \quad r \text{ is } \beta\text{-typical}\}|^{-1} \sim |R(q,h)|^{-1} = |V|^{-(n-1)}\end{aligned}$$

uniformly for all α-typical $q \in V^n$ and β-typical $r \in R(q,h)$. Here in the second line, we used part (i) of Lemma 3.9. Finally, using part (iv) of Lemma 3.9 and (3.6), we get Theorem 2.3.

3.2 The proof of Theorem 2.2

We start by a simple lemma.

Lemma 3.13. *For $q, r \in V^n$, and $h \geq 2$, we have $\mathbb{P}(A_n^{(h)} q = r) \leq |S(q)|^{-1}$.*

Proof. Let q' be a uniform random permutation of q independent from $A_n^{(h-1)}$. Observe that $A_n^{(h)} q$ has the same distribution as $A_n^{(h-1)} q + q'$. The statement of the lemma follows from the facts that

$$\mathbb{P}(A_n^{(h-1)} q + q' = r| \quad r - A_n^{(h-1)} q \sim q) = |S(q)|^{-1}$$

CEU eTD Collection

and
$$\mathbb{P}(A_n^{(h-1)}q + q' = r| \quad r - A_n^{(h-1)}q \not\sim q) = 0.$$

□

Now we prove Theorem 2.2 from Theorem 2.3.

Proof. Let $q \in V^n$ be α-typical, and let $r \in R(q,d)$. Let q' be a uniform random permutation of q independent from $A_n^{(d-1)}$. Observe that $A_n^{(d)}q$ has the same distribution as $A_n^{(d-1)}q + q'$. Now, we have
$$\mathbb{P}(A_n^{(d)}q = r) = \mathbb{E}\mathbb{P}(A_n^{(d-1)}q = r - q'),$$
where the expectation is over the random choice of q'.

Observe that

- $\mathbb{P}(A_n^{(d-1)}q = r - q') \sim |V|^{-(n-1)}$ uniformly, if $r - q'$ is β-typical.
- $0 \le \mathbb{P}(A_n^{(d-1)}q = r - q') \le |S(q)|^{-1}$ otherwise.

Indeed, the first statement follows from Theorem 2.3 and the fact that $r - q' \in R(q, d-1)$. The second statement follows from Lemma 3.13.

Moreover, combining Lemma 10.1 with the union bound, we get the following statement. There is a $c > 0$ such that
$$\mathbb{P}(r - q' \text{ is not } \beta - \text{typical}) \le \exp(-cn^{2\beta-1}).$$

From the law of total probability, we have
$$\begin{aligned}\mathbb{P}(A_n^{(d)}q = r) = {}& \mathbb{P}(A_n^{(d-1)}q = r - q' | r - q' \text{ is } \beta - \text{typical})\mathbb{P}(r - q' \text{ is } \beta - \text{typical}) \\ &+ \mathbb{P}(A_n^{(d-1)}q = r - q' | r - q' \text{ is not } \beta - \text{typical})\mathbb{P}(r - q' \text{ is not } \beta - \text{typical}).\end{aligned}$$

Inserting the inequalities above into this, we obtain that
$$(1+o(1))|V|^{-(n-1)}(1-\exp(-cn^{2\beta-1})) \le \mathbb{P}(A_n^{(d)}q = r) \le (1+o(1))|V|^{-(n-1)} + \frac{\exp(-cn^{2\beta-1})}{|S(q)|}.$$

Since there is c' such that $|S(q)| \ge |V|^n \exp(-c'n^{2\alpha-1})$ for every α-typical $q \in V^n$, we get that $\exp(-cn^{2\beta-1})/|S(q)| = o(|V|^{-n})$. The theorem follows.

□

CEU eTD Collection

4 Only the typical vectors matter

The aim of this section to prove Theorem 1.5. Let $\mathrm{Cos}(V)$ be the set of all cosets in V. Given a function $f(n)$, and a subset W of V, a vector $q \in V^n$ will be called $(W, f(n))$-typical if for every $c \in W$, we have $\left|m_q(c) - \frac{n}{|W|}\right| < n^\alpha$ and $\sum_{c \notin W} m_q(c) \leq f(n)$. In the previous section, we used the term α-typical for $(V, 0)$-typical vectors.

We start by a simple corollary of Theorem 2.2.

Lemma 4.1. *We have*

$$\lim_{n\to\infty} \sum_{W \in \mathrm{Cos}(V)} \sum_{\substack{q \text{ } is \\ (W,0)-typical}} d_\infty(A_n q, U_{q,d}) = 0.$$

Proof. If W is a subgroup of V, then from Theorem 2.2, we know that $d_\infty(A_n q, U_{q,d})$ is $o(|W|^{-n})$ uniformly for all $(W, 0)$-typical q. On the other hand, the number of $(W, 0)$-typical vectors is at most $|W|^n$. Thus,

$$\lim_{n\to\infty} \sum_{q \text{ is } (W,0)-\text{typical}} d_\infty(A_n q, U_{q,d}) = 0.$$

Consider a coset $W \in \mathrm{Cos}(V)$ such that W is not a subgroup of V. Let $t \in W$, then $W_0 = W - t$ is a subgroup of V. For $q = (q_1, q_2, \ldots, q_n) \in W^n$, we define $q' = (q_1 - t, q_2 - t, \ldots, q_n - t)$. Note that $q \mapsto q'$ is a bijection between W^n and W_0^n, and it is also a bijection between $(W, 0)$-typical and $(W_0, 0)$-typical vectors. Using this, it is easy to see that $d_\infty(A_n q, U_{q,d}) = d_\infty(A_n q', U_{q',d})$, which implies that

$$\lim_{n\to\infty} \sum_{q \text{ is } (W,0)-\text{typical}} d_\infty(A_n q, U_{q,d}) = \lim_{n\to\infty} \sum_{q' \text{ is } (W_0,0)-\text{typical}} d_\infty(A_n q', U_{q',d}) = 0,$$

using the already established case. Since $\mathrm{Cos}(V)$ is finite, the statement follows. $\square$

For $q \in V^n$, choose r_q such that

$$\mathbb{P}(A_n q = r_q) = \max_{r \in V^n} \mathbb{P}(A_n q = r).$$

For $W \in \mathrm{Cos}(V)$, we define $I(W^n) = \{q \in W^n \quad | \quad \mathrm{MinC}_q = W\}$.

Note that $V^n = \cup_{W \in \mathrm{Cos}(V)} I(W^n)$, where this is a disjoint union.

CEU eTD Collection

Then

$$
\begin{aligned}
&\limsup_{n\to\infty} \sum_{q\in V^n} d_\infty(A_n q, U_{q,d}) \\
&\quad= \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{q\in I(W^n)} d_\infty(A_n q, U_{q,d}) \\
&\quad= \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q \text{ is} \\ (W,0)-\text{typical}}} d_\infty(A_n q, U_{q,d}) \\
&\qquad+ \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q\in I(W^n) \text{ is} \\ \text{not } (W,0)-\text{typical}}} d_\infty(A_n q, U_{q,d}).
\end{aligned}
\tag{4.1}
$$

Using Lemma 4.1, we have

$$
\limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q \text{ is} \\ (W,0)-\text{typical}}} d_\infty(A_n q, U_{q,d}) = 0.
$$

For $q \in I(W^n)$, we have

$$
d_\infty(A_n q, U_{q,d}) \le |W|^{-(n-1)} + \mathbb{P}(A_n q = r_q)
$$

from the triangle inequality. Moreover,

$$
|\{q \in I(W^n) \quad | \quad q \text{ is not } (W,0) - \text{typical}\}| = o(|W|^n)
$$

from standard concentration results.

Inserting these into Equation (4.1), we obtain that

$$
\begin{aligned}
&\limsup_{n\to\infty} \sum_{q\in V^n} d_\infty(A_n q, U_{q,d}) \\
&\quad\le \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q\in I(W^n) \text{ is} \\ \text{not } (W,0)-\text{typical}}} \Big(|W|^{-(n-1)} + \mathbb{P}(A_n q = r_q)\Big) \\
&\quad= \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} |\{q \in I(W^n) \quad | \quad q \text{ is not } (W,0) - \text{typical}\}||W|^{-(n-1)} \\
&\qquad+ \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q\in I(W^n) \text{ is} \\ \text{not } (W,0)-\text{typical}}} \mathbb{P}(A_n q = r_q) \\
&\quad= \limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q\in I(W^n) \text{ is} \\ \text{not } (W,0)-\text{typical}}} \mathbb{P}(A_n q = r_q).
\end{aligned}
$$

CEU eTD Collection

Thus, in order to prove Theorem 1.5, it is enough to prove that

$$\limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q\in I(W^n) \text{ is} \\ \text{not } (W,0)-\text{typical}}} \mathbb{P}(A_n q = r_q) = 0.$$

We establish this in three steps, namely, we prove that

$$\limsup_{n\to\infty} \sum_{\substack{q\in V^n \text{ is not} \\ (W,n^\alpha)-\text{typical for any } W\in \mathrm{Cos}(V)}} \mathbb{P}(A_n q = r_q) = 0, \tag{4.2}$$

$$\limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q \text{ is } (W,n^\alpha)-\text{typical}, \\ \text{but not } (W,C\log n)-\text{typical}}} \mathbb{P}(A_n q = r_q) = 0, \tag{4.3}$$

$$\limsup_{n\to\infty} \sum_{W\in \mathrm{Cos}(V)} \sum_{\substack{q \text{ is } (W,C\log n)-\text{typical}, \\ \text{but not } (W,0)-\text{typical}}} \mathbb{P}(A_n q = r_q) = 0, \tag{4.4}$$

where C is a constant to be chosen later.

Equations (4.2), (4.3) and (4.4) are proved in Subsections 4.1, 4.3 and 4.4 respectively.

4.1 Proof of Equation (4.2)

The following terminology will be useful for us. With every $(q, d-1)$-tuple $Q = (Q_1, Q_2, \dots, Q_n)$ we associate the random variables $Z \in V$ and $X^Q = (X_1^Q, X_2^Q, \dots, X_{d-1}^Q) \in V^{d-1}$, such that $Z = r_q(i)$ and $X^Q = Q_i$, where i is a uniform random element of the set $\{1, 2, \dots, n\}$. Each X_j^Q has the same distribution as q_i where i is chosen uniformly from $\{1, 2 \dots, n\}$. The random variable $X_\Sigma^Q \in V$ is defined as $X_\Sigma^Q = \sum_{i=1}^{d-1} X_i^Q$. These two sets of $(q, d-1)$-tuples are equal:

$$\{Q \quad | \quad r_q - \Sigma(Q) \sim q\} = \{Q \quad | \quad Z - X_\Sigma^Q \overset{\mathrm{d}}{=} X_1^Q\}.$$

Here $\overset{\mathrm{d}}{=}$ means that the two random variables have the same distribution. Thus,

$$\mathbb{P}\left(r_q - A_n^{(d-1)} q \sim q\right) = \mathbb{P}_{\bar{Q}}\left(Z - X_\Sigma^{\bar{Q}} \overset{\mathrm{d}}{=} X_1^{\bar{Q}}\right),$$

where the subscript in the notation $\mathbb{P}_{\bar{Q}}$ indicates that the probability is over the random choice of $\bar{Q}$.

We call the random variables $Z, X_1, ..., X_{d-1} \in V$ ε-independent, if for every $z, x_1, ..., x_{d-1} \in V$, we have

$$|\mathbb{P}(Z = z, X_1 = x_1, ..., X_{d-1} = x_{d-1}) - \mathbb{P}(Z = z)\mathbb{P}(X_1 = x_1) \cdots \mathbb{P}(X_{d-1} = x_{d-1})| < \varepsilon.$$

CEU eTD Collection

Fix $\frac{1}{2} < \eta < \alpha$. The next lemma follows from Lemma 10.2 and the union bound.

Lemma 4.2. *For any $q \in V^n$, we have*

$$\mathbb{P}_{\bar{Q}}(Z, X_1^{\bar{Q}}, X_2^{\bar{Q}}, \dots, X_{d-1}^{\bar{Q}} \text{ are not } n^{\eta-1}\text{-independent}) \leq |V|^d 2(d-1)\exp\left(-\frac{2n^{2\eta-1}}{(d-1)^2}\right). \quad \square$$

The crucial step in the proof of Equation (4.2) is the following lemma, which is proved in the next subsection.

Lemma 4.3. *Let $d \geq 3$. There is C and $\varepsilon_0 > 0$ (which may depend on d and V), such that the following holds. Assume that $Z, X_1, X_2, ..., X_{d-1}$ are ε-independent V-valued random variables, for some $0 < \varepsilon < \varepsilon_0$. Let $X_\Sigma = X_1 + X_2 + \cdots + X_{d-1}$. Assume that $X_1, X_2, \dots, X_{d-1}$ and $Z - X_\Sigma$ have the same distribution π. Then there is a coset W in V such that $d_\infty(\pi, \pi_W) < C\varepsilon$.*

Here π_W is the uniform distribution on W. For two distribution π and μ on the same finite set $\mathcal{R}$, their distance $d_\infty(\pi, \mu)$ is defined as

$$d_\infty(\pi, \mu) = \max_{r \in \mathcal{R}} |\pi(r) - \mu(r)|.$$

Combining the last lemma with Lemma 4.2, we get the following lemma.

Lemma 4.4. *Assume that n is large enough. Let $q \in V^n$. If*

$$\mathbb{P}\left(r_q - A_n^{(d-1)} q \sim q\right) = \mathbb{P}_{\bar{Q}}\left(Z - X_\Sigma^{\bar{Q}} \overset{\mathrm{d}}{=} X_1^{\bar{Q}}\right) > |V|^d 2(d-1)\exp\left(-\frac{2n^{2\eta-1}}{(d-1)^2}\right),$$

then q is (W, n^α)-typical for some coset W in V. In other words, if q is not (W, n^α)-typical for any coset W, then

$$\mathbb{P}\left(r_q - A_n^{(d-1)} q \sim q\right) = \mathbb{P}_{\bar{Q}}\left(Z - X_\Sigma^{\bar{Q}} \overset{\mathrm{d}}{=} X_1^{\bar{Q}}\right) \leq |V|^d 2(d-1)\exp\left(-\frac{2n^{2\eta-1}}{(d-1)^2}\right).$$

Proof. Combining our assumptions on q with Lemma 4.2, we have

$$\mathbb{P}_{\bar{Q}}\left(Z, X_1^{\bar{Q}}, X_2^{\bar{Q}}, \dots, X_{d-1}^{\bar{Q}} \text{ are } n^{\eta-1}\text{-independent and } Z - X_\Sigma^{\bar{Q}} \overset{\mathrm{d}}{=} X_1^{\bar{Q}}\right) > 0.$$

So there exist $n^{\eta-1}$-independent random variables $Z, X_1, X_2, \dots, X_{d-1}$, such that $X_1, X_2, \dots, X_{d-1}$ and $Z - X_\Sigma = Z - \sum_{i=1}^{d-1} X_i$ all have the same distribution as q_i where i is chosen uniformly from $\{1, 2, ..., n\}$. Let us call this distribution π. For large enough n, we have $n^{\eta-1} < \varepsilon_0$, so Lemma 4.3 can be applied to give us that there is a coset W in V such that $d_\infty(\pi, \pi_W) < Cn^{\eta-1}$. Since $n^\alpha > C|V|n^\eta$, this implies that q is (W, n^α)-typical. $\square$

Now we made all the necessary preparations to prove Equation (4.2).

Due to symmetry if $q_1 \sim q_2$, then $\mathbb{P}(A_n^{(d)} q_1 = r_{q_1}) = \mathbb{P}(A_n^{(d)} q_2 = r_{q_2})$. Let $q^{(d)}$ be a uniform random permutation of q independent from $A_n^{(d-1)}$.

CEU eTD Collection

We have

$$\begin{aligned}\sum_{q'\sim q}\mathbb{P}(A_n^{(d)}q'=r_{q'}) &= |S(q)|\mathbb{P}(A_n^{(d)}q=r_q)\\ &= |S(q)|\mathbb{P}(A_n^{(d-1)}q+q^{(d)}=r_q)\\ &= |S(q)|\sum_{q'\sim q}\mathbb{P}(A_n^{(d-1)}q=r_q-q')\mathbb{P}(q^{(d)}=q')\\ &= \sum_{q'\sim q}\mathbb{P}(A_n^{(d-1)}q=r_q-q')=\mathbb{P}(r_q-A_n^{(d-1)}q\sim q).\end{aligned}$$

Let $T_n \subset V^n$ be such that it contains exactly one element of each equivalence class. Then, assuming that n is large enough, we have

$$\begin{aligned}\sum_{\substack{q\in V^n \text{ is not}\\ (W,n^\alpha)-\text{typical for any } W\in\mathrm{Cos}(V)}} & \mathbb{P}(A_n^{(d)}q=r_q)\\ &= \sum_{\substack{q\in T_n \text{ is not}\\ (W,n^\alpha)-\text{typical for any } W\in\mathrm{Cos}(V)}} \mathbb{P}(r_q-A_n^{(d-1)}q\sim q)\\ &\le |T_n||V|^d 2(d-1)\exp\left(-\frac{2n^{2\eta-1}}{(d-1)^2}\right).\end{aligned}$$

In the last step, we used Lemma 4.4. Equation (4.2) follows from the fact that $|T_n| = o\left(n^{|V|+1}\right) = o\left(\exp\left(\frac{2n^{2\eta-1}}{(d-1)^2}\right)\right)$.

4.2 The proof of Lemma 4.3

Although we will not use the following lemma directly, we include it and its proof, because it contains many ideas, that will occur later, in a much clearer form.

Lemma 4.5. *Let $Z, X_1, X_2, ..., X_{d-1}$ be independent V-valued random variables. Let $X_\Sigma = X_1 + X_2 + \cdots + X_{d-1}$. Assume that $X_1, X_2, \ldots, X_{d-1}$ and $Z - X_\Sigma$ have the same distribution π. Then $\pi = \pi_W$ for some coset W in V.*

Proof. We use discrete Fourier transform, that is, for $\varrho \in \hat{V} = \mathrm{Hom}(V, \mathbb{C}^*)$, we define

$$\hat{\pi}(\varrho) = \sum_{v\in V}\pi(v)\varrho(v)$$

and

$$\hat{\mu}(\varrho) = \sum_{v\in V}\mathbb{P}(Z=v)\varrho(v).$$

CEU eTD Collection

The assumptions of the lemma imply that

$$\hat{\mu}(\varrho)\left(\overline{\hat{\pi}(\varrho)}\right)^{d-1} = \hat{\pi}(\varrho)$$

for every $\varrho \in \hat{V}$. In particular $|\hat{\mu}(\varrho)| \cdot |\hat{\pi}(\varrho)|^{d-1} = |\hat{\pi}(\varrho)|$ for every $\varrho \in \hat{V}$. Since $|\hat{\mu}(\varrho)|, |\hat{\pi}(\varrho)| \leq 1$, this is only possible if $|\hat{\pi}(\varrho)| \in \{0,1\}$ for every $\varrho \in \hat{V}$. Let us define $\hat{V}_1 = \{\varrho \in \hat{V} | \quad |\hat{\pi}(\varrho)| = 1\}$. Note that $\hat{V}_1$ always contains the trivial character. Then for every $\varrho \in \hat{V}_1$, the character ϱ is constant on the support of π. Or in other words, the support of π is contained in $W_\varrho = \varrho^{-1}(\hat{\pi}(\varrho))$, which is a coset of $\ker \varrho$. Therefore, the support of π is contained in the coset $W = \cap_{\varrho \in \hat{V}_1} W_\varrho$. Now we prove that $\hat{\pi}(\varrho) = \hat{\pi}_W(\varrho)$ for every $\varrho \in \hat{V}$, which implies that $\pi = \pi_W$. This is clear for $\varrho \in \hat{V}_1$, so assume that $\varrho \notin \hat{V}_1$, that is, $\hat{\pi}(\varrho) = 0$. This implies that ϱ is not constant on W. So there are $w_1, w_2 \in W$ such that $\varrho(w_1) \neq \varrho(w_2)$. For $w = w_1 - w_2$, we have $\varrho(w) \neq 1$ and $W = w + W$. Thus

$$\begin{aligned} \hat{\pi}_W(\varrho) &= \frac{1}{|W|}\sum_{v \in W} \varrho(v) = \frac{1}{|W|}\sum_{v \in W} \varrho(w+v) \\ &= \frac{1}{|W|}\varrho(w)\sum_{v \in W} \varrho(v) = \varrho(w)\hat{\pi}_W(\varrho). \end{aligned} \tag{4.5}$$

Since $\varrho(w) \neq 1$, this means that $\hat{\pi}_W(\varrho) = 0$. □

Now we turn to the proof of Lemma 4.3.

Proof. Using the notations of the proof of Lemma 4.5, the conditions of the lemma imply that

$$\left|\hat{\pi}(\varrho) - \hat{\mu}(\varrho)\left(\overline{\hat{\pi}(\varrho)}\right)^{d-1}\right| \leq |V|^d \varepsilon$$

for every $\varrho \in \hat{V}$. Using the fact that $|\hat{\mu}(\varrho)| \leq 1$, we obtain

$$\left|\hat{\pi}(\varrho) - \hat{\mu}(\varrho)\left(\overline{\hat{\pi}(\varrho)}\right)^{d-1}\right| \geq |\hat{\pi}(\varrho)| - |\hat{\mu}(\varrho)| \cdot |\hat{\pi}(\varrho)|^{d-1} \geq |\hat{\pi}(\varrho)| - |\hat{\pi}(\varrho)|^{d-1},$$

which gives us $|\hat{\pi}(\varrho)| - |\hat{\pi}(\varrho)|^{d-1} \leq |V|^d \varepsilon$ for every $\varrho \in \hat{V}$.

Consider the $[0,1] \to [0,1]$ function $x \mapsto x - x^{d-1}$, this function only vanishes at 0 and 1. Moreover, the derivative of this function does not vanish at 0 and 1. This implies that there is an $\varepsilon_1 > 0$ and a $C_1 > 0$ such that for every $0 < \varepsilon < \varepsilon_1$ the following holds. For $x \in [0,1]$, if we have $x - x^{d-1} \leq |V|^d \varepsilon$, then either $x < C_1\varepsilon$ or $x > 1 - C_1\varepsilon$. In the rest of the proof, we assume that $\varepsilon < \varepsilon_1$. Then for every $\varrho \in \hat{V}$, we have either $|\hat{\pi}(\varrho)| < C_1\varepsilon$ or $|\hat{\pi}(\varrho)| > 1 - C_1\varepsilon$.

Let $\hat{V}_1 = \{\varrho \in \hat{V} | 1 - C_1\varepsilon < |\hat{\pi}(\varrho)|\}$. Take any $\varrho \in \hat{V}_1$. Set

$$z = \frac{\overline{\hat{\pi}(\varrho)}}{|\hat{\pi}(\varrho)|}.$$

CEU eTD Collection

Choose $\xi_0 = \xi_0(\varrho)$ in the range $R(\varrho)$ of the character ρ, such that $\operatorname{Re} z\xi_0 = \max_{\xi \in R(\varrho)} \operatorname{Re} z\xi$. An elementary geometric argument gives that for $\xi_0 \neq \xi \in R(\varrho)$, we have $\operatorname{Re} z\xi \leq 1 - \delta$, where $\delta = 1 - \cos \frac{\pi}{|V|} > 0$. Clearly $\operatorname{Re} z\xi_0 \leq 1$. Then we have

$$|\hat{\pi}(\varrho)| = z\hat{\pi}(\varrho) = \operatorname{Re} z\hat{\pi}(\varrho) = \sum_{\xi \in R(\varrho)} \pi(\varrho^{-1}(\xi)) \operatorname{Re} z\xi \leq 1 - \left(1 - \pi(\varrho^{-1}(\xi_0))\right)\delta.$$

Thus, $|\hat{\pi}(\varrho)| > 1 - C_1\varepsilon$ implies that for the coset $W_\varrho = \varrho^{-1}(\xi_0)$, we have $\pi(W_\varrho) > 1 - C_1\delta^{-1}\varepsilon$. So the coset $W = \cap_{\varrho \in \hat{V}_1} W_\varrho$ satisfies $\pi(W) > 1 - C_1\delta^{-1}|V|\varepsilon$.

Consider a $\varrho \in \hat{V}_1$. Let $\xi_0 = \xi_0(\varrho)$ be like above. Note that $\varrho(v) = \xi_0$ for any $v \in W_\varrho$. In particular, we have $\hat{\pi}_W(\varrho) = \xi_0$. Thus,

$$\begin{aligned}
|\hat{\pi}_W(\varrho) - \hat{\pi}(\varrho)| &= \left|\xi_0 - \left(\pi(W_\varrho)\xi_0 - \sum_{v \in V \setminus W_\varrho} \pi(v)\varrho(v)\right)\right| \\
&= \left|(1 - \pi(W_\varrho))\xi_0 - \sum_{v \in V \setminus W_\varrho} \pi(v)\varrho(v)\right| \\
&\leq 1 - \pi(W_\varrho) + \sum_{v \in V \setminus W_\varrho} \pi(v) = 2(1 - \pi(W_\varrho)) \leq 2C_1\delta^{-1}\varepsilon.
\end{aligned}$$

Now take $\varrho \in \hat{V} \setminus \hat{V}_1$. We know that $|\hat{\pi}(\varrho)| < C_1\varepsilon$. We claim that ϱ is not constant on W. To show this, assume that ϱ is constant on W, then

$$|\hat{\pi}(\varrho)| \geq \pi(W) - \pi(V \setminus W) \geq 1 - 2C_1\delta^{-1}|V|\varepsilon > C_1\varepsilon$$

provided that ε is small enough, which gives us a contradiction. Using that ϱ is not constant on W, Equation (4.5) gives us $\hat{\pi}_W(\varrho) = 0$. Thus,

$$|\hat{\pi}(\varrho) - \hat{\pi}_W(\varrho)| = |\hat{\pi}(\varrho)| \leq C_1\varepsilon.$$

This gives us that $|\hat{\pi}(\varrho) - \hat{\pi}_W(\varrho)| \leq 2C_1\delta^{-1}\varepsilon$ for any $\varrho \in \hat{V}$. Since the map $\pi \mapsto \hat{\pi}$ is an invertible linear map, there is a constant $L = L_V$ such that $d_\infty(\pi, \pi_W) \leq L \max_{\varrho \in \hat{V}} |\hat{\pi}(\varrho) - \hat{\pi}_W(\varrho)|$. This gives the statement. □

CEU eTD Collection

4.3 Proof of Equation (4.3)

We start by the following lemma.

Lemma 4.6. *There is a C such that if $W \in \operatorname{Cos}(V)$ and $q \in V^n$ is (W, n^α)-typical, but not $(W, C\log n)$-typical, then for a random $(q, d-1)$-tuple $\bar{Q}$, we have*

$$\mathbb{P}(r_q - \Sigma(\bar{Q}) \sim q) \leq n^{-(|V|+1)}.$$

Proof. Let $E = \sum_{c \notin W} m_q(c)$. Since q is (W, n^α)-typical, we have $E \leq n^\alpha$. Assume that $r = \sum_{i=1}^d q^{(i)}$, where $q^{(i)} \sim q$. Note that

$$\{j| \quad r_j \notin dW\} \subset \cup_{i=1}^d \{j| \quad q^{(i)}(j) \notin W\},$$

so $\sum_{c \notin dW} m_r(c) \leq dE$. In particular, this is true for r_q, that is,

$$\sum_{c \notin dW} m_{r_q}(c) \leq dE.$$

Let

$$H_0 = \{j \quad | \quad r_q(j) \notin dW\}.$$

For $i = 1, 2, ..., d-1$, we define the random subset H_i of $\{1, 2, ..., n\}$ using the random $(q, d-1)$-tuple $\bar{Q} = (\bar{q}^{(1)}, \bar{q}^{(2)}, \dots, \bar{q}^{(d-1)})$ as

$$H_i = \{j \quad | \quad \bar{q}^{(i)}(j) \notin W\},$$

and let the random subset $H^* \subset \{1, 2, \dots, n\}$ be defined as

$$H^* = \{j \quad | r_q(j) - \Sigma(\bar{Q})(j) \notin W\}.$$

Then $0 \leq |H_0| \leq dE$ and $|H_1| = |H_2| = ... = |H_{d-1}| = E$. Let

$$B = \{j \quad | \quad j \text{ is contained in exactly one of the sets } H_0, H_1, H_2, ..., H_{d-1}\}.$$

Then $B \subset H^*$, therefore we have

$$\mathbb{P}(r_q - \Sigma(\bar{Q}) \sim q) \leq \mathbb{P}(|H^*| = E) \leq \mathbb{P}(|B| \leq E).$$

We will need the following inequality

$$|B| \geq \sum_{i=0}^{d-1} |H_i| - 2 \sum_{0 \leq i < j \leq d-1} |H_i \cap H_j| \geq (d-1)E - 2 \sum_{0 \leq i < j \leq d-1} |H_i \cap H_j|.$$

The proof of this is straightforward, or see [26, Chapter IV, 5.(c)]. Thus, if $|B| \leq E$, then

$$2 \sum_{0 \leq i < j \leq d-1} |H_i \cap H_j| \geq (d-2)E.$$

So $|H_i \cap H_j| \geq \frac{(d-2)E}{d(d-1)}$ for some $i < j$. Therefore,

$$\mathbb{P}(r_q - \Sigma(Q) \sim q) \leq \mathbb{P}(|B| \leq E) \leq \sum_{0 \leq i < j \leq d-1} \mathbb{P}\left(|H_i \cap H_j| \geq \frac{(d-2)E}{d(d-1)}\right). \tag{4.6}$$

CEU eTD Collection

Lemma 4.7. *There is a constant C such that, for all a, b and E satisfying $C \log n < E < n^{\alpha}$ and $a, b \leq dE$, if A and B are two random subset of $\{1, 2, ..., n\}$ of size a and b respectively chosen independently and uniformly, then*

$$\mathbb{P}\left(|A \cap B| \geq \frac{(d-2)E}{d(d-1)}\right) < n^{-(|V|+1)} \Big/ \binom{d}{2}.$$

Proof. We may assume that n is large enough, because we can always increase C to handle the small values of n. Let $\delta = \frac{(d-2)}{d(d-1)}$. For large enough n, we have $\frac{ab}{n} \leq \frac{\delta}{2}E$. Using Lemma 10.1, we obtain that

$$\begin{aligned}
\mathbb{P}\left(|A \cap B| \geq \frac{(d-2)E}{d(d-1)}\right) &= \mathbb{P}\left(|A \cap B| \geq \delta E\right) \\
&\leq \mathbb{P}\left(\left||A \cap B| - \frac{ab}{n}\right| \geq \frac{\delta}{2}E\right) \leq 2\exp\left(-\frac{\delta^2 E^2}{2a}\right) \\
&\leq 2\exp\left(-\frac{\delta^2 E}{2d}\right) \leq 2\exp\left(-\frac{\delta^2 C \log n}{2d}\right) \\
&= 2n^{-\frac{\delta^2 C}{2d}} < n^{-(|V|+1)} \Big/ \binom{d}{2}
\end{aligned}$$

for large enough C. ☐

Combining this lemma with Inequality (4.6), we get the statement of Lemma 4.6. ☐

Then Equation (4.3) follows, because

$$\begin{aligned}
&\limsup_{n\to\infty} \sum_{W \in \mathrm{Cos}(V)} \sum_{\substack{q \text{ is } (W, n^{\alpha})-\text{typical}, \\ \text{but not } (W, C\log n)-\text{typical}}} \mathbb{P}(A_n^{(d)} q = r_q) \\
&= \limsup_{n\to\infty} \sum_{W \in \mathrm{Cos}(V)} \sum_{\substack{q \in T_n \text{ is } (W, n^{\alpha})-\text{typical}, \\ \text{but not } (W, C\log n)-\text{typical}}} \mathbb{P}(r_q - A_n^{(d-1)} q \sim q) \\
&\leq \limsup_{n\to\infty} |\mathrm{Cos}(V)| \cdot |T_n| n^{-(|V|+1)} = 0.
\end{aligned}$$

4.4 Proof of Equation (4.4)

Since there are only finitely many cosets in V, it is enough to prove that for any coset $W \in \mathrm{Cos}(V)$, we have

$$\lim_{n\to\infty} \sum_{q \in D_W^n} |S(q)| \mathbb{P}(\Sigma(\bar{Q}) = r_q) = 0,$$

where

$$D_W^n = \{q \in T_n \quad | \quad q \text{ is } (W, C\log n) - \text{typical, but not } (W, 0)\text{-typical}\},$$

and $\bar{Q}$ is a random (q, d)-tuple. (Recall that $S(q)$ is the set of permutations of q.)

CEU eTD Collection

Given a $q \in V^n$, a (q,d)-tuple Q or m_Q itself will be called W-decent if for any $u \in W^d$, we have

$$\frac{1+m_{\Sigma(Q)}(u_\Sigma)}{1+m_Q(u)} \leq \log^2 n,$$

and it will be called W-half-decent if $(1+m_{\Sigma(Q)}(u_\Sigma))/(1+m_Q(u)) \leq \log^4 n$. Or even more generally, a non-negative integral vector m indexed by V^d will be called W-half-decent if for every $u \in W^d$, we have

$$\frac{1+m(\tau_\Sigma = u_\Sigma)}{1+m(u)} \leq \log^4 n,$$

where $n = \sum_{t\in V^d} m(t)$.

Lemma 4.8. *For any coset $W \in \mathrm{Cos}(V)$, we have*

$$\limsup_{n\to\infty} \sum_{q\in D_W^n} |S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q) = \limsup_{n\to\infty} \sum_{q\in D_W^n} |S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q \textit{ and } \bar{Q} \textit{ is } W-\textit{decent}).$$

Proof. It is enough to show that if n is large enough, then

$$|S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is not } W-\text{decent}) \leq n^{-(|V|+1)}$$

for every $q \in D_W^n$. Indeed, once we establish this, it follows that

$$\limsup_{n\to\infty} \sum_{q\in D_W^n} |S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is not } W-\text{decent}) \leq \limsup_{n\to\infty} |T_n| n^{-(|V|+1)} = 0,$$

which gives the statement.

Just for this proof (q,h)-tuples and random (q,h)-tuples will be denoted by Q^h and $\bar{Q}^h$, because it will be important to emphasize the value of h. Given any $(q,d-1)$-tuple $Q^{d-1} = (q^{(1)}, q^{(2)}, \dots, q^{(d-1)})$ such that $r_q - \Sigma(Q^{d-1}) \sim q$ the tuple $(q^{(1)}, q^{(2)}, \dots, q^{(d-1)}, r_q - \Sigma(Q^{d-1}))$ will be a (q,d)-tuple and it is denoted by $\mathrm{Ext}(Q^{d-1})$. It is also clear that $\Sigma(\mathrm{Ext}(Q^{d-1})) = r_q$, and for any (q,d)-tuple Q^d such that $\Sigma(Q^d) = r_q$ there is a unique $(q,d-1)$-tuple Q^{d-1} such that $r_q - \Sigma(Q^{d-1}) \sim q$ and $Q^d = \mathrm{Ext}(Q^{d-1})$. Also note that $\mathbb{P}(\bar{Q}^{d-1} = Q^{d-1}) = |S(q)|\mathbb{P}(\bar{Q}^d = Q^d)$.

Therefore, for any $q \in D_W^n$, we have

$$\begin{aligned} &|S(q)|\mathbb{P}(\Sigma(\bar{Q}^d) = r_q \text{ and } \bar{Q} \text{ is not } W-\text{decent}) \\ &\qquad = \mathbb{P}(r_q - \Sigma(\bar{Q}^{d-1}) \sim q \text{ and } \mathrm{Ext}(\bar{Q}^{d-1}) \text{ is not } W-\text{decent}). \end{aligned}$$

The event on the right-hand side is contained in the even that

there are $t \in W^{d-1}$ and $c \in dW$, such that

$$\frac{1+m_{r_q}(c)}{1+|\{i| \quad r_q(i) = c \text{ and } \bar{Q}^{d-1}(i) = t\}|} > \log^2 n. \tag{4.7}$$

This event has probability at most $n^{-(|V|+1)}$ for every $(W, C\log n)$-typical vector $q \in V^n$, if n is large enough. Indeed, for a $c \in dW$ such that $m_{r_q}(c) < \log^2 n$, Inequality (4.7) can not be true.

CEU eTD Collection

On the other hand, if $m_{r_q}(c) \geq \log^2 n$, then with high probability

$$|\{i| \quad r_q(i) = c \text{ and } \bar{Q}^{d-1}(i) = t\}| > \frac{1}{2}\frac{m_{r_q}(c)}{|W|^{d-1}} > \frac{1 + m_{r_q}(c)}{\log^2 n}$$

for any $t \in W^{d-1}$, as it follows from Lemma 10.2. □

As before, we define

$$\mathcal{M}(q, r) = \{m_Q \quad | \quad Q \in \mathcal{Q}_{q,d}, \Sigma(Q) = r\}.$$

Let

$$\mathcal{M}^\sharp(q, r) = \{m \in \mathcal{M}(q, r)| \quad m \text{ is } W-\text{decent}\}.$$

From the previous lemma, we need to prove that

$$\lim_{n\to\infty} \sum_{q\in D_W^n} \sum_{m\in\mathcal{M}^\sharp(q,r_q)} |S(q)|\mathbb{P}((\Sigma(\bar{Q}) = r_q) \wedge (m_{\bar{Q}} = m)) = 0.$$

Let

$$\mathcal{M} = \{m_Q \quad | \quad Q \text{ is a } (q, d)\text{-tuple for some } n \geq 0 \text{ and } q \in V^n\}.$$

The set $\mathcal{M}$ is the set of non-negative integral points of the linear subspace of $\mathbb{R}^{V^d}$ consisting of the vectors m satisfying the following linear equations:

$$m(\tau_i = c) = m(\tau_1 = c)$$

for every $c \in V$ and $i = 1, 2, \ldots, d$.

In other words, $\mathcal{M}$ consists of the integral points of a rational polyhedral cone. From [54, Theorem 16.4], we know that this cone is generated by an integral Hilbert basis, i. e., we have the following lemma.

Lemma 4.9. *There are finitely many vectors $m_1, m_2, ..., m_\ell \in \mathcal{M}$, such that*

$$\mathcal{M} = \{c_1m_1 + c_2m_2 + \cdots + c_\ell m_\ell \quad | \quad c_1, c_2, \ldots, c_\ell \text{ are non-negative integers}\}. \qquad \square$$

We may assume that the indices in the lemma above are chosen such that there is an h such that the supports of $m_1, m_2, \ldots, m_h$ are contained in W^d, and the supports of $m_{h+1}, m_{h+2}, ..., m_\ell$ are not contained in W^d.

Definition 4.10. Given a vector $m \in \mathcal{M}$, write m as $m = \sum_{i=1}^{\ell} c_i m_i$, where $c_1, c_2, ..., c_\ell$ are non-negative integers, and let $\Delta(m) = \sum_{i=h+1}^{\ell} c_i m_i$. (If the decomposition of m is not unique just pick and fix a decomposition.)

With the notation $\|m\|_{W^C} = m(\tau \notin W^d)$, we have $\|m\|_{W^C} = \|\Delta(m)\|_{W^C}$ and $\|m - \Delta(m)\|_{W^C} = 0$.

CEU eTD Collection

For any non-negative integral vector $m \in \mathbb{R}^{V^d}$, we define

$$E(m) = \frac{\prod_{c\in V} m(\tau_\Sigma = c)!}{\prod_{t\in V^d} m(t)!}\left(\prod_{i=1}^{d}\frac{\prod_{c\in V} m(\tau_i = c)!}{m(V^d)!}\right)^{\frac{d-1}{d}}. \tag{4.8}$$

Lemma 4.11. *For every $q, r \in V^n$ and $m \in \mathcal{M}(q,r)$, we have*

$$|S(q)|\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)) = \frac{\prod_{c\in V} m_r(c)!}{\prod_{t\in V^d} m(t)!}\Big/\left(\frac{n!}{\prod_{c\in V} m_q(c)!}\right)^{d-1} = E(m).$$

Proof. The first equality is a consequence of Lemma 3.1. To prove the second equality, note that since $m \in \mathcal{M}(q,r)$, for any $c \in V$ and $i \in \{1,2,\dots,d\}$, we have $m_q(c) = m(\tau_i = c)$. By taking factorials, we get that $m_q(c)! = m(\tau_i = c)!$. Multiplying all these equations, we get that

$$\prod_{i=1}^{d}\prod_{c\in V} m(\tau_i = c)! = \left(\prod_{c\in V} m_q(c)!\right)^{d},$$

that is,

$$\left(\prod_{i=1}^{d}\prod_{c\in V} m(\tau_i = c)!\right)^{\frac{d-1}{d}} = \left(\prod_{c\in V} m_q(c)!\right)^{d-1}.$$

□

Of course there are many other equivalent ways to express the quantity $|S(q)|\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m))$ and each of them suggests a way to extend the formula to all non-negative integral vectors, but the formula given in Equation (4.8) will be useful for us later.

Lemma 4.12. *Consider a non-negative integral W-half-decent vector $m_0 \in \mathbb{R}^{V^d}$, such that $\|m_0\|_{W^C} = O(\log n)$, where $n = \sum_{t\in V^d} m(t)$. For $u \in V^d$, let $\chi_u \in \mathbb{R}^{V^d}$ be such that $\chi_u(u) = 1$ and $\chi_u(t) = 0$ for every $t \neq u \in V^d$.*

- *If $u \in W^d$, then $E(m_0 + \chi_u)/E(m_0) = O(\log^4 n)$;*
- *If $u \notin W^d$, then $E(m_0 + \chi_u)/E(m_0) = O(n^{-(d-2)/d}\log^2 n)$.*

Proof. Let

$$g = \frac{1 + m_0(\tau_\Sigma = u_\Sigma)}{1 + m_0(u)} \qquad \text{and} \qquad f_i = \frac{1 + m_0(\tau_i = u_i)}{n+1}.$$

Note that

$$E(m_0 + \chi_u)/E(m_0) = g \cdot \left(\prod_{i=1}^{d} f_i\right)^{\frac{d-1}{d}}.$$

CEU eTD Collection

If $u \in W^d$, then since m_0 is W-half-decent, we have $g \le \log^4 n$, and clearly $f_i \le 1$, so the statement follows.

If $u \notin W^d$, we consider the following two cases:

1. If $u_\Sigma \notin dW$, then

$$g \le 1 + m_0(\tau_\Sigma = u_\Sigma) \le 1 + \|m_0\|_{W^c} = O(\log n),$$

and there is an i such that $u_i \notin W$. This imply that $f_i = O\left(\frac{\log n}{n}\right)$. So

$$E(m_0+\chi_u)/E(m_0) = O\left(\log n \left(\frac{\log n}{n}\right)^{\frac{d-1}{d}}\right) = O\left(n^{-\frac{d-2}{d}}\log^2 n\right).$$

2. If $u_\Sigma \in W^d$, then there are at least two indices i such that $u_i \notin W$, for such an index i, we have $f_i = O\left(\frac{\log n}{n}\right)$, clearly $g = O(n)$, so

$$E(m_0+\chi_u)/E(m_0) = O\left(n \left(\frac{\log n}{n}\right)^{\frac{2(d-1)}{d}}\right) = O\left(n^{-\frac{d-2}{d}}\log^2 n\right).$$

□

The next lemma follows easily from the previous one.

Lemma 4.13. *There is a D, such that for any $i \in \{h+1, h+2, \dots, \ell\}$ and any non-negative integral W-half-decent vector $m_0 \in \mathbb{R}^{V^d}$, such that $\|m_0\|_{W^C} = O(\log n)$, we have*

$$E(m_0+m_i)/E(m_0) = O\left(\left(n^{-(d-2)/d}\log^D n\right)^{\|m_i\|_{W^C}}\right). \qquad \square$$

Lemma 4.14. *Assume that n is large enough. Let $q \in V^n$ be $(W, C\log n)$-typical, and let $m \in \mathcal{M}^\sharp(q, r_q)$. If m_0 is an integral vector indexed by V^d such that $(m - \Delta(m))(t) \le m_0(t) \le m(t)$ for every $t \in V^d$, then m is W-half-decent.*

Proof. Let $L = \max_{i=h+1}^{\ell} \|m_i\|_\infty$. Note that $m(t) - m'(t) \le L\|m\|_{W^C} \le LC\log n$ for every $t \in V^d$. Let $n_0 = \sum_{t\in V^d} m_0(t)$. Then

$$n_0 \ge n - L\cdot|V|^d\cdot\|m\|_{W^C} \ge n - L|V|^d C\log n.$$

If n is large enough, then $LC\log^3 n \le \frac{1}{2}\log^4 n_0$. We need to prove that

$$\frac{1+m_0(\tau_\Sigma = u_\Sigma)}{1+m_0(u)} \le \log^4 n_0,$$

CEU eTD Collection

for every $u \in W^d$. If $1 + m_0(\tau_\Sigma = u_\Sigma) \leq \log^4 n_0$, then it is clear. Thus, assume that we have $1 + m_0(\tau_\Sigma = u_\Sigma) > \log^4 n_0$. Then,

$$\begin{aligned} 1 + m_0(\tau_\Sigma = u_\Sigma) &\leq 1 + m(\tau_\Sigma = u_\Sigma) \\ &\leq (1 + m(u)) \log^2 n \\ &\leq (1 + m_0(u) + LC \log n) \log^2 n \\ &\leq (1 + m_0(u)) \log^2 n + \frac{1}{2} \log^4 n_0 \\ &\leq (1 + m_0(u)) \log^2 n + \frac{1}{2} \left(1 + m_0(\tau_\Sigma = u_\Sigma)\right). \end{aligned}$$

Therefore, if n is large enough, then we have

$$\frac{1 + m_0(\tau_\Sigma = u_\Sigma)}{1 + m_0(u)} \leq 2 \log^2 n \leq \log^4 n_0.$$

□

The following estimate will be crucial later.

Lemma 4.15. *There is a K such that for any $(W, C\log n)$-typical $q \in V^n$ and $m \in \mathcal{M}^\sharp(q, r_q)$, we have*

$$E(m) \leq \left(K n^{-(d-2)/d} \log^D n\right)^{\|\Delta(m)\|_{W^C}} E(m - \Delta(m)).$$

Proof. We may assume that n is large enough, because we can increase K to handle the small values of n. Then the statement follows from repeated application of Lemma 4.13. Observe that $m - \Delta(m)$ and all other m_0 we need to apply that lemma is W-half-decent by Lemma 4.14. □

Now we made all the necessary preparations to prove Equation (4.4). With our new notations, we have to prove that

$$\lim_{n\to\infty} \sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^\sharp(q, r_q)} E(m) = 0.$$

We prove it by induction on $|V|$. The statement is clear if $W = V$, because in that case D_n^W is empty. So we may assume that $|W| < |V|$.

Lemma 4.16. *There is a finite $B = B_W$ such that for every n, we have that*

$$\sum_{q \in W^n \cap T_n} |S(q)| \mathbb{P}(A_n^{(d)} q = r_q) < B.$$

Proof. First consider the case when the coset W is a subgroup. Then from the induction hypothesis, we can use Theorem 1.5 to get that that

$$\sum_{q \in W^n} \mathbb{P}(A_n^{(d)} q = r_q) = \sum_{q \in W^n} \mathbb{P}(U_{q,d} = r_q) + o(1).$$

CEU eTD Collection

Recall that for $W_0 \in \mathrm{Cos}(W)$, we defined $I(W_0^n)$ as

$$I(W_0^n) = \{q \in W_0^n \quad | \quad \mathrm{MinC}_q = W_0\}.$$

Now, we have

$$\begin{aligned}\sum_{q \in W^n} \mathbb{P}(U_{q,d} = r_q) &= \sum_{W_0 \in \mathrm{Cos}(W)} \sum_{q \in I(W_0^n)} \mathbb{P}(U_{q,d} = r_q) \\ &= \sum_{W_0 \in \mathrm{Cos}(W)} |I(W_0^n)| \cdot |W_0|^{-(n-1)} \leq \sum_{W_0 \in \mathrm{Cos}(W)} |W_0|.\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{q \in W^n \cap T_n} |S(q)| \mathbb{P}(A_n^{(d)} q = r_q) &= \sum_{q \in W^n} \mathbb{P}(A_n^{(d)} q = r_q) \\ &= \sum_{q \in W^n} \mathbb{P}(U_{q,d} = r_q) + o(1) \leq \sum_{W_0 \in \mathrm{Cos}(W)} |W_0| + o(1).\end{aligned}$$

This proves the lemma when W is a subgroup of V. If the coset W is not a subgroup, then we need to use the bijection given in the proof of Lemma 4.1. $\square$

We need a few notations, let

$$\mathcal{M}_n^{\Delta} = \cup_{q \in D_n^W} \{\Delta(m) \quad | \quad m \in \mathcal{M}^{\sharp}(q, r_q)\}.$$

For $m_\Delta \in \mathcal{M}_n^{\Delta}$ let

$$\Delta_n^{-1}(m_\Delta) = \cup_{q \in D_n^W} \{m \in \mathcal{M}^{\sharp}(q, r_q) \quad | \quad \Delta(m) = m_\Delta\}.$$

Using Lemma 4.15, we obtain that

$$\begin{aligned}\sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^{\sharp}(q, r_q)} E(m) &= \sum_{m_\Delta \in \mathcal{M}_n^{\Delta}} \sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m) \leq \\ &\sum_{m_\Delta \in \mathcal{M}_n^{\Delta}} \left(K n^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{WC}} \sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta). \quad (4.9)\end{aligned}$$

Fix a vector $m_\Delta \in \mathcal{M}_n^{\Delta}$. Set $n' = n - \sum_{t \in V^d} m_\Delta(t)$. Let X be the set of $q \in D_n^W$, such that $\mathcal{M}^{\sharp}(q, r_q) \cap \Delta_n^{-1}(m_\Delta)$ is non-empty.

For each $q \in X$, there is a unique $q' \in W^{n'} \cap T_{n'}$ such that for every $c \in V$, we have $m_{q'}(c) = m_q(c) - m_\Delta(\tau_1 = c)$, and a unique $w_q \in W^{n'} \cap T_{n'}$ such that for every $c \in V$, we have $m_{w_q}(c) = m_{r_q}(c) - m_\Delta(\tau_\Sigma = c)$.

CEU eTD Collection

Note that for any $m \in \mathcal{M}^\sharp(q, r_q) \cap \Delta_n^{-1}(m_\Delta)$, we have $m - m_\Delta \in \mathcal{M}(q', w_q)$. Moreover,

$$E(m - m_\Delta) = |S(q')|\mathbb{P}((\Sigma(\bar{Q}) = w_q) \wedge (m_{\bar{Q}} = m - m_\Delta)),$$

where $\bar{Q}$ is a random (q', d) -tuple. The map $m \mapsto m - m_\Delta$ is injective, so it follows that

$$\sum_{m \in \mathcal{M}^\sharp(q,r_q) \cap \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) \leq |S(q')|\mathbb{P}(A_{n'}^{(d)} q' = w_q).$$

Also note that that the map $q \mapsto q'$ is injective. Therefore,

$$\begin{aligned}
\sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) &= \sum_{q \in X} \sum_{m \in \mathcal{M}^\sharp(q,r_q) \cap \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) \\
&\leq \sum_{q \in X} |S(q')|\mathbb{P}(A_{n'}^{(d)} q' = w_q) \\
&\leq \sum_{q' \in W^{n'} \cap T_{n'}} |S(q')|\mathbb{P}(A_{n'}^{(d)} q' = r_{q'}) < B.
\end{aligned}$$

Thus, continuing Inequality (4.9), we have

$$\sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^\sharp(q,r_q)} E(m) \leq B \sum_{m_\Delta \in \mathcal{M}_n^\Delta} \left(Kn^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{W^C}}.$$

There is an F such that $|\mathcal{M}_n^\Delta| \leq n^F$. We choose a constant G such that for a large enough n, we have $\left(Kn^{-(d-2)/d} \log^{d-1} n\right)^{\|m_\Delta\|_{W^C}} < n^{-(F+1)}$, whenever $\|m_\Delta\|_{W^C} \geq G$. Let H be the cardinality of the set

$$\{m \quad | \quad m = \sum_{i=h+1}^{\ell} c_i m_i, \quad c_{h+1}, c_{h+2}, \dots, c_\ell \text{ non-negative integers}, \|m\|_{W^c} < G\}.$$

Note that $H \leq G^{\ell-h}$. Finally observe that $\|m_\Delta\|_{W^C} \geq 1$ for all $m_\Delta \in \mathcal{M}_n^\Delta$. So for large enough n

$$\begin{aligned}
&B \sum_{m_\Delta \in \mathcal{M}_n^\Delta} \left(Kn^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{W^C}} \\
&= B \sum_{\substack{m_\Delta \in \mathcal{M}_n^\Delta \\ \|m_\Delta\|_{W^C} \geq G}} \left(Kn^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{W^C}} \\
&\quad + B \sum_{\substack{m_\Delta \in \mathcal{M}_n^\Delta \\ \|m_\Delta\|_{W^C} < G}} \left(Kn^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{W^C}} \\
&\leq Bn^F n^{-(F+1)} + BHKn^{-(d-2)/d} \log^D n = o(1).
\end{aligned}$$

CEU eTD Collection

Thus, we have proved Equation (4.4).

5 The connection between the mixing property of the adjacency matrix and the sandpile group

The random $(n-1) \times (n-1)$ matrix A'_n is obtained from A_n by deleting its last row and last column. For $q \in V^{n-1}$, the subgroup generated by $q_1, q_2, \dots, q_{n-1}$ is denoted by G_q. Let U_q be a uniform random element of G_q^{n-1}. The next corollary of Theorem 1.5 states that the distribution of $A'_n q$ is close to that of U_q.

Corollary 5.1. *We have*

$$\lim_{n\to\infty} \sum_{q \in V^{n-1}} d_\infty(A'_n q, U_q) = 0.$$

Proof. For $q \in V^{n-1}$ and $r \in G_q^{n-1}$, we define $\bar{q} = (q_1, q_2, \dots, q_{n-1}, 0) \in V^n$ and $\bar{r} = (r_1, r_2, \dots, r_{n-1}, d \cdot s(q) - s(r)) \in G_q^n$.

Note that $s(\bar{r}) = d \cdot s(q) = d \cdot s(\bar{q})$ and $\mathrm{MinC}_{\bar{q}} = G_q$, so $\bar{r} \in R(\bar{q}, d)$. Moreover, $A'_n q = r$ if and only if $A_n \bar{q} = \bar{r}$, so $\mathbb{P}(A'_n q = r) = \mathbb{P}(A_n \bar{q} = \bar{r})$. From these observations, it follows easily that $d_\infty(A'_n q, U_q) = d_\infty(A_n \bar{q}, U_{\bar{q},d})$. The rest of the proof follows from Theorem 1.5. $\square$

Recall that the reduced Laplacian Δ_n of D_n was defined as $\Delta_n = A'_n - dI$. The next well-known proposition connects $\mathrm{Hom}(\Gamma_n, V)$ and $\mathrm{Sur}(\Gamma_n, V)$ with the kernel of Δ_n when Δ_n acts on V^{n-1}.

Proposition 5.2. *For any finite abelian group V, we have*

$$|\mathrm{Hom}(\Gamma_n, V)| = |\{q \in V^{n-1} \quad | \quad \Delta_n q = 0\}|$$

and

$$|\mathrm{Sur}(\Gamma_n, V)| = |\{q \in V^{n-1} \quad | \quad \Delta_n q = 0, \quad G_q = V\}|.$$

Proof. There is an obvious bijection between $\mathrm{Hom}(\Gamma_n, V)$ and

$$\{\varphi \in \mathrm{Hom}(\mathbb{Z}^{n-1}, V) | \quad \mathrm{RowSpace}(\Delta_n) \subset \ker \varphi\}.$$

Moreover, any $\varphi \in \mathrm{Hom}(\mathbb{Z}^{n-1}, V)$ is uniquely determined by the vector $q = (\varphi(e_1), \varphi(e_2), \dots, \varphi(e_{n-1})) \in V^{n-1}$, where $e_1, e_2, \dots, e_{n-1}$ is the standard generating set of $\mathbb{Z}^{n-1}$. Furthermore, $\mathrm{RowSpace}(\Delta_n) \subset \ker \varphi$ if and only if $\Delta_n q = 0$, so the first statement follows. The second one can be proved similarly. $\square$

CEU eTD Collection

Combining Proposition 2.1 with with Corollary 5.1, we obtain

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}|\operatorname{Sur}(\Gamma_n,V)| &= \lim_{n\to\infty}\sum_{\substack{q\in V^{n-1}\\ G_q=V}}\mathbb{P}(\Delta_n q=0)=\lim_{n\to\infty}\sum_{\substack{q\in V^{n-1}\\ G_q=V}}\mathbb{P}(A'_n q=dq)\\ &= \lim_{n\to\infty}\sum_{\substack{q\in V^{n-1}\\ G_q=V}}\mathbb{P}(U_q=dq)\\ &= \lim_{n\to\infty}|\{q\in V^{n-1}|\quad G_q=V\}|\cdot|V|^{-(n-1)}=1.\end{aligned}$$

This proves Theorem 1.3.

To obtain Theorem 1.1 from this theorem, we need to use the results of Wood on the moment problem.

Theorem 5.3. *(Wood [60, Theorem 3.1] or [58, Theorem 8.3]) Let X_n and Y_n be sequences of random finitely generated abelian groups. Let a be a positive integer and A be the set of (isomorphism classes of) abelian groups with exponent dividing a. Suppose that for every $G\in A$, we have a number $M_G\le|\wedge^2 G|$ such that*

$$\lim_{n\to\infty}\mathbb{E}|\operatorname{Sur}(X_n,G)|=M_G,$$

and

$$\lim_{n\to\infty}\mathbb{E}|\operatorname{Sur}(Y_n,G)|=M_G.$$

Then for every $H\in A$, the limits

$$\lim_{n\to\infty}\mathbb{P}(X_n\otimes\mathbb{Z}/a\mathbb{Z}\simeq H)\quad\textit{and}\quad\lim_{n\to\infty}\mathbb{P}(Y_n\otimes\mathbb{Z}/a\mathbb{Z}\simeq H)$$

exist, and they are equal.

This has the following consequence.

Theorem 5.4. *Let $p_1,p_2,\dots,p_s$ be distinct primes. Let X_n and Y_n be sequences of random finitely generated abelian groups. Assume that for any finite abelian group G, we have a number $M_G\le|\wedge^2 G|$ such that*

$$\lim_{n\to\infty}\mathbb{E}|\operatorname{Sur}(X_n,G)|=M_G,$$

and

$$\lim_{n\to\infty}\mathbb{E}|\operatorname{Sur}(Y_n,G)|=M_G.$$

Let $X_{n,i}$ (resp. $Y_{n,i}$) be the p_i-Sylow subgroup of X_n (resp. Y_n). For $i=1,2,\dots,s$, let G_i be a finite abelian p_i-group. Then the limits

$$\lim_{n\to\infty}\mathbb{P}\left(\bigoplus_{i=1}^s X_{n,i}\simeq\bigoplus_{i=1}^s G_i\right)\quad\textit{and}\quad\lim_{n\to\infty}\mathbb{P}\left(\bigoplus_{i=1}^s Y_{n,i}\simeq\bigoplus_{i=1}^s G_i\right)$$

exist, and they are equal.

CEU eTD Collection

Proof. Let a_0 be the exponent of the group $\bigoplus_{i=1}^s G_i$. Let $a = a_0 \cdot \prod_{i=1}^s p_i$. Observe that $\bigoplus_{i=1}^s X_{n,i} \simeq \bigoplus_{i=1}^s G_i$ if and only if $X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq \bigoplus_{i=1}^s G_i$. Thus, the previous theorem gives the statement. □

The next theorem gives two special cases which are of particular interest for us.

Theorem 5.5. *Let $p_1, p_2, \dots, p_s$ be distinct primes. Let Γ_n be sequence of random finitely generated abelian groups. Let $\Gamma_{n,i}$ be the p_i-Sylow subgroup of Γ_n.*

1. *Assume that for any finite abelian group V, we have*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\Gamma_n, V)| = 1.$$

For $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Then

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^s \Gamma_{n,i} \simeq \bigoplus_{i=1}^s G_i\right) = \prod_{i=1}^s \left(|\operatorname{Aut}(G_i)|^{-1} \prod_{j=1}^\infty (1 - p_i^{-j})\right).$$

2. *Assume that for any finite abelian group V, we have*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\Gamma_n, V)| = |\wedge^2 V|.$$

For $i = 1, 2, \dots, s$, let G_i be a finite abelian p_i-group. Then

$$\lim_{n\to\infty} \mathbb{P}\left(\bigoplus_{i=1}^s \Gamma_{n,i} \simeq \bigoplus_{i=1}^s G_i\right) =$$
$$\prod_{i=1}^s \left(\frac{|\{\phi : G_i \times G_i \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G_i||\operatorname{Aut}(G_i)|} \prod_{j=0}^\infty (1 - p_i^{-2j-1})\right).$$

Proof. The first part follows from the previous theorem and [60, Lemma 3.2] with the choice of $u = 0$. Or alternatively, we can use the results of [24, Section 8]. The second part follows from the previous theorem and [18, Theorem 2 and Theorem 11]. See also the proof of Corollary 9.2 in [58]. □

Combining the first statement of the previous theorem with Theorem 1.3, we obtain Theorem 1.1. The proofs of the corresponding statements about the sandpile group of H_n are postponed to Section 7 and 8.

CEU eTD Collection

6 A version of Theorem 1.5 with uniform convergence

We sate our results for the directed random graph model, but the arguments can be repeated for the undirected model as well. We write $A_n^{(d)}$ in place of A_n to emphasize the dependence on d. We start by a simple lemma.

Lemma 6.1. *For a fixed n and $q \in V^n$, we have*

$$d_\infty(A_n^{(d)} q, U_{q,d}) \leq d_\infty(A_n^{(d-1)} q, U_{q,d-1}).$$

Proof. Take any $r \in R(q,d)$. Observe that for $q' \sim q$, we have $r - q' \in R(q, d-1)$. Let q' be a uniform random element of $S(q)$ independent from $A_n^{(d-1)}$, then

$$\begin{aligned} |\mathbb{P}(A_n^{(d)} q = r) - \mathbb{P}(U_{q,d} = r)| &= |\mathbb{E}\mathbb{P}(A_n^{(d-1)} q = r - q') - |R(q,d)|^{-1}| \\ &\leq \mathbb{E}|\mathbb{P}(A_n^{(d-1)} q = r - q') - |R(q,d-1)|^{-1}| \\ &\leq d_\infty(A_n^{(d-1)} q, U_{q,d-1}). \end{aligned}$$

Note that here the expectations are over the random choice of q'. Since this is true for any $r \in R(q,d)$, the statement follows. □

Using this we can deduce the following uniform version of Theorem 1.5.

Corollary 6.2. *We have*

$$\lim_{n\to\infty} \sup_{d\geq 3} \sum_{q \in V^n} d_\infty(A_n^{(d)} q, U_{q,d}) = 0.$$ □

This also implies a uniform version of Corollary 5.1. Therefore, the limits in Theorem 1.3 are uniform in d. Consequently, Theorem 1.1 remains true if we allow d to vary with n.

7 Sum of matching matrices: Modifications of the proofs

A fixed point free permutation of order 2 is called a matching permutation. The permutation matrix of a matching permutation is called matching matrix. Then $C_n = M_1 + M_2 + \cdots + M_d$, where $M_1, M_2, \ldots, M_d$ are independent uniform random $n \times n$ matching matrices.

Consider a vector $q = (q_1, q_2, ..., q_n) \in V^n$. For a matching permutation π of the set $\{1, 2, \ldots, n\}$ the vector $q_\pi = (q_{\pi(1)}, q_{\pi(2)}, \ldots, q_{\pi(n)})$ is called a matching permutation of q. A random matching permutation of q is defined as the random variable q_π, where π is chosen uniformly from the set of all matching permutations.

A $(q,1,h)$-tuple is a $1+h$-tuple $Q = (q^{(0)}, q^{(1)}, \ldots, q^{(h)})$, where $q^{(0)} = q$ and $q^{(1)}, q^{(2)}, \ldots, q^{(h)}$ are matching permutations of q. A random $(q,1,h)$-tuple is a tuple $\bar{Q} = (\bar{q}^{(0)}, \bar{q}^{(1)}, \ldots \bar{q}^{(h)})$, where $\bar{q}^{(0)} = q$ and $\bar{q}^{(1)}, \bar{q}^{(2)}, \ldots, \bar{q}^{(h)}$ are independent random matching permutations of q. Similarly

CEU eTD Collection

as before, a $(q, 1, h)$-tuple can be viewed as a vector $Q = (Q_1, Q_2, \ldots, Q_n)$ in $(V^{1+h})^n$. For $t \in V^{1+h}$, we define

$$m_Q(t) = |\{i \quad | \quad Q_i = t\}|.$$

In this section the components of a vector $t \in V^{1+h}$ are indexed from 0 to h, that is, $t = (t_0, t_1, \ldots, t_h)$. For $t \in V^{1+h}$, we define $t_\Sigma = \sum_{i=1}^n t_i$. The sum $\Sigma(Q)$ of a $(q, 1, h)$-tuple Q is defined as $\Sigma(Q) = \sum_{i=1}^h q^{(i)}$. Note that the sums above do not include t_0 and $q^{(0)}$.

We define

$$\mathcal{M}^S(q, r) = \{m_Q | \quad Q \text{ is a } (q, 1, h)\text{-tuple such that } \Sigma(Q) = r\}.$$

A $(q, 1, h)$-tuple Q is γ-typical if $\left\| m_Q - \frac{n}{|V|^{1+h}} \mathbb{1} \right\|_\infty < n^\gamma$.

For two vectors $q, r \in V^n$ and $a, b \in V$, we define

$$m_{q,r}(a, b) = |\{i| \quad q_i = a \text{ and } r_i = b\}|.$$

The vector r is called (q, β)-typical if

$$\left\| m_{q,r} - \frac{n}{|V|^2} \mathbb{1} \right\|_\infty < n^\beta.$$

With these notations, we have the following analogue of Theorem 2.3.

Theorem 7.1. *For any fixed finite abelian group V and $h \geq 2$, we have*

$$\lim_{n \to \infty} \sup_{\substack{q \in V^n \quad \alpha-typical \\ r \in R^S(q,h) \quad (q,\beta)-typical}} \left| \mathbb{P}(C_n^{(h)} q = r) \Big/ \left(\frac{2^{\mathrm{Rank}_2(V)} | \wedge^2 V|}{|V|^{n-1}} \right) - 1 \right| = 0.$$

Proof. The proof is analogous with the proof of Theorem 2.3. We need to replace the notion of (q, h)-tuple with the notion of $(q, 1, h)$-tuple, the notion of β-typical vector with the notion of (q, β)-typical vector. Moreover, some of the statements should be slightly changed. Now we list the modified statements.

We start by determining the size of $R^S(q, h)$.

Lemma 7.2. *Let $q \in V^n$ such that* $\mathrm{MinC}_q = V$*, then*

$$|R^S(q, h)| = \frac{|V|^{n-1}}{2^{\mathrm{Rank}_2(V)} | \wedge^2 V|}.$$

Proof. We define the homomorphism $\varphi : V^n \to (V \otimes V) \times V$ by setting

$$\varphi(r) = (< q \otimes r >, s(r))$$

CEU eTD Collection

for every $r \in V^n$. We claim that it is surjective. First, take any $a, b \in V$. The condition $\mathrm{MinC}_q = V$ implies that $q_1 - q_n, q_2 - q_n, \dots, q_{n-1} - q_n$ generate V. In particular, there are integers $c_1, c_2, \dots, c_{n-1}$ such that $a = \sum_{i=1}^{n-1} c_i(q_1 - q_n)$. Let us define

$$r = (c_1 b, c_2 b, \dots, c_{n-1} b, -\sum_{i=1}^{n-1} c_i b) \in V^n$$

.

Then

$$< q \otimes r >= \sum_{i=1}^{n-1} q_i \otimes c_i b + q_n \otimes \left(-\sum_{i=1}^{n-1} c_i b \right) = \left(\sum_{i=1}^{n-1} c_i (q_i - q_n) \right) \otimes b = a \otimes b,$$

and $s(r) = 0$, that is, $\varphi(r) = (a \otimes b, 0)$. Thus, $V \otimes V \times \{0\}$ is contained in the range of φ.

Now take any $(x, v) \in (V \otimes V) \times V$. Clearly, we can pick an $r_1 \in V^n$ such that $s(r_1) = v$. Then from the previous paragraph, there is an r_2 such that $\varphi(r_2) = (x- < q \otimes r_1 >, 0)$. Then $\varphi(r_1 + r_2) = (x, v)$. This proves that φ is indeed surjective. Since $R^S(q, h) = \varphi^{-1}(I_2 \times \{h \cdot s(q)\})$, we have

$$|R^S(q, h)| = \frac{|I_2|}{|(V \otimes V)| \cdot |V|} |V|^n = \frac{|V|^{n-1}}{2^{\mathrm{Rank}_2(V)} | \wedge^2 V|}.$$

□

Lemma 7.3 (The analogue of Lemma 3.1)**.** *Consider $q, r \in V^n$. Let $m \in \mathcal{M}^S(q, r)$. Then m is a nonnegative integral vector with the following properties.*

$$m(\tau_0 = a \text{ and } \tau_i = b) = m(\tau_0 = b \text{ and } \tau_i = a) \qquad \forall i \in \{1, 2, \dots, h\}, \quad a, b \in V, \tag{7.1}$$

$$m(\tau_0 = a \text{ and } \tau_\Sigma = b) = m_{q,r}(a, b) \qquad \forall a, b \in V. \tag{7.2}$$

Moreover,

$$m(\tau_0 = c \text{ and } \tau_i = c) \text{ is even} \qquad \forall i \in \{1, 2, \dots, h\}, \quad c \in V. \tag{7.3}$$

Now assume that m is a nonnegative integral vector satisfying the conditions above. Then

$$\mathbb{P}(\Sigma(\bar{Q}) = r \text{ and } m_{\bar{Q}} = m) = \left(\frac{n!}{2^{n/2}(n/2)!} \right)^{-h} \frac{\prod_{a,b \in V} m(\tau_0 = a, \tau_\Sigma = b)!}{\prod_{t \in V^{1+h}} m(t)!} \times$$
$$\prod_{i=1}^{h} \left(\left(\prod_{a \in V} \frac{m(\tau_i = a, \tau_0 = a)!}{2^{m(\tau_i = a, \tau_0 = a)/2} (m(\tau_i = a, \tau_0 = a)/2)!} \right) \left(\prod_{a \neq b \in V} \sqrt{m(\tau_0 = a, \tau_i = b)!} \right) \right). \tag{7.4}$$

CEU eTD Collection

In particular, $\mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m)) > 0$ *so* $m \in \mathcal{M}^S(q,r)$*. Let* $A^S(q,r)$ *be the affine subspace given by the linear equations (7.1) and (7.2) above. Then* $\mathcal{M}^S(q,r)$ *is the set of non-negative integral points of the affine subspace* $A^S(q,r)$ *satisfying the parity constraints in (7.3) above.*

Proof. We only give the proof of Equation (7.4), since all the other statements of the lemma are straightforward to prove. The number of $(q,1,h)$-tuples Q such that $\Sigma(Q) = r$ and $m_Q = m$ is

$$\frac{\prod_{a,b\in V} m(\tau_0 = a, \tau_\Sigma = b)!}{\prod_{t\in V^{1+d}} m(t)!}.$$

Fix any $(q,1,h)$-tuple $Q = (q^{(0)}, q^{(1)}, \ldots, q^{(h)})$ such that $\Sigma(Q) = r$ and $m_Q = m$. Now, we calculate the probability that $\mathbb{P}(\bar{Q} = Q)$ for a random $(q,1,h)$-tuple $\bar{Q}$. For $i \in \{1,2,\ldots,h\}$ and $a,b \in V$, we define

$$I_{i,a,b} = \{j \in \{1,2,\ldots,n\} \quad | \quad q_j^{(i)} = a \text{ and } q_j^{(0)} = b\}.$$

First, for $i = 1,2,\ldots,h$, we determine the number of matching permutations π such that $q_\pi = q^{(i)}$. In other words, we are interested in the number of perfect matchings M on the set $\{1,2,\ldots,n\}$ such that

1. For every $a \in V$, the restriction of M to the set $I_{i,a,a}$ is a perfect matching.
2. For every unordered pair $\{a,b\} \subset V$, where $a \neq b$, the restriction of M gives a perfect matching between the disjoint set $I_{i,a,b}$ and $I_{i,b,a}$.

Since $|I_{i,a,a}| = m(\tau_i = a, \tau_0 = a)$, we have

$$\frac{m(\tau_i = a, \tau_0 = a)!}{2^{m(\tau_i=a,\tau_0=a)/2}(m(\tau_i = a, \tau_0 = a)/2)!}$$

perfect matchings on the set $I_{i,a,a}$.

For every unordered pair $\{a,b\} \subset V$, where $a \neq b$, let

$$n_{i,\{a,b\}} = m(\tau_i = a, \tau_0 = b) = m(\tau_i = b, \tau_0 = a)$$

be the common size of $I_{i,a,b}$ and $I_{i,b,a}$. Then there are

$$n_{i,\{a,b\}}! = \sqrt{m(\tau_i = a, \tau_0 = b)!} \cdot \sqrt{m(\tau_i = a, \tau_0 = b)!}$$

perfect matchings between $I_{i,a,b}$ and $I_{i,b,a}$. We choose to express $n_{i,\{a,b\}}!$ as above, because this way we get a symmetric expression.

CEU eTD Collection

Since the total number perfect matchings is $\frac{n!}{2^{n/2}(n/2)!}$, we obtain that for a uniform random matching matrix M, we have

$$\mathbb{P}(Mq = q^{(i)}) = \left(\frac{n!}{2^{n/2}(n/2)!}\right)^{-1}$$
$$\times \left(\prod_{a\in V} \frac{m(\tau_i = a, \tau_0 = a)!}{2^{m(\tau_i=a,\tau_0=a)/2}(m(\tau_i = a, \tau_0 = a)/2)!}\right)\left(\prod_{a\neq b\in V} \sqrt{m(\tau_0 = a, \tau_i = b)!}\right).$$

From this, Equation (7.4) follows easily. □

Lemma 7.4 (The analogue of Lemma 3.2)**.** *For any $q, r_1, r_2 \in V^n$, we define the vector $v = v_{q,r_1,r_2} \in \mathbb{R}^{V^{1+h}}$ by*
$$v(t) = \frac{m_{q,r_2}(t_0, t_\Sigma) - m_{q,r_1}(t_0, t_\Sigma)}{|V|^{h-1}}$$
for every $t \in V^{1+h}$. Then we have

$$A^S(q, r_1) + v_{q,r_1,r_2} = A^S(q, r_2).$$ □

Lemma 7.5 (The analogue of Lemma 3.4)**.** *Assume that n is large enough. For an α-typical vector $q \in V^n$ and $r \in R^S(q, h)$, the affine subspace $A^S(q, r)$ contains an integral vector satisfying the parity constraints in (7.3) of Lemma 7.3.*

To prove Lemma 7.5 we need a few lemmas. The group V has a decomposition $V = \bigoplus_{i=1}^{\ell} < v_i >$ such that $o_1|o_2|\cdots|o_\ell$, where o_i is order of v_i.

Lemma 7.6. *Let $q \in V^n$ be such that $m_q(v_i) > 0$ for every $1 \leq i \leq \ell$. Let $r \in V^n$ such that $< q\otimes r >\in I_2$. Then there is a symmetric matrix A over $\mathbb{Z}$ such that $r = Aq$ and all the diagonal entries of A are even.*

Proof. We express q_k as $q_k = \sum_{i=1}^{\ell} q_k(i)v_i$, and similarly we express r_k as $r_k = \sum_{i=1}^{\ell} r_k(i)v_i$, where $q_k(i), r_k(i) \in \mathbb{Z}$. The condition that $< q \otimes r >\in I_2$ is equivalent to the following. For $1 \leq i \leq j \leq \ell$, we have

$$\sum_{k=1}^{n} q_k(i)r_k(j) \equiv \sum_{k=1}^{n} q_k(j)r_k(i) \pmod{o_i} \tag{7.5}$$

and whenever o_i is even, we have

$$\sum_{k=1}^{n} q_k(i)r_k(i) \text{ is even.} \tag{7.6}$$

CEU eTD Collection

Due to symmetries and the fact that $m_q(v_i) > 0$ for every $1 \leq i \leq \ell$, we may assume that $q_i = v_i$ for $1 \leq i \leq \ell$. We define the symmetric matrix $A = (a_{ij})$ by

$$a_{ij} = \begin{cases} r_i(j) & \text{for } \ell < i \leq n \text{ and } 1 \leq j \leq \ell, \\ r_j(i) & \text{for } 1 \leq i \leq \ell \text{ and } \ell < j \leq n, \\ 0 & \text{for } \ell < i \leq n \text{ and } \ell < j \leq n, \\ r_i(j) + r_j(i) - \sum_{k=1}^n q_k(j) r_k(i) & \text{for } 1 \leq i \leq j \leq \ell, \\ r_i(j) + r_j(i) - \sum_{k=1}^n q_k(i) r_k(j) & \text{for } 1 \leq j < i \leq \ell. \end{cases}$$

From Equation (7.5) we obtain that for $1 \leq j < i \leq \ell$, we have

$$a_{ij} \equiv r_i(j) + r_j(i) - \sum_{k=1}^n q_k(j) r_k(i) \pmod{o_j}.$$

In particular, $a_{ij} q_j = a_{ij} v_j = (r_i(j) + r_j(i)) v_j - \sum_{k=1}^n q_k(j) r_k(i) v_j$ for every $1 \leq i, j \leq \ell$.

Let $w = Aq$. We need to prove that $w_i = r_i$ for every $1 \leq i \leq n$. It is easy to see for $i > \ell$. Now assume that $i \leq \ell$. Then

$$\begin{aligned} w_i &= \sum_{h=1}^{\ell} \sum_{j=1}^{n} a_{ij} q_j(h) v_h = \sum_{h=1}^{\ell} \left(a_{ih} v_h + \sum_{j=\ell+1}^{n} r_j(i) q_j(h) v_h \right) \\ &= \sum_{h=1}^{\ell} \left(r_i(h) + r_h(i) - \sum_{k=1}^{n} q_k(h) r_k(i) + \sum_{j=\ell+1}^{n} r_j(i) q_j(h) \right) v_h \\ &= \sum_{h=1}^{\ell} \left(r_i(h) + r_h(i) - \sum_{k=1}^{\ell} q_k(h) r_k(i) \right) v_h = \sum_{h=1}^{\ell} r_i(h) v_h = r_i. \end{aligned}$$

Now we modify A slightly to achieve that all the diagonal entries are even. If $i > \ell$, then $a_{ii} = 0$ which is even. If $1 \leq i \leq \ell$ and o_i is even, then $a_{ii} = 2r_i(i) - \sum_{k=1}^n q_k(i) r_k(i)$, which is even using the condition (7.6) above. If $1 \leq i \leq \ell$, o_i is odd and a_{ii} is odd, we replace a_{ii} by $a_{ii} + o_i$, this way we can achieve that a_{ii} is even, without changing Aq. To see this, observe that $o_i q_i = o_i v_i = 0$. □

For $q, w \in V^n$ and $c \in V$, we define

$$z_{q,w}(c) = \sum_{\substack{1 \leq i \leq n \\ q_i = c}} w_i.$$

Note that $< q \otimes w >= \sum_{c \in V} c \otimes z_{q,w}(c)$.

Lemma 7.7. *Let $q \in V^n$ such that $m_q(c) > 10|V|^2$ for every $c \in V$, and let $z \in V^V$. Then there is an matching permutation w of q such that $z_{q,w} = z$, if and only if*

$$\sum_{c \in V} z(c) = s(q) \tag{7.7}$$

CEU eTD Collection

and

$$\sum_{c\in V} c\otimes z(c)\in I_2. \tag{7.8}$$

Proof. It is clear that the conditions are indeed necessary, so we only need to prove the other direction. Since $m_q(c)>0$ for all $c\in V$, we can find a w_0 such that $z_{q,w_0}=z$. (Of course w_0 is not necessarily a matching permutation of q.) Condition (7.8) gives us that $< q\otimes w_0 >\in I_2$. Using Lemma 7.6, it follows that there is a symmetric matrix $A=(a_{ij})$, such that $Aq=w_0$ and all the diagonal entries of A are even. For $a,b\in V$ we define

$$m_0(a,b)=\sum_{\substack{1\le i,j\le n\\ q_i=a,\quad q_j=b}} a_{ij}.$$

Since A is symmetric and the diagonal entries are even, we have $m_0(a,b)=m_0(b,a)$ and $m(a,a)$ is even for every $a,b\in V$.

Let $m=m_0$. Replace $m(a,b)$ by $m(a,b)-2\ell|V|$, where ℓ is an integer chosen such that $0\le m(a,b)-\ell 2|V|<2|V|$. Now for every $0\neq a\in V$, we do the following procedure. We find the unique integer ℓ such that for

$$\Delta=m_q(a)-\sum_{b\in V} m(a,b)-\ell 2|V|,$$

we have $0\le\Delta<2|V|$. Now increase $m(a,a)$ by $\ell 2|V|$. (Note that ℓ is non-negative because of the condition $m_q(a)>10|V|^2$.) Increase both $m(a,0)$ and $m(0,a)$ by Δ. Finally, let $\Delta_0=m_q(0)-\sum_{b\in V} m(0,b)$, and increase $m(0,0)$ by Δ_0. (Once again Δ_0 is non-negative because of the condition $m_q(a)>10|V|^2$.)

This way we achieved that for every $a\in V$, we have $\sum_{b\in V} m(a,b)=m_q(a)$. It is clear that $m(a,b)$ is a non-negative integer and $m(a,b)=m(b,a)$ for every $a,b\in V$. Moreover, $m(a,a)$ is even for $0\neq a\in V$. It is also true for $a=0$, but this requires some explanation. Indeed, $m(0,0)$ can be expressed as

$$\begin{aligned} m(0,0)&=\sum_{a,b\in V} m(a,b)-2\sum_{\substack{\{a,b\}\\ a\neq b\in V}} m(a,b)-\sum_{0\neq a\in V} m(a,a)\\ &=n-2\sum_{\substack{\{a,b\}\\ a\neq b\in V}} m(a,b)-\sum_{0\neq a\in V} m(a,a). \end{aligned}$$

Here in the last row, every term is even, so $m(0,0)$ is even too. From these observations, it follows that there is an matching permutation w of q such that $m_{q,w}=m$. We will prove that $z_{q,w}=z$. Consider an $0\neq a\in V$. Observe that $m(a,b)\equiv m_0(a,b)$ modulo $|V|$ for $b\neq 0$. Thus,

CEU eTD Collection

$$z_{q,w}(a) = \sum_{\substack{1\le i\le n\\ q_i=a}} w_i = \sum_{b\in V} m_{q,w}(a,b)b = \sum_{b\in V} m_0(a,b)b = \sum_{b\in V} \sum_{\substack{1\le i,j\le n\\ q_i=a,\quad q_j=b}} a_{ij}b$$
$$= \sum_{b\in V} \sum_{\substack{1\le i,j\le n\\ q_i=a,\quad q_j=b}} a_{ij}q_j = \sum_{\substack{1\le i\le n\\ q_i=a}} \sum_{j=1}^{n} a_{ij}q_j = \sum_{\substack{1\le i\le n\\ q_i=a}} w_0(i) = z_{q,w_0}(a) = z(a).$$

Finally

$$z_{q,w}(0) = \sum_{a\in V} z_{q,w}(a) - \sum_{0\ne a\in V} z_{q,w}(a) = \sum_{i=1}^{n} q_i - \sum_{0\ne a\in V} z_{q,w}(a)$$
$$= s(q) - \sum_{0\ne a\in V} z(a) = \sum_{a\in V} z(a) - \sum_{0\ne a\in V} z(a) = z(0),$$

using condition (7.7). □

The proof of Lemma 3.4 also gives us the following statement.

Lemma 7.8. *Let $q_1, q_2, \dots, q_h \in V^n$ and $r \in V^n$. Assume that $\sum_{i=1}^n s(q_i) = s(r)$. Then there is an integral vector m indexed by V^h such that*[6]

$$m(\tau_i = b) = m_{q_i}(b)$$

for every $i = 1, 2, \dots, h$ and $b \in V$, and

$$m(\tau_\Sigma = b) = m_r(b)$$

for every $b \in V$. □

Now we are ready to prove Lemma 7.5.

Proof. Fix an α-typical q, and $r \in R^S(q,h)$. Let W be the set of $z \in V^V$ satisfying the conditions (7.7) and (7.8) of Lemma 7.7. Observe that W is a coset of V^V. Moreover, $r \in R^S(q,h)$ implies that $z_{q,r} \in hW$. Thus, we can find $z_1, z_2, \dots, z_h \in W$ such that $z_{q,r} = \sum_{i=1}^h z_i$. If n is large enough, then for an α-typical q, we have $m_q(c) > 10|V|^2$. By using Lemma 7.7, for each $i \in \{1, 2, \dots, h\}$ we can find a matching permutation w_i of q such that $z_{q,w_i} = z_i$. For $a \in V$, let $w_i^a \in V^{m_q(a)}$ be the vector obtained from w_i by projecting to the coordinates in the set $\{i|\quad q_i = a\}$. Similarly, r^a is obtained from r by projecting to the same set of coordinates. Observe that $\sum_{i=1}^h s(w_i^a) = \sum_{i=1}^h z_i(a) = z_{q,r}(a) = s(r^a)$. Thus, from Lemma 7.8, we obtain an integral vector m^a indexed by V^h such that

$$m^a(\tau_i = b) = m_{w_i^a}(b) = m_{q,w_i}(a,b)$$

[6] Unlike in the rest of this section, here the components of a $t \in V^h$ are indexed from 1 to h.

CEU eTD Collection

for every $i = 1, 2, \dots, h$ and $b \in V$, and

$$m^a(\tau_\Sigma = b) = m_{r^a}(b) = m_{q,r}(a, b)$$

for every $b \in V$.

Then the vector m defined by

$$m((t_0, 1_1, \dots, t_h)) = m^{t_0}((t_1, \dots, t_h))$$

gives us an integral point in $A^S(q, r)$ satisfying the parity constraints in (7.3) of Lemma 7.3. $\square$

Lemma 7.9 (The analogue of Lemma 3.5)**.** *For an α-typical $q \in V^n$, a (q, β)-typical $r \in R^S(q, h)$, $r_0 = r_0(q)$ and $m \in \mathcal{M}^{S*}(q, r_0)$, we have that*

$$\mathbb{P}((\Sigma(\bar{Q}) = r_0) \wedge (m_{\bar{Q}} = m)) \sim \mathbb{P}((\Sigma(\bar{Q}) = r) \wedge (m_{\bar{Q}} = m + \hat{v}_{q,r_0,r}))$$

uniformly.

Proof. For any α-typical $q \in V^n$, (q, β)-typical $r \in R^S(q, h)$ and $m \in \mathcal{M}^{S*}(q, r)$, we have

$$\mathbb{P}(\Sigma(Q) = r \text{ and } m_Q = m) \sim f(q) \exp\left(\frac{1}{2n} B\left(m - \frac{1}{|V|^{h+1}}\mathbb{1}, m - \frac{1}{|V|^{h+1}}\mathbb{1}\right)\right)$$

uniformly, where $f(q)$ is some function of q and the bilinear form $B(x, y)$ is defined as

$$B(x, y) = -|V|^{1+h} \sum_{t \in V^{1+h}} x(t)y(t) + \frac{|V|^2}{2} \sum_{i=1}^{h} \sum_{a,b \in V} x(\tau_0 = a, \tau_i = b)y(\tau_0 = a, \tau_i = b)$$
$$+ |V|^2 \sum_{a,b \in V} x(\tau_0 = a, \tau_\Sigma = b)y(\tau_0 = a, \tau_\Sigma = b).$$

The statement follows from the fact that $v_{q,r_0,r}$ is in the radical of B. $\square$

Lemma 7.10 (The analogue of Lemma 3.9 part (iv))**.** *The following holds*

$$\lim_{n\to\infty} \sup_{\substack{q \in V^n \quad \alpha-typical \\ r \in R^S(q,h) \quad (q,\beta)-typical}} \mathbb{P}\left((\Sigma(\bar{Q}) = r) \wedge (\bar{Q} \textit{ is not } \gamma - \textit{typical})\right) |V|^n = 0.$$

Proof. Take any α-typical $q \in V^n$ and (q, β)-typical $r \in R^S(q, h)$. We define

$$S(q, r) = \{r' \in V^n | \quad m_{q,r'} = m_{q,r}\}.$$

From symmetry, it follows that $\mathbb{P}\left((\Sigma(\bar{Q}) = r') \wedge (\bar{Q} \text{ is not } \gamma - \text{typical})\right)$ is the same for every $r' \in S(q, r)$. Thus,

$$\mathbb{P}\left((\Sigma(\bar{Q}) = r) \wedge (\bar{Q} \text{ is not } \gamma - \text{typical})\right) \leq \frac{\mathbb{P}(\bar{Q} \text{ is not } \gamma - \text{typical})}{|S(q, r)|}.$$

CEU eTD Collection

Since there is $c > 0$ such that $|S(q,r)| \geq |V^n| \exp(-cn^{2\beta-1})$, the statement follows as in the proof of Lemma 3.12. □

This concludes the proof of Theorem 7.1.

□

The analogue of Theorem 2.2 is the following.

Theorem 7.11. *For any fixed finite abelian group V and $d \geq 3$, we have*

$$\lim_{n\to\infty} |V|^n \sup_{q\in V^n \quad \alpha-typical} d_\infty(C_n^{(d)} q, U_{q,d}^S) = 0.$$

This theorem follows immediately from Theorem 7.1 once we prove the following analogue of Lemma 3.13.

Lemma 7.12. *Let $q \in V^n$ be α-typical, $r \in V^n$, $h \geq 2$ and Q is a random (q,h)-tuple. Then there is a polynomial g and a constant C (not depending on q and r), such that*

$$\mathbb{P}(\Sigma(Q) = r) \leq g(n)|V|^{-n} \exp(Cn^{2\alpha-1}).$$

This will be proved after Lemma 7.15, because the proofs of these two lemmas share some ideas.

Once we have Theorem 7.11, we only need to control the non-typical vectors to obtain Theorem 1.6. This can be done almost the same way as in Section 4. Here we list the necessary modifications.

In the next few lemmas, our main tool will be the notion of *Shannon entropy*. Given a random variable X taking values in a finite set $\mathcal{R}$, its Shannon entropy $H(X)$ is defined as

$$H(X) = \sum_{r\in\mathcal{R}} -\mathbb{P}(X = r) \log \mathbb{P}(X = r).$$

In the rest of this discussion, we always assume that random variables have finite range, and all the random variables are defined on the same probability space. If $X_1, X_2, \ldots, X_k$ is a sequence random variables, then their joint Shannon entropy $H(X_1, X_2, \ldots, X_k)$ is defined as the Shannon entropy $H(X)$ of the (vector valued) random variable $X = (X_1, X_2, \ldots, X_k)$. See [21] for more information on Shannon entropy.

A few basic properties of Shannon entropy are given in the next lemma.

Lemma 7.13. *Let X, Y, Z be three random variables. Then*

$$H(X,Y) \leq H(X) + H(Y), \tag{7.9}$$

and

$$H(X,Z) + H(Y,Z) \geq H(Z) + H(X,Y,Z). \tag{7.10}$$

CEU eTD Collection

Let X, Y be two random variables such that Y is a function of X. Then

$$H(X, Y) = H(X).$$

Proof. Note that the quantity $H(X,Z) + H(Y,Z) - H(Z) - H(X,Y,Z)$ is usually denoted by $I(X;Y|Z)$ and it is called conditional mutual information. It is well known that $I(X;Y|Z) \geq 0$. See [21, (2.92)]. This proves Inequality (7.10). We can obtain Inequality (7.9) as a special case of Inequality (7.10), if we we choose Z to be constant. The last statement is straightforward from the definitions. $\square$

Later we will need the following lemma.

Lemma 7.14. *For $d \geq 1$, let $Y_0, Y_1, \dots, Y_d$ be $d+1$ random variables. Then*

$$H(Y_0, Y_1, \dots, Y_d) \leq \sum_{i=1}^{d} H(Y_0, Y_i) - (d-1)H(Y_0).$$

Proof. The statement can be proved by induction. Indeed, from Inequality (7.10), we have

$$H(Y_0, Y_1, \dots, Y_d) + H(Y_0) \leq H(Y_0, Y_1, \dots, Y_{d-1}) + H(Y_0, Y_d).$$

Therefore,

$$\begin{aligned} H(Y_0, Y_1, \dots, Y_d) &\leq H(Y_0, Y_1, \dots, Y_{d-1}) + H(Y_0, Y_d) - H(Y_0) \\ &\leq \sum_{i=1}^{d} H(Y_0, Y_i) - (d-1)H(Y_0), \end{aligned}$$

where in the last step we used the induction hypothesis. $\square$

In Section 4, we used the fact that $|S(q)|\mathbb{P}(A_n^{(d)}q = r) = \mathbb{P}(r - A_n^{(d-1)}q \sim q)$. This equality is replaced by the following lemma.

Lemma 7.15. *Let $q, r \in V^n$ and*

$$m \in \mathcal{M}^S(q,r) = \{m_Q | \quad Q \text{ is a } (q,1,d)\text{-tuple and } \Sigma(Q) = r\}.$$

We define

$$E(m) = |S(q)|\mathbb{P}(m_{\bar{Q}} = m \text{ and } \Sigma(\bar{Q}) = r),$$

where $\bar{Q}$ is random $(q,1,d)$-tuple.

Moreover, let $p(m)$ be the probability of the event that for a random $(q,1,d-1)$-tuple $\bar{Q} = (\bar{q}^{(0)}, \bar{q}^{(1)}, \dots, \bar{q}^{(d-1)})$, we have that $r - \Sigma(\bar{Q})$ is a matching permutation of q and the $(q,1,d)$-tuple $Q' = (\bar{q}^{(0)}, \bar{q}^{(1)}, \dots, \bar{q}^{(d-1)}, r - \Sigma(\bar{Q}))$ satisfies $m_{Q'} = m$. Then there is a polynomial $f(n)$ (not depending on q, r or m) such that

$$E(m) \leq f(n)p(m)^{\frac{1}{d-1}}.$$

CEU eTD Collection

Furthermore, there is a polynomial $g(n)$ such that

$$|S(q)|\mathbb{P}(C_n^{(d)}q = r) \leq g(n)\mathbb{P}(r - C_n^{(d-1)}q \sim q)^{\frac{1}{d-1}}.$$

Proof. Let $X = (X_0, X_1, X_2, \ldots, X_d) \in V^{1+d}$ be a random variable, such that $\mathbb{P}(X = t) = \frac{m(t)}{n}$ for every $t \in V^{1+d}$. We define $X_\Sigma = \sum_{i=1}^{d} X_i$. Then

$$E(m) = c_1(m)\exp\left(n\left(H(X_0) + H(X) - H(X, X_\Sigma) - \frac{1}{2}\sum_{i=1}^{d} H(X_0, X_i)\right)\right),$$

and

$$p(m) = c_2(m)\exp\left(n\left(H(X) - H(X_0, X_\Sigma) - \frac{1}{2}\sum_{i=1}^{d-1} H(X_0, X_i)\right)\right),$$

where $\frac{1}{b(n)} \leq c_1(m), c_2(m) \leq b(n)$ for some polynomial $b(n)$.

Since $X_d = X_\Sigma - \sum_{i=1}^{d-1} X_i$ and $X_\Sigma = \sum_{i=1}^{d} X_i$, applying the last statement of Lemma 7.13 twice, we get that

$$\begin{aligned} H(X) = (X_0, X_1, \ldots, X_d) &= H(X_0, X_1, \ldots, X_d, X_\Sigma) \\ &= H(X_0, X_1, \ldots, X_{d-1}, X_\Sigma). \end{aligned} \tag{7.11}$$

Combining this with Lemma 7.14, we get that

$$\begin{aligned} H(X) &= H(X_0, ..., X_{d-1}, X_\Sigma) \\ &\leq \sum_{i=1}^{d-1} H(X_0, X_i) + H(X_0, X_\Sigma) - (d-1)H(X_0). \end{aligned}$$

Or more generally, for every $i = 1, 2, \ldots, d$, we have

$$H(X) \leq \sum_{\substack{1 \leq j \leq d \\ j \neq i}} H(X_0, X_j) + H(X_0, X_\Sigma) - (d-1)H(X_0).$$

Summing up these inequalities for $i = 1, 2, ..., d-1$, we get that

$$\begin{aligned} &(d-1)H(X) \\ &\quad \leq (d-2)\sum_{i=1}^{d-1} H(X_0, X_i) + (d-1)H(X_0, X_d) + (d-1)H(X_0, X_\Sigma) - (d-1)^2 H(X_0). \end{aligned} \tag{7.12}$$

CEU eTD Collection

Note that $X_0, X_1, \dots, X_d$ all have the same distribution, so $H(X_0) = H(X_1) = \dots = H(X_d)$. Combining this with Equation (7.11) and Inequality (7.9), we have

$$\begin{aligned} H(X) &= H(X_0, ..., X_{d-1}, X_\Sigma) \\ &\le H(X_0, X_\Sigma) + \sum_{i=1}^{d-1} H(X_i) = H(X_0, X_\Sigma) + (d-1)H(X_0). \end{aligned} \tag{7.13}$$

Therefore,

$$\begin{aligned} &H(X_0) + H(X) - H(X_0, X_\Sigma) - \frac{1}{2}\sum_{i=1}^{d} H(X_0, X_i) \\ &= H(X_0) + H(X) - H(X_0, X_\Sigma) - \frac{1}{2(d-1)}\sum_{i=1}^{d-1} H(X_0, X_i) \\ &\quad - \frac{1}{2}\left(\frac{d-2}{d-1}\sum_{i=1}^{d-1} H(X_0, X_i) + H(X_0, X_d)\right) \\ &\le H(X_0) + H(X) - H(X_0, X_\Sigma) - \frac{1}{2(d-1)}\sum_{i=1}^{d-1} H(X_0, X_i) \\ &\quad - \frac{1}{2}\left(H(X) + (d-1)H(X_0) - H(X_0, X_\Sigma)\right) \\ &= \frac{1}{d-1}\left(H(X) - H(X_0, X_\Sigma) - \frac{1}{2}\sum_{i=1}^{d-1} H(X_0, X_i)\right) \\ &\quad + \frac{d-3}{2(d-1)}(H(X) - H(X_0, X_\Sigma)) - \frac{(d-3)}{2}H(X_0) \\ &\le \frac{1}{d-1}\left(H(X) - H(X_0, X_\Sigma) - \frac{1}{2}\sum_{i=1}^{d-1} H(X_0, X_i)\right), \end{aligned}$$

where at the first inequality, we used Inequality (7.12), and at the second inequality, we used Inequality (7.13). This gives the first statement. To get the second one, observe that

$$\begin{aligned} |S(q)|\mathbb{P}(C_n^{(d)}q = r) &= \sum_{m \in \mathcal{M}^S(q,r)} E(m) \le \sum_{m \in \mathcal{M}^S(q,r)} f(n)p(m)^{\frac{1}{d-1}} \\ &\le |\mathcal{M}^S(q,r)| f(n)\mathbb{P}(r - C_n^{(d-1)}q \sim q)^{\frac{1}{p-1}}. \end{aligned}$$

□

CEU eTD Collection

Now we prove Lemma 7.12.

Proof. Clearly we may assume that $h = 2$. The size of $\mathcal{M}^S(q, r)$ is polynomial in n, so it is enough to prove that for a fixed $m \in \mathcal{M}^S(q, r)$, we have a good upper bound on $\mathbb{P}(\Sigma(Q) = r \text{ and } m_Q = m)$. To show this, let $X = (X_0, X_1, X_2) \in V^{1+2}$ be a random variable, such that $\mathbb{P}(X = t) = \frac{m(t)}{n}$ for every $t \in V^{1+2}$, and let $X_\Sigma = X_1 + X_2$. Then $\mathbb{P}(\Sigma(Q) = r \text{ and } m_Q = m)$

can be upper bounded by some polynomial multiple of

$$\begin{aligned}
&\exp\left(n\left(H(X)-H(X_0,X_\Sigma)-\frac{1}{2}\left(H(X_0,X_1)+H(X_0,X_2)\right)\right)\right)\\
&\quad=\exp\Big(n\big(-H(X_0)-\frac{1}{2}((H(X_0,X_1)+H(X_0,X_\Sigma)-H(X)-H(X_0))\\
&\qquad\quad+(H(X_0,X_2)+H(X_0,X_\Sigma)-H(X)-H(X_0)))\big)\Big)\\
&\quad\leq \exp(-nH(X_0))\leq |V|^{-n}\exp(Cn^{2\alpha-1}),
\end{aligned}$$

using the fact that for $i\in\{1,2\}$, we have

$$H(X_0,X_i)+H(X_0,X_\Sigma)\geq H(X_0)+H(X_0,X_i,X_\Sigma)=H(X_0)+H(X),$$

which is a combination of Inequality (7.10) and the last statement of Lemma 7.13. □

For any non-negative integral vector m indexed by V^{1+d} and for $i\in\{1,2,\dots,d\}$, we define

$$E_0(m)=\frac{m(V^{1+d})!}{\prod_{c\in V}m(\tau_0=c)!}\frac{\prod_{a,b\in V}m(\tau_0=a,\tau_\Sigma=b)!}{\prod_{t\in V^{1+d}}m(t)!},$$

and

$$\begin{aligned}
E_i(m)=&\left(\frac{m(V^{1+d})!}{2^{m(V^{1+d})/2}(m(V^{1+d})/2)!}\right)^{-1}\\
&\times\left(\prod_{a\in V}\frac{m(\tau_i=a,\tau_0=a)!}{2^{m(\tau_i=a,\tau_0=a)/2}(m(\tau_i=a,\tau_0=a)/2)!}\right)\left(\prod_{a\neq b\in V}\sqrt{m(\tau_0=a,\tau_i=b)!}\right).
\end{aligned}$$

Finally, let

$$E(m)=E_0(m)\prod_{i=1}^{d}E_i(m).$$

Here we need to define $(\ell+\frac{1}{2})!$ for an integer ℓ. The simple definition $(\ell+\frac{1}{2})!=\ell!\sqrt{\ell+1}$ is good enough for our purposes.

Recall that for $q,r\in V^n$ and $m\in\mathcal{M}^S(q,r)$, we already defined $E(m)$ as

$$E(m)=|S(q)|\mathbb{P}(m_{\bar{Q}}=m\text{ and }\Sigma(\bar{Q})=r),$$

where $\bar{Q}$ is a random $(q,1,d)$-tuple.

Using Equation (7.4), it is straightforward to verify that for a special m like above, the two definitions coincide.

CEU eTD Collection

Given a $q \in V^n$, a $(q,1,d)$-tuple Q or m_Q itself will be called W-decent if for any $u \in W^{1+d}$ we have
$$\frac{1+m_Q(\tau_0 = u_0, \tau_\Sigma = u_\Sigma)}{1+m_Q(u)} \le \log^2 n.$$

A non-negative integral vector m indexed by V^{1+d} will be called W-half-decent if for every $u \in W^{1+d}$, we have
$$\frac{1+m(\tau_0 = u_0, \tau_\Sigma = u_\Sigma)}{1+m(u)} \le \log^4 n,$$
and for every $c \in W$, we have
$$\left| m(\tau_0 = c) - \frac{n}{|W|} \right| < 2n^\alpha,$$
where $n = \sum_{t \in V^{1+d}} m(t)$.

Lemma 7.16 (The analogue of Lemma 4.8)**.** *For any coset $W \in \mathrm{Cos}(V)$, we have*
$$\limsup_{n\to\infty} \sum_{q \in D_W^n} |S(q)| \mathbb{P}(\Sigma(\bar{Q}) = r_q) = \limsup_{n\to\infty} \sum_{q \in D_W^n} |S(q)| \mathbb{P}(\Sigma(\bar{Q}) = r_q \textit{ and } \bar{Q} \textit{ is } W-\textit{decent}).$$

Proof. As in the proof of Lemma 4.8, it is enough to show that
$$|S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is not } W-\text{decent}) < n^{-(|V|+1)}$$
for every $(W, C\log n)$-typical vector $q \in V^n$ if n is large enough.

Consider a $(W, C\log n)$-typical vector $q \in V^n$, and let
$$\mathcal{M}_B = \{m_Q | \quad Q \text{ is a not } W\text{-decent } (q,1,d)\text{-tuple, such that } \Sigma(Q) = r_q\} \subset \mathcal{M}^S(q, r_q).$$

Recall that for $m \in \mathcal{M}^S(q, r_q)$, we defined $p(m)$ as the probability of the event that for a random $(q,1,d-1)$-tuple $\bar{Q} = (\bar{q}^{(0)}, \bar{q}^{(1)}, \dots, \bar{q}^{(d-1)})$, we have that $r_q - \Sigma(\bar{Q})$ is a matching permutation of q and the $(q,1,d)$-tuple $Q' = (\bar{q}^{(0)}, \bar{q}^{(1)}, \dots, \bar{q}^{(d-1)}, r_q - \Sigma(\bar{Q}))$ satisfies $m_{Q'} = m$.

Note that for $m \in \mathcal{M}_B$ the event above is contained in the event that

there is a $t \in W^{1+(d-1)}$ and $c \in dW$ such that
$$\frac{1+|\{i| \quad r_q(i) = c \text{ and } q_i = t_0\}|}{1+|\{i| \quad r_q(i) = c \text{ and } \bar{Q}(i) = t\}|} > \log^2 n.$$

CEU eTD Collection

Let $p'(q)$ be the probability of the latter event. As we just observed, $p(m) \leq p'(q)$ for all $m \in \mathcal{M}_B$. Using Lemma 7.15 and Lemma 10.3, we obtain

$$\begin{aligned}
|S(q)|\mathbb{P}(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is not } W-\text{decent}) &= \sum_{n\in\mathcal{M}_B} E(m) \\
&\leq \sum_{n\in\mathcal{M}_B} f(n)p(m)^{\frac{1}{d-1}} \\
&\leq |\mathcal{M}_B| f(n) p'(q)^{\frac{1}{d-1}} < n^{-(|V|+1)}
\end{aligned}$$

for large enough n. □

Let

$$\mathcal{M}^S = \{m_Q \quad | \quad Q \text{ is a } (q,1,d)\text{-tuple for some } n \geq 0 \text{ and } q \in V^n\}.$$

Lemma 7.17 (The analogue of Lemma 4.9)**.** *There are finitely many vectors $m_1, m_2, ..., m_\ell \in \mathcal{M}^S$, such that*

$$\mathcal{M}^S = \{c_1 m_1 + c_2 m_2 + \cdots + c_\ell m_\ell \quad | \quad c_1, c_2, \ldots, c_\ell \textit{ are non-negative integers}\}.$$

Proof. We define

$$\mathcal{R} = \left\{(m,g) \quad | \quad m \in \mathbb{R}^{V^{1+d}}, \quad g \in \mathbb{R}^{\{1,2,\ldots,d\}\times V}\right\}.$$

Consider the linear subspace $\mathcal{R}'$ of $\mathcal{R}$ consisting of pairs (m,g) satisfying the following liner equations:

$$m(\tau_0 = a \text{ and } \tau_i = b) = m(\tau_0 = b \text{ and } \tau_i = a)$$

for all $a, b \in V$ and $i \in \{1, 2, \ldots, d\}$, moreover,

$$m(\tau_0 = c \text{ and } \tau_i = c) = 2g(i,c)$$

for all $c \in V$ and $i \in \{1, 2, \ldots, d\}$.

Let $\mathcal{M}_0$ be the set of non-negative integral points of $\mathcal{R}'$. Observe that $\mathcal{M}_0$ consists of the integral points of a rational polyhedral cone. From [54, Theorem 16.4], we know that this cone is generated by an integral Hilbert basis, i. e., there are finitely many vectors $(m_1, g_1), (m_2, g_2), ..., (m_\ell, g_\ell) \in \mathcal{M}_0$, such that

$$\mathcal{M}_0 = \{c_1 \cdot (m_1, g_1) + \cdots + c_\ell \cdot (m_\ell, g_\ell) | \quad c_1, c_2, \ldots, c_\ell \text{ are non-negative integers}\}.$$

Then the vectors $m_1, m_2, \ldots, m_\ell \in \mathcal{M}^S$ have the required properties.

Note we only introduced the extra component g to enforce the parity constraints in (7.3). □

As before, we may assume that the indices in the lemma above are chosen such that there is an h such that the supports of $m_1, m_2, \ldots, m_h$ are contained in W^{1+d}, and the supports of $m_{h+1}, m_{h+2}, ..., m_\ell$ are not contained in W^{1+d}.

CEU eTD Collection

Lemma 7.18 (The analogue of Lemma 4.12)**.** *Consider a non-negative integral W-half-decent vector $m_0 \in \mathbb{R}^{V^{1+d}}$, such that $\|m_0\|_{W^C} = m(t \notin W^{1+d}) = O(\log n)$, where $n = \sum_{t \in V^{1+d}} m(t)$. For $u \in V^{1+d}$, let $\chi_u \in \mathbb{R}^{V^{1+d}}$ be such that $\chi_u(u) = 1$ and $\chi_u(t) = 0$ for every $t \neq u \in V^{1+d}$.*

- *If $u \in W^{1+d}$, then $E(m_0 + \chi_u)/E(m_0) = O\left(\log^4 n\right)$;*
- *If $u_0 \notin W$, then $E(m_0 + \chi_u)/E(m_0) = O\left(\frac{\log^{d+1} n}{n^{d/2-1}}\right)$;*
- *If $u_0 \in W$ and $u \notin W^{1+d}$, then $E(m_0 + \chi_u)/E(m_0) = O\left(\log^2 n\right)$.*

Proof. Let

$$
\begin{aligned}
g &= \frac{1 + m_0(\tau_0 = u_0, \tau_\Sigma = u_\Sigma)}{1 + m_0(u)},\\
h &= \frac{n+1}{m(\tau_0 = u_0) + 1}, \qquad\qquad \text{and}\\
f_i &= \sqrt{\frac{1 + m_0(\tau_0 = u_0, \tau_i = u_i)}{n+1}}.
\end{aligned}
$$

Lemma 7.19.

$$E(m_0 + \chi_u)/E(m_0) = O(g \cdot h \cdot \prod_{i=1}^{d} f_i).$$

Proof. It is straightforward to check that $E_0(m_0 + \chi_u)/E_0(m_0) = g \cdot h$. Let $i \in \{1, 2, \ldots, d\}$. First assume that $u_i \neq u_0$, then

$$E_i(m_0 + \chi_u)/E_i(m_0) = \frac{\sqrt{2}}{n+1} \cdot \frac{\left(\frac{n+1}{2}\right)!}{\left(\frac{n}{2}\right)!} \cdot \sqrt{m_0(\tau_i = u_i, \tau_0 = u_0) + 1}.$$

Recall that for any integer ℓ we defined $(\ell + \frac{1}{2})!$ as $(\ell + \frac{1}{2})! = \ell!\sqrt{\ell + 1}$. Thus, if n is even, then

$$\frac{\left(\frac{n+1}{2}\right)!}{\left(\frac{n}{2}\right)!} = \sqrt{\frac{n}{2} + 1} = O(\sqrt{n+1}),$$

and if n is odd, then

$$\frac{\left(\frac{n+1}{2}\right)!}{\left(\frac{n}{2}\right)!} = \sqrt{\frac{n+1}{2}} = O(\sqrt{n+1}).$$

Therefore, $E_i(m_0 + \chi_u)/E_i(m_0) = O(f_i)$. In the case $u_i = u_0 = c$, we have

$$E_0(m_0 + \chi_u)/E_0(m_0) = \frac{\sqrt{2}}{n+1} \cdot \frac{\left(\frac{n+1}{2}\right)!}{\left(\frac{n}{2}\right)!} \cdot \frac{m_0(\tau_i = c, \tau_0 = c) + 1}{\sqrt{2}} \cdot \frac{\left(\frac{m_0(\tau_i = c, \tau_0 = c)}{2}\right)!}{\left(\frac{m_0(\tau_i = c, \tau_0 = c) + 1}{2}\right)!}.$$

CEU eTD Collection

A similar argument as above gives that $E_i(m_0 + \chi_u)/E_i(m_0) = O(f_i)$ also holds in this case. The statement follows from the fact that

$$E(m_0 + \chi_u)/E(m_0) = \prod_{i=0}^{d} E_i(m_0 + \chi_u)/E_i(m_0).$$

□

If $u \in W^{1+d}$, then since m_0 is W-half-decent, we have $g \leq \log^4 n$, $h = O(1)$ and clearly $f_i \leq 1$, thus the statement follows.

If $u_0 \notin W$, then $g = O(\log n)$, $h = O(n)$, $f_i = O(\frac{\log n}{\sqrt{n}})$, and the statement follows.

If $u_0 \in W$ and $u \notin W^{1+d}$, then we consider two cases:

1. If $u_\Sigma \in dW$, then $g = O(n)$, $h = O(1)$, moreover there are at least two indices i such that $u_i \notin W$. For such an i, we have $f_i = O(\frac{\log n}{\sqrt{n}})$, otherwise we have $f_i \leq 1$, from these the statement follows.
2. If $u_\Sigma \notin dW$, then $g = O(\log n)$, $h = O(1)$ and $f_i \leq 1$ for every i. The statement follows.

□

The previous lemma has the following consequence.

Lemma 7.20 (The analogue of Lemma 4.13)**.** *There are $D, \delta > 0$, such that for any $i \in \{h+1, h+2, \dots, \ell\}$ and any non-negative integral W-half-decent vector $m_0 \in \mathbb{R}^{V^{1+d}}$, such that $\|m_0\|_{W^C} = O(\log n)$, we have*

$$E(m_0 + m_i)/E(m_0) = O\left(\left(n^{-\delta} \log^D n\right)^{\|m_i\|_{W^C}}\right).$$

Proof. Take any $i \in \{h+1, h+2, \dots, \ell\}$. Since m_i is not supported on W^{1+d}, we have a $u \notin W^{1+d}$ such that $m_i(u) \geq 1$. If $u_0 \notin W$, then $m_i(\tau_0 \notin W) \geq m_i(\tau_0 = u_0) \geq 1$. If $u_0 \in W$, then there is a j such that $u_j \notin W$, thus

$$m_i(\tau_0 \notin W) \geq m_i(\tau_0 = u_j, \tau_j = u_0) = m_i(\tau_0 = u_0, \tau_j = u_j) \geq m_i(u) \geq 1.$$

In both cases, we obtained that $m_i(\tau_0 \notin W) \geq 1$. Note that for $d \geq 3$, we have $d/2 - 1 > 0$. From the previous statements and Lemma 7.20, it follows that for a large enough D and a small enough $\delta > 0$, we have

$$E(m_0 + m_i)/E(m_0) = O\left(\left(\log^D n\right)^{\|m_i\|_{W^C}} n^{-(d/2-1)}\right) = O\left(\left(n^{-\delta} \log^D n\right)^{\|m_i\|_{W^C}}\right).$$

□

CEU eTD Collection

With these modifications above, we proved Theorem 1.6.

As an easy consequence of Theorem 1.6 we obtain following analogue of Corollary 5.1. The random $(n-1)\times(n-1)$ matrix C'_n is obtained from C_n by deleting its last row and last column. Recall $q \in V^{n-1}$ the subgroup generated by $q_1, q_2, \dots, q_{n-1}$ is denoted by G_q. Let U_q^S be a uniform random element of the set

$$\{w \in G_q^{n-1} | \quad < q \otimes w > \in I_2\}.$$

Corollary 7.21. *We have*

$$\lim_{n\to\infty} \sum_{q \in V^{n-1}} d_\infty(C'_n q, U_q^S) = 0.$$

□

Note that for $q \in V^{n-1}$ such that $G_q = V$, if $r \in V^{n-1}$ and $< q \otimes r > \in I_2$ then $\mathbb{P}(U_q^S = r) = |V|^{-(n-1)} 2^{\mathrm{Rank}_2(V)} |\wedge^2 V|$. Therefore, Theorem 1.4 can be proved using the following observation.

Lemma 7.22. *If d is even, then $< q \otimes dq > \in I_2$ for every $q \in V^{n-1}$. If d is odd, then $< q \otimes dq > \in I_2$ if and only if $s(q)$ is an element of the subgroup $V' = \{2v | v \in V\}$. The subgroup V' has index $2^{\mathrm{Rank}_2(V)}$ in V.* □

For odd d, Theorem 1.2 follows from Theorem 1.4 and Theorem 5.5 part (2).

8 The 2-Sylow subgroup in the case of even d

Assume that d is even. Let Δ_n be the reduced Laplacian of H_n, and Γ_n be the corresponding sandpile group. Theorem 1.4 provides us the limit of the surjective V-moments of Γ_n. However, these moments grow too fast, so Theorem 5.3 can not be applied to get the existence of a limit distribution. We can overcome this difficulty by using that Γ_n has a special property given in the next lemma.

Lemma 8.1. *The group $\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}$ has odd rank.*

Given any integral matrix M, let $\overline{M}$ be its mod 2 reduction. That is, $\overline{M}$ is a matrix over the 2 element field, where an entry is 1 if and only if the corresponding entry of M is odd.

Proposition 8.2. *Let M be a integral $m \times m$ matrix. Then*

$$\mathrm{Rank}(\mathrm{cok}(M) \otimes \mathbb{Z}/2\mathbb{Z}) = \dim\ker \overline{M} = m - \mathrm{Rank}(\overline{M}).$$

Proof. It is straightforward to verify the statement if M is diagonal. If M is not diagonal, then M can be written as $M = ADB$, where D is diagonal, and $A, B \in \mathrm{GL}_m(\mathbb{Z})$. This is the so-called Smith normal form. The statement follows from the fact that $\dim\ker \overline{M} = \dim\ker \overline{ADB} = \dim\ker \overline{A} \cdot \overline{D} \cdot \overline{B} = \dim\ker \overline{D}$, and $\mathrm{cok}\, M = \mathrm{cok}\, ADB = \mathrm{cok}\, D$. □

CEU eTD Collection

Proof. (Lemma 8.1) Observe that $\overline{\Delta_n}$ is a symmetric matrix, where all the diagonal entries are 0. Such a matrix alway has even rank. See for example [44, Theorem 3]. Recall that Δ_n is an $(n-1) \times (n-1)$ matrix, where n is even. Thus, the statement follows from the previous proposition. □

In the first part of this section, we prove a modified version of Theorem 5.3, which allows us to make use of the fact that $\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}$ has odd rank. For most of the proof we can follow the original argument of Wood [58] almost word by word with only small modifications. A few proofs are omitted, since they are almost identical to the proofs of Wood [58]. The interested reader can find them in the Appendix of the paper [48].

We start by giving a few definitions. A partition λ of length m is a sequence $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m \geq 1$ of positive integers. It will be a convenient notation to also define $\lambda_i = 0$ for $i > m$. The transpose partition λ' of λ is defined by setting λ'_j to be the number of λ_i that are at least j. Thus, the length of λ' is λ_1. Recall that any finite abelian p-group G is isomorphic to

$$\bigoplus_{i=1}^{m} \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$$

for some partition λ of length m. We call λ the type of the group G. In fact, this provides a bijection between the set of isomorphism classes of finite abelian p-groups and the set of partitions.

Lemma 8.3.

1. *Given a positive integer m, and $b \in \mathbb{Z}^m$ such that b_1 is odd, $b_1 \geq b_2 \geq \cdots \geq b_m$, we have an entire analytic function in the m variables $z_1, \dots, z_m$*

$$H_{m,2,b}(z) = \sum_{\substack{d_1,\dots,d_m \geq 0 \\ d_2+\cdots+d_m \leq b_1}} a_{d_1,\dots,d_m} z_1^{d_1} \cdots z_m^{d_m}$$

and a constant E such that

$$a_{d_1,\dots,d_m} \leq E 2^{-b_1 d_1 - d_1(d_1+1)}.$$

Further, if f is a partition of length $\leq m$ such that $f > b$ (in the lexicographic ordering), f_1 is odd, then $H_{m,2,b}(2^{f_1}, 2^{f_1+f_2}, \dots, 2^{f_1+\cdots+f_m}) = 0$. If $f = b$, then $H_{m,2,b}(2^{f_1}, 2^{f_1+f_2}, \dots, 2^{f_1+\cdots+f_m}) \neq 0$.

2. *Given a positive integer m, a prime $p > 2$,[7] and $b \in \mathbb{Z}^m$ with $b_1 \geq b_2 \geq \cdots \geq b_m$, we have an entire analytic function in the m variables $z_1, \dots, z_m$*

$$H_{m,p,b}(z) = \sum_{\substack{d_1,\dots,d_m \geq 0 \\ d_2+\cdots+d_m \leq b_1}} a_{d_1,\dots,d_m} z_1^{d_1} \cdots z_m^{d_m}$$

[7] In fact, this statement is also true for $p = 2$, but we will not use this.

CEU eTD Collection

and a constant E such that

$$a_{d_1,\dots,d_m} \leq Ep^{-b_1 d_1 - \frac{d_1(d_1+1)}{2}}.$$

Further, if f is a partition of length $\leq m$ and $f > b$ (in the lexicographic ordering), then $H_{m,p,b}(p^{f_1}, p^{f_1+f_2}, \dots, p^{f_1+\dots+f_m}) = 0$. If $f = b$, then $H_{m,p,b}(p^{f_1}, p^{f_1+f_2}, \dots, p^{f_1+\dots+f_m}) \neq 0$.

Proof. See the Appendix of [48] for the proof. □

In the original proof of Wood [58], the prime 2 was not handled separately. That is, the functions given in part (2) of Lemma 8.3 were used for all primes. Let us restrict our attention to random groups G where $G \otimes \mathbb{Z}/2\mathbb{Z}$ has odd rank. Then, for the prime 2, we can use the functions given in part (1) of Lemma 8.3 instead of the ones given in part (2), and still proceed with the proof, as we show in the next lemmas. Note that part (1) provides better bounds for the coefficients. This allows us to handle faster growing moments.

Theorem 8.4. *Let $2 = p_1, \dots, p_s$ be distinct primes. Let $m_1, \dots, m_s \geq 1$ be integers.*

Let M_j be the set of partitions λ at most m_j parts. Let $M = \prod_{j=1}^{s} M_j$. For $\mu \in M$, we write μ^j for its jth entry, which is a partition consisting of non-negative integers μ_i^j with $\mu_1^j \geq \mu_2^j \geq \dots \mu_{m_j}^j$. Let

$$M_0 = \{\mu \in M \quad | \quad \mu_1^1 \text{ is odd}\}.$$

Suppose we have non-negative reals x_μ, y_μ, for each tuple of partitions $\mu \in M_0$. Further suppose that we have non-negative reals C_λ for each $\lambda \in M$ such that

$$C_\lambda \leq 2^{\lambda_1^1} \prod_{j=1}^{s} F^{m_j} p_j^{\sum_i \frac{\lambda_i^j(\lambda_i^j - 1)}{2}},$$

where $F > 0$ is an absolute constant. Suppose that for all $\lambda \in M$,

$$\sum_{\mu \in M_0} x_\mu \prod_{j=1}^{s} p_j^{\sum_i \lambda_i^j \mu_i^j} = \sum_{\mu \in M_0} y_\mu \prod_{j=1}^{s} p_j^{\sum_i \lambda_i^j \mu_i^j} = C_\lambda. \tag{8.1}$$

Then for all $\mu \in M_0$, we have that $x_\mu = y_\mu$.

Proof. See the Appendix of [48] for the proof. □

Lemma 8.5. *There is a constant F, such that for any finite abelian p-group G of type λ, we have*

$$\sum_{G_1 \text{ subgroup of } G} |\wedge^2 G_1| \leq F^{\lambda_1} p^{\sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}.$$

Moreover, if G finite abelian 2-group G of type λ, we have

$$\sum_{G_1 \text{ subgroup of } G} 2^{\mathrm{Rank}_2(G_1)} |\wedge^2 G_1| \leq F^{\lambda_1} 2^{\lambda_1' + \sum_i \frac{\lambda_i'(\lambda_i'-1)}{2}}.$$

CEU eTD Collection

Proof. The first statement is the same as [58, Lemma 7.5].[8] The second statement follows from first by using the elementary fact that for any subgroup G_1 of G, we have $\mathrm{Rank}_2(G_1) \leq \mathrm{Rank}_2(G) = \lambda'_1$. □

Lemma 8.6. *([58, Lemma 7.1]) Let G_μ and G_λ be two finite abelian p-groups of type μ and λ. Then*

$$|\operatorname{Hom}(G_\mu, G_\lambda)| = p^{\sum_i \mu'_i \lambda'_i}.$$

Theorem 8.7. *Let X_n be a sequence of random variables taking values in finitely generated abelian groups. Let a be an even positive integer and A be the set of (isomorphism classes of) abelian groups with exponent dividing a. Assume that $\mathrm{Rank}(X_n \otimes \mathbb{Z}/2\mathbb{Z})$ is odd with probability 1 for every n. Suppose that for every $G \in A$, we have*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(X_n, G)| = 2^{\mathrm{Rank}_2(G)}|\wedge^2 G|.$$

Then for every $H \in A$, the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ exists, and for all $G \in A$, we have

$$\sum_{H\in A} \lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)|\operatorname{Sur}(H, G)| = 2^{\mathrm{Rank}_2(G)}|\wedge^2 G|.$$

Suppose Y_n is a sequence of random variables taking values in finitely generated abelian groups such that $\mathrm{Rank}(Y_n \otimes \mathbb{Z}/2\mathbb{Z})$ is odd with probability 1 for every n, and for every $G \in A$, we have

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(Y_n, G)| = 2^{\mathrm{Rank}_2(G)}|\wedge^2 G|.$$

Then, we have that for every every $H \in A$

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H) = \lim_{n\to\infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H).$$

Proof. See the Appendix of [48] for the proof. □

In the rest of the section we find a sequence of random groups, such that they have same limiting surjective moments as the sequence of sandpile groups of H_n. The nice algebraic properties of these groups allow us to give an explicit formula for their limiting distribution. Then the previous theorem can be used to conclude that the sandpile group of H_n has the same limiting distribution.

We start by showing that Lemma 7.6 is true under slightly weaker conditions.

Lemma 8.8. *Assume that $n \geq 2|V|$. Let $q \in V^n$ be such that $G_q = V$. Let $r \in V^n$ such that $< q \otimes r > \in I_2$. Then there is a symmetric matrix A over $\mathbb{Z}$ such that $r = Aq$ and all the diagonal entries of A are even.*

Proof. We start by the following lemma. As in Lemma 7.6, let $V = \bigoplus_{i=1}^{\ell} < v_i >$.

[8] In the latest arxiv version of this paper this is Lemma 7.4

CEU eTD Collection

Lemma 8.9. *There is an invertible integral matrix B, such that B^{-1} is integral, and $q' = Bq$ satisfies that $m_{q'}(v_i) > 0$ for every $1 \leq i \leq \ell$.*

Proof. Using the condition $n \geq 2|V|$ and $G_q = V$, we can choose $n - \ell$ components of q such that they generate V. Due to symmetry we may assume that $q_{\ell+1}, q_{\ell+2}, \dots, q_n$ generates V. Let us define $q' = (v_1, v_2, \dots, v_\ell, q_{\ell+1}, q_{\ell+2}, \dots, q_n)$. We define the integral matrix $B = (b_{ij})$ by

$$b_{ij} = \begin{cases} 1 & \text{for } 1 \leq i = j \leq n, \\ 0 & \text{for } 1 \leq j < i \leq n, \\ 0 & \text{for } \ell < i < j \leq n, \\ 0 & \text{for } 1 \leq i < j \leq \ell. \end{cases}$$

We still have not defined b_{ij} for $1 \leq i \leq \ell$ and $\ell < j \leq n$. Since $q_{\ell+1}, q_{\ell+2}, \dots, q_n$ generates V we can choose these entries such that $Bq = q'$. Since B is an upper triangular integral matrix such that each diagonal entry is 1, it is invertible and the inverse is an integral matrix. □

Let B the matrix provided by the lemma above. Set $q' = Bq$ and $r' = \left(B^{-1}\right)^T r$. Observe that

$$< q' \otimes r' >=< Bq \otimes \left(B^{-1}\right)^T r >=< B^{-1}Bq \otimes r >=< q \otimes r >\in I_2.$$

Applying Lemma 7.6, we obtain a symmetric integral matrix A' with even diagonal entries such that $r' = A'q'$. Consider $A = B^T A' B$. Then A is a a symmetric integral matrix with even diagonal entries. Moreover,

$$Aq = B^T A' B q = B^T A' q' = B^T r' = B^T \left(B^{-1}\right)^T r = r.$$

□

Lemma 8.10. *Let V be a finite abelian 2-group. Assume that 2^k is divisible by the exponent of V. Let A_n be uniformly chosen from the set of symmetric matrices in $M_n(\mathbb{Z}/2^k\mathbb{Z})$, such that all the diagonal entries are even. Then we have*

$$\lim_{n\to\infty} \mathbb{E}|\{q \in V^n| \quad G_q = V, \quad A_n q = 0\}| = 2^{\mathrm{Rank}_2(V)}|\wedge^2 V|.$$

Proof. Take any $q \in V^n$ such that $G_q = V$. Let N_n be the set of symmetric matrices with even diagonal entries in $M_n(\mathbb{Z}/2^k\mathbb{Z})$. The distribution of $A_n q$ is the uniform distribution on the image of the $N_n \to V^n$ homomorphism $C \mapsto Cq$. From Lemma 8.8 one can see that if n is large enough then this image is $\{r \in V^n| < q \otimes r >\in I_2\}$, which has size $|V|^n \left(2^{\mathrm{Rank}_2(V)}|\wedge^2 V|\right)^{-1}$. It is clear that 0 is always contained in the image, thus $\mathbb{P}(A_n q = 0) = |V|^{-n} 2^{\mathrm{Rank}_2(V)}|\wedge^2 V|$. Thus

$$\lim_{n\to\infty} \mathbb{E}|\{q \in V^n| \quad G_q = V, \quad A_n q = 0\}| =$$

$$\lim_{n\to\infty} \mathbb{E}|\{q \in V^n| \quad G_q = V\}| \frac{2^{\mathrm{Rank}_2(V)}|\wedge^2 V|}{|V^n|} = 2^{\mathrm{Rank}_2(V)}|\wedge^2 V|.$$

□

CEU eTD Collection

Let $\mathbb{Z}_2$ be the ring of 2-adic integers. Recall the fact that $\mathbb{Z}_2$ is the inverse limit of $\mathbb{Z}/2^k\mathbb{Z}$. Thus combining the lemma above with the analogue of Proposition 2.1, we get the following.

Lemma 8.11. *Let* $\mathrm{Symm}_0(n)$ *be the set of* $n \times n$ *symmetric matrices over* $\mathbb{Z}_2$*, such that all diagonal entries are even. Let* Q_n *be a Haar-uniform element of* $\mathrm{Symm}_0(n)$*. For any finite abelian* 2*-group* V*, we have*

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\operatorname{cok}(Q_n), V)| = 2^{\mathrm{Rank}_2(V)}|\wedge^2 V|.$$

Moreover, if $\overline{Q}_n \in M_n(\mathbb{Z}/2\mathbb{Z})$ *is obtained by reducing each entry of* Q_n *modulo* 2*, then* $\overline{Q}_n$ *is a symmetric matrix with* 0 *as its diagonal entries. Consequently,* $\mathrm{Rank}(\operatorname{cok}(Q_n)) \equiv n$ *modulo* 2*.* □

The next lemma gives an explicit formula for the limiting distribution of $\operatorname{cok}(Q_n)$. The author is grateful to Melanie Wood who proved this result for him.

Lemma 8.12. *(Wood [59]) For any finite abelian* 2*-group* G *of odd rank, we have*

$$\lim_{\substack{n\to\infty\\ n \text{ is odd}}} \mathbb{P}(\operatorname{cok}(Q_n) \simeq G) =$$

$$2^{\mathrm{Rank}(G)} \frac{|\{\phi : G \times G \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G||\operatorname{Aut}(G)|} \prod_{j=0}^{\infty} (1 - 2^{-2j-1}).$$

Proof. Assume that $G = \bigoplus_{i=1}^{k} (\mathbb{Z}/2^{e_i}\mathbb{Z})^{n_i}$ where $e_1 > e_2 > \cdots > e_k > 0$.

We consider $\mathbb{Z}_2^n$ as a $\mathbb{Z}_2$ module. Let $L_n(G)$ be the set of submodules M of $\mathbb{Z}_2^n$ such that $\mathbb{Z}_2^n/M$ is isomorphic to G.

$$\mathbb{P}(\operatorname{cok}(Q_n) \simeq G) = \mathbb{P}(\operatorname{RowSpace}(Q_n) \in L_n(G)) = \sum_{M \in L_n(G)} \mathbb{P}(\operatorname{RowSpace}(Q_n) = M).$$

Let μ_n be the Haar probability measure on $\mathrm{Symm}_0(n)$. Fix $M \in L_n(G)$. We are interested in the probability

$$\mathbb{P}(\operatorname{RowSpace}(Q_n) = M) = \mu_n(\{S \in \mathrm{Symm}_0(n) | \operatorname{RowSpace}(S) = M\}).$$

Fix any (not necessary symmetric) $n \times n$ matrix N over $\mathbb{Z}_p$ such that $\operatorname{RowSpace}(N) = M$. Observe that

$$\{S \in \mathrm{Symm}_0(n) | \operatorname{RowSpace}(S) = M\} = \{CN | \quad CN \in \mathrm{Symm}_0(n), C \in GL_n(\mathbb{Z}_2)\}.$$

Since $\mathbb{Z}_p$ is a principal ideal domain N has a Smith normal form, that is, we can find $A, B \in GL_n(\mathbb{Z}_2)$ such that $D = ANB$ is a diagonal matrix. Since each nonzero element of $\mathbb{Z}_2$ can written as $2^d u$, where d is a nonnegative integer, u is a unit in $\mathbb{Z}_2$, we may assume each entry of D is of the form 2^d for some d. But since $\mathbb{Z}_2^n/\operatorname{RowSpace}(D) \simeq \mathbb{Z}_2^n/\operatorname{RowSpace}(N) \simeq G$, we know

CEU eTD Collection

exactly what is D. Let $n_{k+1} = n - \sum_{i=1}^{k} n_i$, and $e_{k+1} = 0$. From now on it will be convenient to view $n \times n$ matrices as $(k+1) \times (k+1)$ block matrices, where the block at the position (i,j) is an $n_i \times n_j$ matrix. Then D is a block matrix $(D_{ij})_{i,j=1}^{k+1}$ where all the off-diagonal blocks are zero and $D_{ii} = 2^{e_i} I$.

Observe that map $S \mapsto B^T S B$ is an automorphism of the abelian group $\mathrm{Symm}_0(n)$. Thus, it pushes forward μ_n to μ_n, which gives us

$$\begin{aligned}
&\mu_n(\{CN| \quad CN \in \mathrm{Symm}_0(n), C \in GL_n(\mathbb{Z}_2)\}) \\
&\qquad = \mu_n(\{B^T CNB| \quad B^T CNB \in \mathrm{Symm}_0(n), C \in GL_n(\mathbb{Z}_2)\}) \\
&\qquad = \mu_n(\{B^T CA^{-1}ANB| \quad B^T CA^{-1}ANB \in \mathrm{Symm}_0(n), C \in GL_n(\mathbb{Z}_2)\}) \\
&\qquad = \mu_n(\{B^T CA^{-1}D| \quad B^T CA^{-1}D \in \mathrm{Symm}_0(n), C \in GL_n(\mathbb{Z}_2)\}) \\
&\qquad = \mu_n(\{FD| \quad FD \in \mathrm{Symm}_0(n), F \in GL_n(\mathbb{Z}_2)\}).
\end{aligned}$$

We consider $F = (F_{ij})_{i,j=1}^{k+1}$ as $(k+1) \times (k+1)$ block matrix as it was described above. Then $FD \in \mathrm{Symm}_0(n)$ if and only if for every $i < j$, we have

$$F_{ij} = 2^{e_i - e_j} F_{ji}^T \tag{8.2}$$

and the diagonal entries of $F_{k+1,k+1}$ are even. Assuming that F has these properties, when does F belong to $GL_n(\mathbb{Z}_2)$? Observe that $F \in GL_n(\mathbb{Z}_2)$ if and only if the mod 2 reduction $\overline{F}$ of F is invertible, but Equation (8.2) tells us $\overline{F}$ is a block lower triangular matrix, so $F \in GL_n(\mathbb{Z}_2)$ if and only if $F_{ii} \in GL_{n_i}(\mathbb{Z}_2)$ for each i.

From this it follows that $\{FD| \quad FD \in \mathrm{Symm}_0(n), F \in GL_n(\mathbb{Z}_2)\}$ consists of all block matrices $H \in \mathrm{Symm}_0(n)$, such that

1. For $1 \le i,j \le k+1$ all entries of the block H_{ij} is divisible by $2^{\max(e_i,e_j)}$.
2. For $1 \le i \le k+1$ the mod 2 reduction of the matrix $2^{-e_i} H_{ii}$ is an invertible symmetric matrix over $\mathbb{F}_2$. Moreover, if $i = k+1$, then all its diagonal entries are zero.

Let p_m be the probability that a uniform random symmetric $m \times m$ matrix over $\mathbb{F}_2$ is invertible, and let p'_m be the probability that a uniform random symmetric $m \times m$ matrix over $\mathbb{F}_2$ is invertible and all its diagonal entries are zero.

$$\begin{aligned}
\mathbb{P}(\mathrm{RowSpace}(Q_n) = M) &= \mu_n(\{FD| \quad FD \in \mathrm{Symm}_0(n), F \in GL_n(\mathbb{Z}_2)\}) \\
&= 2^n p'_{n_{k+1}} \prod_{i=1}^{k} p_{n_i} 2^{e_i\left(n_i(n - \sum_{j=1}^{i} n_j) + \binom{n_i+1}{2}\right)}.
\end{aligned}$$

CEU eTD Collection

In particular, this does not depend on the choice of $M \in L_n(G)$. Thus, we obtain that

$$\mathbb{P}(\operatorname{cok}(Q_n) \simeq G) = |L_n(G)| 2^n p'_{n_{k+1}} \prod_{i=1}^{k} p_{n_i} 2^{e_i\left(n_i(n-\sum_{j=1}^{i} n_j)+\binom{n_i+1}{2}\right)}.$$

Now let Q'_n be a Haar-uniform $n \times n$ symmetric matrix over $\mathbb{Z}_2$. A very similar calculation as above gives that

$$\mathbb{P}(\operatorname{cok}(Q'_n) \simeq G) = |L_n(G)| p_{n_{k+1}} \prod_{i=1}^{k} p_{n_i} 2^{e_i\left(n_i(n-\sum_{j=1}^{i} n_j)+\binom{n_i+1}{2}\right)}.$$

Therefore,

$$\begin{aligned} \frac{\mathbb{P}(\operatorname{cok}(Q_n) \simeq G)}{\mathbb{P}(\operatorname{cok}(Q'_n) \simeq G)} &= 2^n \frac{p'_{n_{k+1}}}{p_{n_{k+1}}} = 2^{n-n_{k+1}} \frac{2^{n_{k+1}} p'_{n_{k+1}}}{p_{n_{k+1}}} \\ &= 2^{\operatorname{Rank}(G)} \frac{2^{n_{k+1}} p'_{n_{k+1}}}{p_{n_{k+1}}} = 2^{\operatorname{Rank}(G)}. \end{aligned} \tag{8.3}$$

The last equality follows from the results of MacWilliams [44]. Note that here we needed to use that n and $\operatorname{Rank}(G)$ are both odd, therefore n_{k+1} is even. As we already mentioned in the Introduction in line (1.3) by the result of [18], we have

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(Q'_n) \simeq G) = \frac{|\{\phi : G \times G \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G||\operatorname{Aut}(G)|} \prod_{j=0}^{\infty} (1 - 2^{-2j-1}).$$

Combining this with line (8.3) above, we get the statement. □

Now we can prove the remaining part of Theorem 1.2

Proof. (Theorem 1.2 for even d)

Let $p_i^{k_i}$ be the exponent of G_i.

Let $Q_{n,1}$ be a Haar-uniform element of the the set of $(2n-1) \times (2n-1)$ symmetric matrices over $\mathbb{Z}_2$, where all the diagonal entries are even. For $i > 1$, let $Q_{n,i}$ be a Haar-uniform element of the the set of $(2n-1) \times (2n-1)$ symmetric matrices over $\mathbb{Z}_{p_i}$. All the choices are made independently. Let $\bar{Q}_{n,i} \in M_{2n-1}(\mathbb{Z}/p_i^{k_i+1}\mathbb{Z})$ be the mod $p_i^{k_i+1}$ reduction of $Q_{n,i}$.

Let $a = \prod_{i=1}^{s} p_i^{k_i+1}$. Let X_n be the sandpile group Γ_{2n} of H_{2n}. Let $Y_n = \bigoplus_{i=1}^{s} \operatorname{cok}(\bar{Q}_{n,i})$. Let V be a finite abelian group with exponent dividing a. Then, from Theorem 1.4, we have

$$\lim_{m\to\infty} \mathbb{E}|\operatorname{Sur}(X_n, V)| = 2^{\operatorname{Rank}_2(V)} |\wedge^2 V|.$$

Let V_i be the p_i-Sylow subgroup of V. From Lemma 8.10, we have

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\operatorname{cok}(\bar{Q}_{n,1}), V_1)| = 2^{\operatorname{Rank}_2(V_1)} |\wedge^2 V_1|.$$

CEU eTD Collection

For $i > 1$, from [18, Theorem 11], we have

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\operatorname{cok}(\bar{Q}_{n,1}), V_1)| = |\wedge^2 V_i|.$$

It is also clear that

$$|\operatorname{Sur}(Y_n, V)| = \prod_{i=1}^{s} |\operatorname{Sur}(\operatorname{cok}(\bar{Q}_{n,i}), V_i)|.$$

Thus, from the independence of $Q_{n,i}$, we get that

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(Y_n, V)| &= \prod_{i=1}^{s} \lim_{n\to\infty} \mathbb{E}|\operatorname{Sur}(\operatorname{cok}(\bar{Q}_{n,i}), V_i)| \\ &= 2^{\operatorname{Rank}_2(V_1)} \prod_{i=1}^{s} |\wedge^2 V_i| = 2^{\operatorname{Rank}_2(V)} |\wedge^2 V|.\end{aligned}$$

From Lemma 8.12 and [18, Theorem 2], we have

$$\lim_{n\to\infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq \bigoplus_{i=1}^{s} G_i) = \lim_{n\to\infty} \prod_{i=1}^{s} \mathbb{P}(\operatorname{cok}(Q_{n,i}) \simeq G_i) =$$
$$2^{\operatorname{Rank}(G_1)} \prod_{i=1}^{s} \left(\frac{|\{\phi : G_i \times G_i \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}\}|}{|G_i||\operatorname{Aut}(G_i)|} \prod_{j=0}^{\infty} (1 - p_i^{-2j-1}) \right).$$

Note that $\bigoplus_{i=1}^{s} \Gamma_{n,i} \simeq \bigoplus_{i=1}^{s} G_i$ if and only if $X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq \bigoplus_{i=1}^{s} G_i$. Note that both $\operatorname{Rank}_2(X_n \otimes \mathbb{Z}/2\mathbb{Z})$ and $\operatorname{Rank}_2(Y_n \otimes \mathbb{Z}/2\mathbb{Z})$ are odd. Therefore, Theorem 8.7 can be applied to finish the proof. □

9 The sublinear growth of rank

In this section we prove Theorem 1.9. Let Γ_n be the sandpile group of H_n. We start by a simple lemma. Recall that $\operatorname{Rank}_p(\operatorname{tors}(\Gamma_n))$ is the rank of the p-Sylow subgroup of $\operatorname{tors}(\Gamma_n)$.

Lemma 9.1. *There is a constant c_d such that $|\operatorname{tors}(\Gamma_n)| < c_d^n$. Consequently, for any prime p, we have*

$$\operatorname{Rank}_p(\operatorname{tors}(\Gamma_n)) \le \frac{n \log c_d}{\log p}.$$

Proof. Let $v_1, v_2, ..., v_k = n$ be a subset of the vertices of H_n, such that each connected component of H_n contains exactly one of them. (With high probability $k = 1$.) Let Δ_0 be the matrix obtained from the Laplacian by deleting the rows and columns corresponding to the vertices $v_1, v_2, \ldots, v_k$. Observe that $\operatorname{tors}(\Gamma_n) = |\det \Delta_0|$. Each row of Δ_0 has Euclidean norm at most

CEU eTD Collection

$c_d = \sqrt{2d^2}$. Thus, $\operatorname{tors}(\Gamma_n) = |\det \Delta_0| \le c_d^{n-k} < c_d^n$, from Hadamard's inequality [12]. The proof of the second statement is straightforward from this. $\square$

The lemma above will be used for large primes, for small primes we will use the next lemma.

Lemma 9.2. *For every prime p, there is a constant C_p such that for any n and $\varepsilon > 0$, we have*

$$\mathbb{P}(\operatorname{Rank}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}) \ge \varepsilon n) \le C_p p^{-\varepsilon n}.$$

Proof. It is an easy consequence of Corollary 7.21 and Proposition 2.1 that

$$\lim_{n\to\infty} \mathbb{E}|\operatorname{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})|$$

exists. This implies that there is a constant C_p such that

$$\mathbb{E}|\operatorname{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \le C_p$$

for any n. Note that $|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| = |\operatorname{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})|$. Thus, from Markov's inequality

$$\begin{aligned}\mathbb{P}(\operatorname{Rank}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}) \ge \varepsilon n) &= \mathbb{P}(|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| \ge p^{\varepsilon n}) \le p^{-\varepsilon n}\mathbb{E}|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| \\ &= p^{-\varepsilon n}\mathbb{E}|\operatorname{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \le C_p p^{-\varepsilon n}.\end{aligned}$$

$\square$

Now we are ready to prove Theorem 1.9. Take any $\varepsilon > 0$. Set $K = \exp(\varepsilon^{-1}\log c_d)$. Let $\{p_1, p_2, \dots, p_s\}$ be the set of primes that are at most K. Using Lemma 9.2, we get that

$$\mathbb{P}(\operatorname{Rank}(\Gamma_n \otimes \mathbb{Z}/p_i\mathbb{Z}) \ge \varepsilon n \text{ for some } i \in \{1, 2, \dots, s\}) \le \sum_{i=1}^{s} C_{p_i} p_i^{-\varepsilon n}.$$

Since $\sum_{n=1}^{\infty}\sum_{i=1}^{s} C_{p_i} p_i^{-\varepsilon n}$ is convergent, the Borel-Cantelli lemma gives us the following. With probability 1 there is an N such that for every $n > N$ and $i = 1, 2, \dots, s$, we have $\operatorname{Rank}(\Gamma_n \otimes \mathbb{Z}/p_i\mathbb{Z}) < \varepsilon n$. By the choice of K and Lemma 9.1, for a prime $p > K$, we have $\operatorname{Rank}_p(\operatorname{tors}(\Gamma_n)) \le \varepsilon n$. Write Γ_n as $\Gamma_n = \mathbb{Z}^f \times \operatorname{tors}(\Gamma_n)$. Then for $n > N$, we have

$$\begin{aligned}\operatorname{Rank}(\Gamma_n) &= f + \max_{p \text{ is a prime}} \operatorname{Rank}_p(\operatorname{tors}(\Gamma_n)) \\ &\le \operatorname{Rank}(\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}) + \max_{p \text{ is a prime}} \operatorname{Rank}_p(\operatorname{tors}(\Gamma_n)) \le \varepsilon n + \varepsilon n.\end{aligned}$$

Tending to 0 with ε, we get the statement.

CEU eTD Collection

10 Bounding the probabilities of non-typical events

At several points of the chapter we need to bound the probability of that something is not-typical. These estimates are all based on the following lemma.

Lemma 10.1. *Given $0 \le a, b \le n$, let A and B be a uniform independent random subset of $\{1, 2, \dots, n\}$ such that $|A| = a$ and $|B| = b$. Then for any $k > 0$, we have*

$$\mathbb{P}\left(\left||A \cap B| - \frac{ab}{n}\right| \ge k\right) \le 2\exp\left(-\frac{2k^2}{a}\right) \le 2\exp\left(-\frac{2k^2}{n}\right).$$

Proof. Note that $A \cap B$ has the same distribution as $\sum_{i=1}^{a} X_i$, where $X_1, X_2 \dots, X_a$ is a random sample drawn without replacement from an n element multiset, where 1 has multiplicity b and 0 has multiplicity $n - b$. Then the statement follows from [8, Proposition 1.2]. □

Applying this iteratively we get the following lemma.

Lemma 10.2. *Given $0 \le a_1, a_2, ..., a_d \le n$, let $A_1, A_2, ..., A_d$ be uniform independent random subsets of $\{1, 2, \dots, n\}$ such that $|A_i| = a_i$ for $i = 1, 2, \dots, d$. Then we have*

$$\mathbb{P}\left(\left||A_1 \cap \cdots \cap A_d| - n\prod_{i=1}^{d}\frac{a_i}{n}\right| \ge (d-1)k\right) \le 2(d-1)\exp\left(-\frac{2k^2}{a_1}\right)$$
$$\le 2(d-1)\exp\left(-\frac{2k^2}{n}\right).$$

Proof. The proof is by induction. For $d = 2$, it is true as Lemma 10.1 shows. Now we prove for d. By induction

$$\mathbb{P}\left(\left||A_1 \cap \dots A_{d-1}| - n\prod_{i=1}^{d-1}\frac{a_i}{n}\right| \ge (d-2)k\right) \le 2(d-2)\exp\left(-\frac{2k^2}{a_1}\right).$$

Using Lemma 10.1 for $A_1 \cap \dots A_{d-1}$ and A_d and the fact that $|A_1 \cap \dots A_{d-1}| \le a_1$, we have

$$\mathbb{P}\left(\left||A_1 \cap \dots A_d| - \frac{|A_1 \cap \cdots \cap A_{d-1}|a_d}{n}\right| \ge k\right) \le 2\exp\left(-\frac{2k^2}{a_1}\right).$$

Thus, with probability at least $1 - 2(d-1)\exp\left(-\frac{2k^2}{a_1}\right)$, we have that

$$\left||A_1 \cap \dots A_d| - \frac{|A_1 \cap \cdots \cap A_{d-1}|a_d}{n}\right| \le k$$

and for

$$\Delta = |A_1 \cap \dots A_{d-1}| - n\prod_{i=1}^{d-1}\frac{a_i}{n},$$

CEU eTD Collection

the inequality $|\Delta| \le (d-2)k$ holds. Therefore,

$$\begin{aligned}\left| |A_1 \cap \cdots \cap A_d| - n \prod_{i=1}^{d} \frac{a_i}{n} \right| &= \left| |A_1 \cap \cdots \cap A_d| - \frac{a_d(|A_1 \cap \cdots \cap A_{d-1}| - \Delta)}{n} \right| \\ &\le \left| |A_1 \cap \cdots \cap A_d| - \frac{a_d |A_1 \cap \cdots \cap A_{d-1}|}{n} \right| + \frac{a_d |\Delta|}{n} \\ &\le k + (d-2)k \le (d-1)k. \end{aligned}$$

□

Next we give the analogue of Lemma 10.1 for uniform random perfect matchings.

Lemma 10.3. *Assume that n is even. Let A and B be two fixed subsets of $\{1, 2, \ldots, n\}$, let $|A| = a$ and $|B| = b$. Let M be uniform random perfect matching on the set $\{1, 2, \ldots, n\}$. Let X be the number of elements in A that are paired with an element in B in the matching M. Then for any $k > 0$, we have*

$$\mathbb{P}\left(\left| X - \frac{ab}{n} \right| \ge 4k \right) \le 6 \exp\left(-\frac{2k^2}{a} \right) \le 6 \exp\left(-\frac{2k^2}{n} \right).$$

Proof. Observe that the uniform random matching M can be generated as follows. First we partition the set $\{1, 2, \ldots, n\}$ into two disjoint subsets H_1 and H_2 of size $\frac{n}{2}$ uniformly at random. Then we consider a uniform random perfect matching between H_1 and H_2. For $i \in \{1, 2\}$, let $a_i = |A \cap H_i|$, and let $b_i = |B \cap H_i|$. Let X_i be the number of element in $A \cap H_i$ that are paired with an element in B. From Lemma 10.1, we have

$$\begin{aligned}\mathbb{P}\left(\left| a_1 - \frac{a}{2} \right| \ge k \right) &\le 2 \exp\left(-\frac{2k^2}{a} \right), \\ \mathbb{P}\left(\left| X_1 - \frac{2a_1 b_2}{n} \right| \ge k \right) &\le 2 \exp\left(-\frac{2k^2}{a_1} \right), \\ \mathbb{P}\left(\left| X_2 - \frac{2a_2 b_1}{n} \right| \ge k \right) &\le 2 \exp\left(-\frac{2k^2}{a_2} \right).\end{aligned}$$

It follows from the union bound that with probability at least $1 - 6\exp\left(-\frac{2k^2}{a}\right)$, we have that

$$\left| a_1 - \frac{a}{2} \right| < k, \quad \left| X_1 - \frac{2a_1 b_2}{n} \right| < k \text{ and } \left| X_2 - \frac{2a_2 b_1}{n} \right| < k.$$

On this event

$$\begin{aligned}\left| X - \frac{ab}{n} \right| &= \left| \left(X_1 - \frac{ab_2}{n} \right) + \left(X_2 - \frac{ab_1}{n} \right) \right| \\ &\le \left| X_1 - \frac{ab_2}{n} \right| + \left| X_2 - \frac{ab_1}{n} \right| \\ &\le \left| X_1 - \frac{2a_1 b_2}{n} \right| + \left| \frac{2a_1 b_2}{n} - \frac{ab_2}{n} \right| + \left| X_2 - \frac{a_2 b_1}{2n} \right| + \left| \frac{2a_2 b_1}{n} - \frac{ab_1}{n} \right| \\ &< 2k + \frac{2b_1}{n} \left| a_2 - \frac{a}{2} \right| + \frac{2b_2}{n} \left| a_1 - \frac{a}{2} \right| < 4k.\end{aligned}$$

CEU eTD Collection

□

Applying this iteratively, we can get a lemma similar to Lemma 10.2.

CEU eTD Collection

3

Limiting entropy of determinantal processes

We extend Lyons's tree entropy theorem to general determinantal measures. As a byproduct we show that the sofic entropy of an invariant determinantal measure does not depend on the chosen sofic approximation.

1 Introduction

Let $P = (p_{ij})$ be an orthogonal projection matrix, where rows and columns are both indexed with a finite set V. Then there is a unique probability measure η_P on the subsets of V such that for every $F \subset V$ we have

$$\eta_P(\{B|F \subset B \subset V\}) = \det(p_{ij})_{i,j\in F}.$$

The measure η_P is called the *determinantal measure* corresponding to P [42]. Let B^P be a random subset of V with distribution η_P. In this chapter we investigate the asymptotic behavior of the *Shannon-entropy* of B^P defined as

$$H(B^P) = \sum_{A\subset V} -\mathbb{P}(B^P = A)\log \mathbb{P}(B^P = A).$$

Let $P_1, P_2, \ldots$ be a sequence of orthogonal projection matrices. Assume that rows and columns of P_n are both indexed with the finite set V_n. Let G_n be a graph on the vertex set V_n. Throughout the chapter we assume that the degrees of graphs are at most D for some fixed finite D.

CEU eTD Collection

Our main theorem is the following.

Theorem. *Assume that the sequence of pairs* (G_n, P_n) *is Benjamini-Schramm convergent and tight. Then*

$$\lim_{n\to\infty} \frac{H(B^{P_n})}{|V_n|}$$

exists.

Note that this theorem will be restated in a slightly more general and precise form as Theorem 2.5 in the next section. We will also give a formula for the limit.

We define *Benjamini-Schramm convergence* of (G_n, P_n) along the lines of [10] and [4] via the following local sampling procedure. Fix any positive integer r, this will be our radius of sight. For a vertex $o \in V_n$ let $B_r(G_n, o)$ be the r-neighborhood of o in the graph G_n, and let $M_{n,r,o}$ be the submatrix of P_n determined by rows and columns with indeces in $B_r(G_n, o)$. Then the outcome of the local sampling at o is the pair $(B_r(G_n, o), M_{n,r,o})$. Of course, we are only interested in the outcome up to rooted isomorphism. Now if we pick o as a uniform random element of V_n, we get a probability measure $\mu_{n,r}$ on the set of isomorphism classes of pairs (H, M), where H is a rooted r-neighborhood and M is a matrix where rows and columns are indexed with the vertices of H. We say that the sequence (G_n, P_n) converges if for any fixed r the measures $\mu_{n,r}$ converge weakly as n tends to infinity. See the next section for more details including the description of the limit object.

To define the notion of tightness, we introduce a measure ν_n on $\mathbb{N} \cup \{\infty\}$ for each pair (G_n, P_n) as follows. Given $k \in \mathbb{N} \cup \{\infty\}$ we set

$$\nu_n(\{k\}) = |V_n|^{-1} \sum_{\substack{u,v \in V_n \\ d_n(u,v)=k}} |P_n(u, v)|^2,$$

where d_n is the graph metric on $V_n = V(G_n)$. Then the sequence (G_n, P_n) is tight if the family of measures ν_n is tight, that is, for each $\varepsilon > 0$ we have a finite R such that

$$\nu_n(\{R+1, R+2, \dots\} \cup \{\infty\}) < \varepsilon$$

for all n. Tightness makes sure that the local sampling procedure from the previous paragraph detects most of the significant matrix entries for large enough r.

Note that a related convergence notion of operators was introduced by Lyons and Thom [43]. We expect that their notion is slightly stronger, but were unable to clarify this.

The idea of the proof of the main theorem is the following. Consider a uniform random ordering of V_n. Then using the chain rule for conditional entropy we can write $H(B^{P_n})$ as the sum of $|V_n|$ conditional entropies. We show that in the limit we can control these conditional entropies. This method in the context of local convergence first appeared in [15].

CEU eTD Collection

Now we describe a special case of our theorem. Consider a finite connected graph G, and consider the uniform measure on the set of spanning trees of G. This measure turns out to be a determinantal measure, the corresponding projection matrix $P_\bigstar(G)$ is called the transfer-current matrix [17]. Since this is a uniform measure, the Shannon-entropy is simply $\log \tau(G)$, where $\tau(G)$ is the number of spanning trees in G. A theorem of Lyons [41] states that if G_n is a Benjamini-Schramm convergent sequence of finite connected graphs then

$$\lim_{n\to\infty} \frac{\log \tau(G_n)}{|V(G_n)|}$$

exists. This theorem now follows from our results, because it is easy to see that the sequence $(L(G_n), P_\bigstar(G_n))$ is convergent and tight in our sense, where $L(G_n)$ is the line graph of G_n. See Section 7. Note that we need to take the line graph of G_n, because the uniform spanning tree measure is defined on the edges of G_n rather than the vertices of G_n. We also obtain a formula for the limit which is different from Lyons's original formula. However, in practice it seems easier to evaluate Lyons's original formula.

Another application comes from ergodic theory. Let Γ be a finitely generated countable group, and let T be an invariant positive contraction on $\ell^2(\Gamma)$. Here a linear operator is called a positive contraction if it is positive semidefinite and has operator norm at most 1. Invariance means that for any $\gamma, g_1, g_2 \in \Gamma$ we have

$$\langle Tg_1, g_2\rangle = \langle T(\gamma^{-1}g_1), \gamma^{-1}g_2\rangle.$$

Note that here we identify elements of Γ with their characteristic vectors. Then the determinantal measure μ_T corresponding to T gives us an invariant measure on $\{0,1\}^\Gamma$. Note that there is a natural graph structure on Γ. Namely, we can fix a finite generating set S, and consider the corresponding Cayley-graph $\mathrm{Cay}(\Gamma, S)$. When Γ belongs to the class of sofic groups, one can define the so-called sofic entropy of this invariant measure [3]. This is done by first considering an approximation of $\mathrm{Cay}(\Gamma, S)$ by a sequence of finite graphs G_n, and then investigating how we can model μ_T on these finite graphs. In general it is not known whether sofic entropy depends on the chosen approximating sequence G_n or not, apart from certain trivial examples. However, in our special case, our results allow us to give a formula for the sofic entropy, which only depends on the measure μ_T, but not on the finite approximations. This shows that in this case the sofic entropy does not depend on the chosen sofic approximation.

Observe that in our main theorem the graphs G_n do not play any role in the definition of the random subsets B^{P_n} or the Shannon entropy $H(B^{P_n})$, they are only there to help us define our convergence notion. This suggests that there might be a notion of convergence of orthogonal projection matrices without any additional graph structure such that the normalized Shannon entropy of B^{P_n} is continuous.

Structure of the chapter. In Section 2 we explain the basic definitions and state our results. In Section 3 we investigate what happens if we condition a Benjamini-Schramm convergence sequence of determinantal measures in a Benjamini-Schramm convergent way. In Sections 4, 5 and 6 we prove the theorems stated in Section 2. In Section 7 we explain the connections

CEU eTD Collection

of our results and Lyons's tree entropy theorem. The proof of a technical lemma about the measurability of the polar decomposition is given in the Appendix.

2 Definitions and statements of the results

2.1 The space of rooted graphs and sofic groups

Fix a degree bound D. A *rooted graph* is a pair (G, o) where G is a (possibly infinite) connected graph with degrees at most D, $o \in V(G)$ is a distinguished vertex of G called the root. Given two rooted graphs (G_1, o_1) and (G_2, o_2) their distance is defined to be the infimum over all $\varepsilon > 0$ such that for $r = \lfloor \varepsilon^{-1} \rfloor$ there is a root preserving graph isomorphism from $B_r(G_1, o_1)$ to $B_r(G_2, o_2)$. Let $\mathcal{G}$ be the set of isomorphism classes of rooted graphs. With the above defined distance $\mathcal{G}$ is a compact metric space. Therefore, the set of probability measures $\mathcal{P}(\mathcal{G})$ endowed with the weak* topology is also compact. A sequence of random rooted graphs (G_n, o_n) *Benjamini-Schramm converges* to the random rooted graph (G, o), if their distributions converge in $\mathcal{P}(\mathcal{G})$. Given any finite graph G, we can turn it into a random rooted graph $U(G) = (G_o, o)$ by considering a uniform random vertex o of G and its connected component G_o. A sequence of finite graphs G_n Benjamini-Schramm converges to the random rooted graph (G, o) if the sequence $U(G_n)$ Benjamini-Schramm converges to (G, o).

Let S be a finite set, an *S-labeled Schreier graph* is a graph where each edge is oriented and labeled with an element from S, moreover for every vertex v of the graph and every $s \in S$ there is exactly one edge labeled with s entering v and there is exactly one edge labeled with s leaving v. For example, if Γ is a group with generating set S, then its Cayley-graph $\mathrm{Cay}(\Gamma, S)$ is an S-labeled Schreier-graph. The notion of Benjamini-Schramm convergence can be extended to the class of S-labeled Schreier-graphs with the modification that graph isomorphisms are required to respect the orientation and labeling of the edges. Let Γ be a finitely generated group. Fix a finite generating set S, and consider the Cayley-graph $G_\Gamma = \mathrm{Cay}(\Gamma, S)$. Let e_Γ be the identity of Γ. We say that Γ is *sofic* if there is a sequence of finite S-labeled Schreier-graphs G_n, such that G_n Benjamini-Schramm converges to (G_Γ, e_Γ).

2.2 The space of rooted graph-operators

Fix a degree bound D, and let K be a non-empty finite set.

A *rooted graph-operator* (RGO) is a triple (G, o, T), where (G, o) is a rooted graph and T is a bounded operator on $\ell^2(V(G) \times K)$. In this chapter we will use real Hilbert spaces, but the results can be generalized to the complex case as well. Note that to prove our main theorem it suffices to only consider the case $|K| = 1$. The usefulness of allowing $|K| > 1$ will be only clear in Section 5, where we extend our results to positive contractions.

Given two RGOs (G_1, o_1, T_1) and (G_2, o_2, T_2) their distance $d((G_1, o_1, T_1), (G_2, o_2, T_2))$ is defined as the infimum over all $\varepsilon > 0$ such that for $r = \lfloor \varepsilon^{-1} \rfloor$ there is a root preserving graph isomorphism

CEU eTD Collection

ψ from $B_r(G_1, o_1)$ to $B_r(G_2, o_2)$ with the property that

$$|\langle T_1(v,k),(v',k')\rangle - \langle T_2(\psi(v),k),(\psi(v'),k')\rangle| < \varepsilon \tag{2.1}$$

for every $v, v' \in V(B_r(G_1, o_1))$ and $k, k' \in K$. Here we identified elements of $V(G_i) \times K$ with their characteristic vectors in $\ell^2(V(G_i) \times K)$.

Two RGOs (G_1, o_1, T_1) and (G_2, o_2, T_2) are called isomorphic if their distance is 0, or equivalently if there is a root preserving graph isomorphism ψ from (G_1, o_1) to (G_2, o_2) such that

$$\langle T_1(v,k),(v',k')\rangle = \langle T_2(\psi(v),k),(\psi(v'),k')\rangle$$

for every $v, v' \in V(G_1)$ and $k, k' \in K$. Let $\mathcal{RGO}$ be the set of isomorphism classes of RGOs. For any $0 < B < \infty$, we define

$$\mathcal{RGO}(B) = \{(G,o,T) \in \mathcal{RGO} | \quad \|T\| \leq B\}.$$

One can prove that $\mathcal{RGO}(B)$ is a compact metric space with the above defined distance d. Let $\mathcal{P}(\mathcal{RGO}(B))$ be the set of probability measures on $\mathcal{RGO}(B)$ endowed with the weak* topology, this is again a compact space. Often it will be more convenient to consider an element $\mathcal{P}(\mathcal{RGO})$ as a random RGO.

A RGO (G, o, T) is called a *rooted graph-positive-contraction* (RGPC) if T is a self-adjoint positive operator with norm at most 1. Then the set $\mathcal{RGPC}$ of isomorphism classes of RGPCs is a compact metric space. Therefore, $\mathcal{P}(\mathcal{RGPC})$ with the weak* topology is compact.

We need a slight generalization of the notion of RGO. An *h-decorated RGO* is a tuple $(G, o, T, A^{(1)}, A^{(2)}, \dots, A^{(h)})$, where G, o and T are like above, $A^{(1)}, A^{(2)}, \dots, A^{(h)}$ are subsets of $V(G) \times K$. Given two h-decorated RGOs $(G_1, o_1, T_1, A_1^{(1)}, A_1^{(2)}, \dots, A_1^{(h)})$ and $(G_2, o_2, T_2, A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(h)})$ their distance is defined as the infimum over all $\varepsilon > 0$ such that for $r = \lfloor \varepsilon^{-1} \rfloor$ there is a root preserving graph isomorphism ψ from $B_r(G_1, o_1)$ to $B_r(G_2, o_2)$ satisfying the property given in (2.1), and for $i = 1, 2, \dots, h$ we have

$$\bar{\psi}(A_1^{(i)} \cap (B_r(G_1, o_1) \times K)) = A_2^{(i)} \cap (B_r(G_2, o_2) \times K),$$

where $\bar{\psi}(v, k) = (\psi(v), k)$.

Two h-decorated RGOs $(G_1, o_1, T_1, A_1^{(1)}, \dots, A_1^{(h)})$ and $(G_2, o_2, T_2, A_2^{(1)}, \dots, A_2^{(h)})$ are called isomorphic if their distance is 0. Let $\mathcal{RGO}_h$ be the set of isomorphism classes of h-decorated RGOs. We also define $\mathcal{RGO}_h(B)$ and $\mathcal{RGPC}_h$ the same way as their non-decorated versions were defined. With the above defined distance they are compact metric spaces. Similarly as before, $\mathcal{P}(\mathcal{RGO}_h(B))$ and $\mathcal{P}(\mathcal{RGPC}_h)$, endowed with the weak* topology, are compact spaces. Whenever the value of h is clear from the context, we omit it and simply use the term "decorated RGO".

CEU eTD Collection

A *finite graph-positive-contraction* is a pair (G, T), where G is finite graph with degrees at most D, and T is a positive contraction on $\ell^2(V(G) \times K)$. It can be turned into a random RGPC

$$U(G, T) = (G_o, o, T_o)$$

by choosing o as a uniform random vertex of G.

Note that all the definitions above depend on the choice of the finite set K. In most of the chapter we can keep K as fixed. Whenever we need to emphasize the specific choice of K, we will refer to K as the support set of RGOs. Unless stated otherwise the support set is always assumed to be K. Let $L \subset K$ and let (G, o, T) be a RGO with support set K. Let P_L be the orthogonal projection from $\ell^2(V(G) \times K)$ to $\ell^2(V(G) \times L) \subset \ell^2(V(G) \times K)$. We define the operator $\mathrm{rest}_L(T)$ on $\ell^2(V(G) \times L)$ as $\mathrm{rest}_L(T) = P_L T \restriction_{\ell^2(V(G)\times L)}$. So $(G, o, \mathrm{rest}_L(T))$ is an RGO with support set L.

Sometimes we need to consider more than one operator on a rooted graph. A *double RGO* will mean a tuple (G, o, T_1, T_2) where (G, o) is a rooted graph and T_1, T_2 are bounded operators on $\ell^2(V(G) \times K)$. We omit the details how the set of isomorphism classes of double RGOs can be turned into a metric space. It is also clear what we mean by a decorated double RGO, or a triple RGO, or a double RGPC.

2.3 Determinantal processes

Let E be a countable set, and T be a positive contraction of $\ell^2(E)$. Then there is a random subset B^T of E with the property that for each finite subset F of E we have

$$\mathbb{P}[F \subset B^T] = \det(\langle Tx, y\rangle)_{x,y\in F},$$

where we identify an element $x \in E$ with its characteristic vector in $\ell^2(E)$. The distribution of B^T is uniquely determined by these constraints, and it is called the *determinantal measure* corresponding to T [42].

Using the definition of the random subset B^T, we can define a map $\tau : \mathcal{RGPC} \to \mathcal{P}(\mathcal{RGPC}_1)$ by $\tau(G, o, T) = (G, o, T, B^T)$. This induces a map $\tau_* : \mathcal{P}(\mathcal{RGPC}) \to \mathcal{P}(\mathcal{P}(\mathcal{RGPC}_1))$. Taking expectation we get the map $\mathbb{E}\tau_* : \mathcal{P}(\mathcal{RGPC}) \to \mathcal{P}(\mathcal{RGPC}_1)$. So given a random RGPC (G, o, T) the meaning of (G, o, T, B^T) is ambiguous. Unless stated otherwise (G, o, T, B^T) will mean a random decorated RGPC, i.e., its distribution is an element of $\mathcal{P}(\mathcal{RGPC}_1)$.

Proposition 2.1. *The maps τ, τ_* and $\mathbb{E}\tau_*$ are continuous.*

2.4 Trace and spectral measure

Given a random RGO (G, o, T) we define

$$\mathrm{Tr}(G, o, T) = \mathbb{E} \sum_{k\in K} \langle T(o, k), (o, k)\rangle.$$

CEU eTD Collection

We extend the definition to the decorated case in the obvious way.

Given a random RGPC (G,o,T) its *spectral measure* is the unique measure $\mu=\mu_{(G,o,T)}$ on $[0,1]$ with the property that, for any integer $n\geq 0$ we have

$$\mathrm{Tr}(G,o,T^n)=\int_0^1 x^n d\mu.$$

Note that $\mu([0,1])=|K|$. Also if T is a projection with probability 1, then we have

$$\mu=\mathrm{Tr}(G,o,T)\delta_1+(|K|-\mathrm{Tr}(G,o,T))\delta_0.$$

If (G,T) is a finite graph-positive-contraction, then the spectral measure of $U(G,T)$ can be obtained as

$$\frac{1}{|V(G)|}\sum_{i=1}^{|V(G)\times K|}\delta_{\lambda_i},$$

where $\lambda_1,\lambda_2,\dots,\lambda_{|V(G)\times K|}$ are the eigenvalues of T with multiplicity.

2.5 An equivalent characterization of tightness

We already defined the notion of tightness in the Introduction. Here we repeat the definition in a slightly more general setting. For a finite graph-positive-contraction (G,T) we define the measure $\nu_{(G,T)}$ on $\mathbb{N}\cup\{\infty\}$ by setting

$$\nu_{(G,T)}(\{t\})=|V(G)|^{-1}\sum_{\substack{(v_1,k_1),(v_2,k_2)\in V(G)\times K\\ d_G(v_1,v_2)=t}}|\langle T(v_1,k_1),(v_2,k_2)\rangle|^2,$$

for all $t\in\mathbb{N}\cup\{\infty\}$. A sequence (G_n,T_n) of finite graph-positive-contractions is tight if the family of measures $\nu_{(G_n,T_n)}$ is tight, that is, for each $\varepsilon>0$ we have a finite R such that

$$\nu_{(G_n,T_n)}(\{R+1,R+2,\dots\}\cup\{\infty\})<\varepsilon$$

for all n. The next lemma gives an equivalent characterization of tightness.

Lemma 2.2. *Let (G_n,P_n) be a Benjamini-Schramm convergent sequence of finite graph-positive-contractions with limit (G,o,T). Assume that $P_1,P_2,\dots$ are orthogonal projections. Then the following are equivalent*

i) The sequence (G_n,P_n) is tight.

ii) The limit T is an orthogonal projection with probability 1 and $\nu_{(G_n,P_n)}(\{\infty\})=0$ for every n.

Proof. i)$\Rightarrow$ ii): Recall the following well-known result.

CEU eTD Collection

Proposition 2.3. *Let E be a countable set, and let T be a positive contraction on $\ell^2(E)$. Then for all $e \in E$ we have $\langle T^2 e, e\rangle \le \langle Te, e\rangle$. Moreover, if for all $e \in E$ we have $\langle T^2 e, e\rangle = \langle Te, e\rangle$, then T is an orthogonal projection.*

Let $(H_n, o_n, T_n) = U(G_n, P_n)$. Then

$$\nu_{(G_n,P_n)}(\mathbb{N} \cup \{\infty\}) = |V(G_n)|^{-1} \operatorname{Tr}(P_n^* P_n) = |V(G_n)|^{-1} \operatorname{Tr}(P_n) = \operatorname{Tr}(H_n, o_n, T_n).$$

Combining this with the definition of tightness we get that for any $\varepsilon > 0$ we have an R such that

$$\mathbb{E} \sum_{k \in K} \sum_{(v,k') \in B_R(H_n,o_n) \times K} |\langle T_n(o_n, k), (v, k')\rangle|^2 > \operatorname{Tr}(H_n, o_n, T_n) - \varepsilon \tag{2.2}$$

for every n.

Using the convergence of (H_n, o_n, T_n) we get that

$$\lim_{n\to\infty} \operatorname{Tr}(H_n, o_n, T_n) = \operatorname{Tr}(G, o, T),$$

and

$$\lim_{n\to\infty} \mathbb{E} \sum_{k \in K} \sum_{(v,k') \in B_R(H_n,o_n) \times K} |\langle T_n(o_n, k), (v, k')\rangle|^2 = \mathbb{E} \sum_{k \in K} \sum_{(v,k') \in B_R(G,o) \times K} |\langle T(o, k), (v, k')\rangle|^2.$$

Combining these with inequality (2.2) we get that

$$\begin{aligned}\operatorname{Tr}(G, o, T^2) &= \mathbb{E} \sum_{k \in K} \sum_{(v,k') \in V(G) \times K} |\langle T(o, k), (v, k')\rangle|^2 \\ &\ge \mathbb{E} \sum_{k \in K} \sum_{(v,k') \in B_R(G,o) \times K} |\langle T(o, k), (v, k')\rangle|^2 \ge \operatorname{Tr}(G, o, T) - \varepsilon.\end{aligned}$$

Tending to 0 with ε we get that

$$\operatorname{Tr}(G, o, T^2) \ge \operatorname{Tr}(G, o, T).$$

Combining this with the first statement of Proposition 2.3 we get that with probability 1 we have $\langle T^2(o, k), (o, k)\rangle = \langle T(o, k), (o, k)\rangle$ for every $k \in K$. But then it follows from the unimodularity of (G, o, T) that with probability 1 we have $\langle T^2(v, k), (v, k)\rangle = \langle T(v, k), (v, k)\rangle$ for any $(v, k) \in V(G) \times K$. See [4, Lemma 2.3 (Everything Shows at the Root)] and Section 3. Then Proposition 2.3 gives us that T is a projection with probability 1. From the definition of tightness it is clear that $\nu_n(\{\infty\}) = 0$ for every n.

ii)$\Rightarrow$ i): Pick any $\varepsilon > 0$. From the monotone convergence theorem and the fact that T is a projection with probability 1, we have

CEU eTD Collection

$$\begin{aligned}\operatorname{Tr}(G,o,T) = \operatorname{Tr}(G,o,T^2) &= \mathbb{E}\sum_{k\in K}\sum_{(v,k')\in V(G)\times K} |\langle T(o,k),(v,k')\rangle|^2\\ &= \lim_{R\to\infty}\mathbb{E}\sum_{k\in K}\sum_{(v,k')\in B_R(G,o)\times K} |\langle T(o,k),(v,k')\rangle|^2.\end{aligned}$$

Thus, if we choose a large enough R_0, then we have

$$\operatorname{Tr}(G,o,T) - \mathbb{E}\sum_{k\in K}\sum_{(v,k')\in B_{R_0}(G,o)\times K} |\langle T(o,k),(v,k')\rangle|^2 < \frac{\varepsilon}{2}.$$

Then from the convergence of (H_n, o_n, T_n) we get that there is an N such that if $n > N$ we have

$$\begin{aligned}&\nu_{(G_n,P_n)}(\{R_0+1, R_0+2,\dots\}\cup\{\infty\}) =\\ &\qquad \operatorname{Tr}(H_n,o_n,T_n) - \mathbb{E}\sum_{k\in K}\sum_{(v,k')\in B_{R_0}(H_n,o_n)\times K} |\langle T_n(o_n,k),(v,k')\rangle|^2 < \varepsilon.\end{aligned}$$

Using the condition that $\nu_{(G_n,P_n)}(\{\infty\}) = 0$ for all n and the definition of $\nu_{(G_n,P_n)}$ we get that the support of the measure $\nu_{(G_n,P_n)}$ is contained in $\{0,1,\dots,|V(G_n)|\}$. Thus, the choice $R = \max(R_0, |V(G_1)|, |V(G_2)|,\dots,|V(G_N)|)$ is good for ε. □

2.6 Sofic entropy

Let C be a finite set and let Γ be a finitely generated group. Let f be a random coloring of Γ with C, that is a random element of C^Γ. (The measurable structure of C^Γ comes from the product topology on C^Γ.) Given a coloring $f \in C^\Gamma$ and $\gamma\in\Gamma$ we define the coloring f_γ by $f_\gamma(g) = f(\gamma^{-1}g)$ for all $g\in\Gamma$. This notation extends to random colorings in the obvious way. A random coloring f is invariant if for every $\gamma\in\Gamma$ the distribution of f_γ is the same as the distribution of f.

Now assume that Γ is a finitely generated sofic group, and f is an invariant random coloring of Γ. Let S be a finite generating set, and let $G_1, G_2,\dots$ be a sequence of S-labeled Schreier-graphs Benjamini-Schramm converging to the Cayley-graph $G_\Gamma = \operatorname{Cay}(\Gamma, S)$. Now we define the so called *sofic entropy* of f. There are many slightly different versions of this notion [16, 5], we will follow Abért and Weiss [3]. Let G be a finite S-labeled Schreier graph and g be a random coloring of $V(G)$. Given $\varepsilon > 0$ and a positive integer r, we say that g is an (ε, r) approximation of f on the graph G, if there are at least $(1-\varepsilon)|V(G)|$ vertices $v\in V(G)$, such that $B_r(G,v)$ is isomorphic to $B_r(G_\Gamma, e_\Gamma)$, moreover $d_{TV}(f\restriction B_r(G_\Gamma,e_\Gamma), g\restriction B_r(G,v)) < \varepsilon$, where d_{TV} is the total variational distance, and it is meant that we identify $B_r(G_\Gamma, e_\Gamma)$ and $B_r(G,v)$. Let us define

$$H(G,\varepsilon,r) = \sup\left\{\frac{H(g)}{|V(G)|}\ \middle|\ g \text{ is an } (\varepsilon,r) \text{ approximation of } f \text{ on } G\right\}.$$

CEU eTD Collection

Here $H(g)$ is the Shannon-entropy of g. Let $H(\varepsilon, r)$ be the supremum of $H(G, \varepsilon, r)$, over all finite S-labeled Schreier graphs G. We define two versions of sofic entropy. The first one

$$h(f) = \inf_{\varepsilon, r} \limsup_{n\to\infty} H(G_n, \varepsilon, r).$$

Note that this might depend on the chosen sofic approximation. Another option is to define sofic entropy as

$$h'(f) = \inf_{\varepsilon, r} H(\varepsilon, r).$$

Observe that $h'(f) \geq h(f)$. It is open whether $h'(f) = h(f)$ for any sofic approximation apart from trivial counterexamples. We can also express these quantities as

$$h(f) = \inf_{\varepsilon} \limsup_{n\to\infty} H(G_n, \varepsilon, \lfloor \varepsilon^{-1} \rfloor) \text{ and } h'(f) = \inf_{\varepsilon} H(\varepsilon, \lfloor \varepsilon^{-1} \rfloor).$$

The quantities $h(f)$ and $h'(f)$ are isomorphism invariants in the abstract ergodic theoretic sense.

Remark. Sofic entropy can be defined in a more general setting. Namely, let Q be a locally finite vertex transitive graph. Let o be any vertex of it. Assume that (Q, o) is a Benjamini-Schramm limit of finite graphs. Let f be a random coloring of $V(Q)$ with C such that the distribution of f is invariant under all automorphisms of Q. We would like to define the sofic entropy of f the same way as above. The only problematic point is that in the definition of (ε, r)-approximation we need to identify $B_r(G, v)$ with $B_r(Q, o)$. But $B_r(Q, o)$ might have non-trivial automorphisms, in which case there are more than one possible identifications and it is not clear which we should choose. If all the automorphisms $B_r(Q, o)$ can be extended to an automorphism of Q, then we can choose any identification, because they all give the same total variation distance. But if $B_r(Q, o)$ has other automorphisms then things get more complicated. However, one can overcome these difficulties and get a sensible notion of sofic entropy [3]. Here we do not give the details, we just mention that Theorem 2.6 stated in the next subsection can be extended to this more general setting.

2.7 Our main theorems

Let E be a countable set, and T be a positive contraction on $\ell^2(E)$. Let c be a $[0, 1]$ labeling of E. For $e \in E$ let $I(e)$ be the indicator of the event that $e \in B^T$. For $e \in E$ we define

$$\bar{h}(e, c, T) = H(I(e) | \{I(f) | c(f) < c(e)\}).$$

Here, H is the conditional entropy, that is, with the notation

$$g(x) = -x \log x - (1 - x) \log(1 - x),$$

we have

$$H(I(e) | \{I(f) | c(f) < c(e)\}) = \mathbb{E} g(\mathbb{E}[I(e) | \{I(f) | c(f) < c(e)\}]).$$

CEU eTD Collection

Moreover, we define
$$\bar{h}(e,T) = \mathbb{E}\bar{h}(e,c,T),$$
where c is an i.i.d. uniform $[0,1]$ labeling of E.

For a random RGPC (G,o,T) we define
$$\bar{h}(G,o,T) = \mathbb{E}\sum_{k\in K}\bar{h}((o,k),T).$$

If $L\subset K$ and (G,T) is a finite graph-positive-contraction we define $h_L(G,T)$ to be the Shannon entropy of $B^T\cap(V(G)\times L)$.

Theorem 2.4. *Let (G_n,P_n) be a sequence of finite graph-positive-contractions, such that $\lim_{n\to\infty}U(G_n,P_n)=(G,o,P)$ for some random RGPC (G,o,P). Assume that $P_1,P_2,\dots$ are orthogonal projections, and P is an orthogonal projection with probability 1. Let $L\subset K$. Then*
$$\lim_{n\to\infty}\frac{h_L(G_n,P_n)}{|V(G_n)|} = \bar{h}(G,o,\mathrm{rest}_L(P)).$$

Using Lemma 2.2 we immediately get the following theorem.

Theorem 2.5. *Let (G_n,P_n) be a* ***tight*** *sequence of finite graph-positive-contractions, such that $\lim_{n\to\infty}U(G_n,P_n)=(G,o,P)$ for some random RGPC (G,o,P). Assume that $P_1,P_2,\dots$ are orthogonal projections. Let $L\subset K$. Then*
$$\lim_{n\to\infty}\frac{h_L(G_n,P_n)}{|V(G_n)|} = \bar{h}(G,o,\mathrm{rest}_L(P)).$$

Let Γ be a finitely generated sofic group. A positive contraction T on $\ell^2(\Gamma\times K)$ is called invariant, if for any $\gamma,g_1,g_2\in\Gamma$ and $k_1,k_2\in K$ we have
$$\langle T(g_1,g_1),(g_2,k_2)\rangle = \langle T(\gamma^{-1}g_1,k_1),(\gamma^{-1}g_2,k_2)\rangle.$$

For an invariant positive contraction if we regard the random subset B^T as a random coloring with $\{0,1\}^K$, we see that B^T is an invariant coloring. Thus we can speak about its sofic entropy.

As before let S be a finite generating set of Γ, let e_Γ be the identity of Γ, and $G_\Gamma=\mathrm{Cay}(\Gamma,S)$ be the Cayley-graph of Γ.

Theorem 2.6. *Let Γ be a finitely generated sofic group. If T is an invariant positive contraction on $\ell^2(\Gamma\times K)$ then we have*
$$h(B^T) = h'(B^T) = \bar{h}(G_\Gamma,e_\Gamma,T)$$
for any sofic approximation of Γ.

CEU eTD Collection

Note that we can easily generalize the definition of $\bar{h}$ to any invariant random coloring f. It is known that even in this more general setting $\bar{h}$ is an upper bound on the sofic entropy. However, $\bar{h}$ is not an isomorphism invariant in the ergodic theoretic sense. See [55].

The random ordering idea above was used by Borgs, Chayes, Kahn and Lovász [15] to give the growth of the partition function and entropy of certain Gibbs measures at high temperature on Benjamini-Schramm convergent graph sequences. See also [6].

2.8 An example: Why tightness is necessary?

We consider two connected graphs H_1 and H_2. Let H_1 be the complete graph on 4 vertices, and let H_2 be the graph that is obtained from a star with 3 edges by doubling each edge. Both have 4 vertices and 6 edges. Let T_i be a uniform random spanning tree of H_i, and let P_i be the corresponding 6×6 transfer-current matrix. It is straightforward to check that for any $e \in E(H_i)$ we have $\mathbb{P}(e \in T_i) = \frac{1}{2}$. Thus, in both P_1 and P_2 all the diagonal entries are equal to $\frac{1}{2}$. Now let G_i be the empty graph on the vertex set $E(H_i)$. Then the pairs (G_1, P_1) and (G_2, P_2) are indistinguishable by local sampling, that is, $U(G_1, P_1)$ and $U(G_2, P_2)$ have the same distribution. On the other hand H_1 has 16 spanning trees, and H_2 has only 8 spanning trees. So $|V(G_1)|^{-1}H(B^{P_1}) \neq |V(G_2)|^{-1}H(B^{P_2})$. This shows that the condition of tightness can not be omitted in Theorem 2.5. One could think that this only works, because the graphs G_1 and G_2 are not connected. But Theorem 2.5 still fails without the assumption of tightness, even if we assume that all the graphs are connected. We sketch the main idea. Let $i \in \{1, 2\}$. For each n we consider a block diagonal matrix $B_{i,n}$, where we have n diagonal blocks each of which equal to P_i. Then we take a connected graph $G_{i,n}$ on $V_{i,n}$ (the set of columns of $B_{i,n}$) in such a way that if two columns are in the same block, then they must be at least at distance $d(n)$ in the graph $G_{i,n}$ for some $d(n)$ tending to infinity. Moreover, we can choose $G_{i,n}$ such that the sequences $(G_{1,n})$ and $(G_{2,n})$ have the same Benjamini-Schramm limit (G, o). Then both of the sequences $(G_{1,n}, B_{1,n})$ and $(G_{2,n}, B_{2,n})$ have the same limit, namely, $(G, o, \frac{1}{2}I)$. But their asymptotic entropies are different.

3 Unimodularity and conditional determinantal processes

3.1 Unimodularity

We define bi-rooted graph-operators as tuples (G, o, o', T), where G is a connected graph with degree bound D, $o, o' \in V(G)$ and T is a bounded operator on $\ell^2(V(G) \times K)$. Let $bi\mathcal{RGO}$ be the set of isomorphism classes of bi-rooted graph-operators. We omit the details how to endow this space with a measurable structure. A random RGO (G, o, T) is called *unimodular*, if for any non-negative measurable function $f : bi\mathcal{RGO} \to \mathbb{R}$ we have

$$\mathbb{E} \sum_{v \in V(G)} f(G, o, v, T) = \mathbb{E} \sum_{v \in V(G)} f(G, v, o, T).$$

CEU eTD Collection

The next lemma gives some examples of unimodular random RGOs. The proof goes like the one given in [10].

Lemma 3.1. *If* (G, T) *is a finite graph-positive-contraction, then* $U(G, T)$ *is unimodular. The limit of unimodular random RGOs is unimodular.*

Of course the notion of unimodularity can be extended to double/triple (decorated) RGOs. We will use the following consequence of unimodularity.

Lemma 3.2. *Let* (G, o, T, S) *be a unimodular random double RGO. Assume that there is a finite* B *such that* $\|T\|, \|S\| < B$ *with probability* 1. *Then*

$$\mathrm{Tr}(G, o, TS) = \mathrm{Tr}(G, o, ST).$$

Proof. The proof is the same as in [4, Section 5]. □

It has the following consequences.

Lemma 3.3. *In the following statements we always assume that* P *and* P_i *are all orthogonal projections with probability* 1.

1. *Let* (G, o, P_1, P_2, U) *be a unimodular random triple RGO, such that with probability* 1 *we have* $U \restriction \ker P_1 \equiv 0$ *and* $U \restriction \mathrm{Im}\, P_1$ *is an isomorphism between* $\mathrm{Im}\, P_1$ *and* $\mathrm{Im}\, P_2$. *Then*

$$\mathrm{Tr}(G, o, P_1) = \mathrm{Tr}(G, o, P_2).$$

2. *Let* (G, o, P_1, P_2, T) *be a unimodular random triple RGO, such that with probability* 1 *we have* $\overline{\mathrm{Im}\, TP_1} = \mathrm{Im}\, P_2$ *and* T *is injective on* $\mathrm{Im}\, P_1$. *Then*

$$\mathrm{Tr}(G, o, P_1) = \mathrm{Tr}(G, o, P_2).$$

3. *(rank-nullity theorem) Let* (G, o, P, P_1, P_2, T) *be a unimodular random quadruple RGO, such that with probability* 1 *we have that* P_1 *is the orthogonal projection to* $\ker(T \restriction \mathrm{Im}\, P)$ *and* P_2 *is the orthogonal projection to* $\overline{\mathrm{Im}(T \restriction \mathrm{Im}\, P)}$. *Then*

$$\mathrm{Tr}(G, o, P) = \mathrm{Tr}(G, o, P_1) + \mathrm{Tr}(G, o, P_2).$$

Proof. To prove part 1 observe that $P_1 U^* U = P_1$ and $U P_1 U^* = P_2$. Note that all operators have norm at most 1, so from Lemma 3.2

$$\mathrm{Tr}(G, o, P_1) = \mathrm{Tr}(G, o, (P_1 U^*) U) = \mathrm{Tr}(G, o, U(P_1 U^*)) = \mathrm{Tr}(G, o, P_2).$$

To prove part 2 let $TP_1 = UH$ be the unique polar decomposition of TP_1, then (G, o, P_1, P_2, UP_1) satisfies the conditions in part 1, so the statement follows. The rather technical details why the

CEU eTD Collection

polar decomposition is measurable are given in the Appendix. Note that once we established the measurability of U, unimodularity follows from the uniqueness of the decomposition.

To prove part 3 let $H = \operatorname{Im} P \cap (\ker T \restriction \operatorname{Im} P)^\perp$. Let P_H be the orthogonal projection to H, then we have $P = P_1 + P_H$. Therefore, $\operatorname{Tr}(G, o, P) = \operatorname{Tr}(G, o, P_1) + \operatorname{Tr}(G, o, P_H)$. It is also clear that $\overline{\operatorname{Im} TP} = \overline{\operatorname{Im}(T \restriction H)}$ and T is injective on H. Thus part 2 gives us $\operatorname{Tr}(G, o, P_H) = \operatorname{Tr}(G, o, P_2)$. Putting everything together we obtain that

$$\operatorname{Tr}(G, o, P) = \operatorname{Tr}(G, o, P_1) + \operatorname{Tr}(G, o, P_H) = \operatorname{Tr}(G, o, P_1) + \operatorname{Tr}(G, o, P_2).$$

□

3.2 Conditional determinantal processes

Let P be an orthogonal projection to a closed subspace H of $\ell^2(E)$. Given $C \subset E$, let $[C]$ be the closed subspace generated by $e \in C$, and let $[C]^\perp$ be the orthogonal complement of it. Note that $[C]^\perp = [E \backslash C]$. We define $P_{/C}$ as the orthogonal projection to the closed subspace $(H \cap [C]^\perp) + [C]$, and $P_{\times C}$ as the orthogonal projection to the closed subspace $H \cap [C]^\perp$. We also define $P_{-C} = I - (I - P)_{/C}$.

Proposition 3.4. *We have $P_{/C} = P_{\times C} + P_{[C]}$, where $P_{[C]}$ is the orthogonal projection to $[C]$. In other words $P_{/C} e = e$ for $e \in C$ and $P_{/C} e = P_{\times C} e$ for $e \in E \backslash C$. Moreover, if C_n is an increasing sequence of subsets of E and $C = \cup C_n$, then $P_{/C_n}$ converges to $P_{/C}$ in the strong operator topology. Furthermore, the sequence $\langle P_{\times C_n} e, e\rangle$ is monotone decreasing.*

Proof. The first statement is trivial. To prove the second statement, observe that $P_{\times C_n}$ is a sequence of orthogonal projections to a monotone decreasing sequence of closed subspaces with intersection $\operatorname{Im} P_{\times C}$, so $P_{\times C_n}$ converge to $P_{\times C}$ in the strong operator topology. It is also clear that $P_{[C_n]}$ converge to $P_{[C]}$, so from $P_{/C_n} = P_{\times C_n} + P_{[C_n]}$ the statement follows. To prove the third statement observe that $\langle P_{\times C_n} e, e\rangle = \|P_{\times C_n} e\|_2^2$. So the statement follows again from the fact that $P_{\times C_n}$ is a sequence of orthogonal projections to a monotone decreasing sequence of closed subspaces. □

For $C, D \subset E$ we define $P_{/C-D} = (P_{/C})_{-D}$, and we define $P_{-D/C} = (P_{-D})_{/C}$. We only include the next lemma here to make it easier to compare formulas in [42] with our formulas.

Lemma 3.5. *Let P be an orthogonal projection to a closed subspace H. Then for any $D \subset E$ we have*

$$\operatorname{Im} P_{-D} = \overline{H + [D]} \cap [D]^\perp.$$

Moreover, if C and D are disjoint subsets of E, then

$$\operatorname{Im} P_{/C-D} = \overline{(H \cap [C]^\perp) + [C \cup D]} \cap [D]^\perp$$

and

$$\operatorname{Im} P_{-D/C} = (\overline{H + [D]} \cap [C \cup D]^\perp) + [C].$$

CEU eTD Collection

If C and D are finite, then the above formulas are true even if we omit the closures.

Proof. We only prove the first statement. The other statements can be easily deduced from it. Unpacking the definitions we need to prove that

$$((H^{\perp} \cap [D]^{\perp}) + [D])^{\perp} = \overline{H + [D]} \cap [D]^{\perp}.$$

As a first step observe that $\overline{H + [D]} \cap [D]^{\perp} = \overline{\mathrm{Im}(P_{[D]^{\perp}} \restriction H)}$. Indeed, if $x \in \overline{(\mathrm{Im}\, P_{[D]^{\perp}} \restriction H)}$, then $x = \lim x_n$, where for all n we have $x_n \in [D]^{\perp}$ and there is an $y_n \in [D]$ such that $x_n + y_n \in H$. But then $x_n = (x_n + y_n) - y_n \in H + [D]$, which implies that $x \in \overline{H + [D]}$. Clearly $x \in [D]^{\perp}$, so $x \in \overline{H + [D]} \cap [D]^{\perp}$.

To prove the other containment let $x \in \overline{H + [D]} \cap [D]^{\perp}$, then $x = \lim x_n$ where $x_n = y_n + z_n$ with $y_n \in H$ and $z_n \in [D]$. Since $P_{[D]^{\perp}}$ is continuous, we have

$$x = P_{[D]^{\perp}} x = \lim P_{[D]^{\perp}}(y_n + z_n) = \lim P_{[D]^{\perp}} y_n \in \overline{\mathrm{Im}(P_{[D]^{\perp}} \restriction H)}.$$

Now it is easy to see that we need to prove that

$$(H^{\perp} \cap [D]^{\perp}) + [D] = (\mathrm{Im}\, P_{[D]^{\perp}} \restriction H)^{\perp}.$$

First let $x \in (\mathrm{Im}\, P_{[D]^{\perp}} \restriction H)^{\perp}$. Then for any $h \in H$ we have

$$0 = \langle x, P_{[D]^{\perp}} h \rangle = \langle P_{[D]^{\perp}} x, h \rangle,$$

which implies that $P_{[D]^{\perp}} x \in H^{\perp} \cap [D]^{\perp}$. Thus, $x = P_{[D]^{\perp}} x + P_{[D]} x \in (H^{\perp} \cap [D]^{\perp}) + [D]$. To show the other containment let us consider $x = y + z$ such that $y \in H^{\perp} \cap [D]^{\perp}$ and $z \in [D]$. Then for any $h \in H$ we have

$$\langle x, P_{[D]^{\perp}} h \rangle = \langle P_{[D]^{\perp}} x, h \rangle = \langle y, h \rangle = 0,$$

because $y \in H^{\perp}$.

For the last statement, see the discussion in the paper [42] after the proof of Corollary 6.4. □

CEU eTD Collection

We have the following lemma. See [42, Equation (6.5)].

Lemma 3.6. *Let C and D be disjoint finite subsets of E such that $\mathbb{P}[B^P \cap (C \cup D) = C] > 0$. Then $P_{/C-D} = P_{-D/C}$ and conditioned on the event $B^P \cap (C \cup D) = C$, the distribution of B^P is the same as that of $B^{P_{/C-D}}$.*

The lemma above shows why the pairs (C, D) of finite disjoint sets with the property that $\mathbb{P}[B^P \cap (C \cup D) = C] > 0$ are interesting for us. The next proposition gives an equivalent characterization of these pairs.

Proposition 3.7. *Let C and D be disjoint finite subsets of E. Then we have $\mathbb{P}[B^P \cap (C \cup D) = C] > 0$ if and only if $\mathrm{Im}\, P_{[C]} P = [C]$ and $\mathrm{Im}\, P_{[D]}(I - P) = [D]$.*

This motivates the following definitions. A (not necessary finite) subset C of E is called *independent* (with respect to P) if $\overline{\operatorname{Im} P_{[C]}P} = [C]$. A subset D of E is called *dually* independent (with respect to P) if $\overline{\operatorname{Im} P_{[D]}(I-P)} = [D]$. A pair (C, D) of subsets of E is called *permitted* (with respect to P) if C and D are disjoint, C is independent and D is dually independent.

We will need the following theorem of Lyons [42, Theorem 7.2].

Theorem 3.8. *The pair $(B^P, E\backslash B^P)$ is permitted with probability* 1.

We will also need the following statements.

Proposition 3.9. *If (C, D) is permitted, $C' \subset C$ and $D' \subset D$, then (C', D') is permitted.*

Proposition 3.10. *Assume (C, D) is a permitted pair. Then D is dually independent with respect to $P_{/C}$, or equivalently, D is independent with respect to $I - P_{/C}$.*

Proof. By the definition of a permitted pair $\overline{\operatorname{Im} P_{[D]}(I-P)} = [D]$, so it is enough to show that $\operatorname{Im} P_{[D]}(I-P) \subset \operatorname{Im} P_{[D]}(I-P_{/C})$. Take any $r \in \operatorname{Im} P_{[D]}(I-P)$, then there is x such that $r = P_{[D]}(I-P)x$. Let $y = P_{[C]^\perp}(I-P)x$. We claim that $y \in \operatorname{Im}(I-P_{/C})$, or in other words, y is orthogonal to any element $w \in \operatorname{Im} P_{/C}$. We can write w as $w = w_0 + w_1$, where $w_0 \in \operatorname{Im} P \cap [C]^\perp$ and $w_1 \in [C]$. We have

$$\langle y, w_0\rangle = \langle P_{[C]^\perp}(I-P)x, w_0\rangle = \langle (I-P)x, P_{[C]^\perp} w_0\rangle = \langle (I-P)x, w_0\rangle = 0,$$

since $w_0 \in \operatorname{Im} P$. Moreover $\langle y, w_1\rangle = 0$, because $y \in [C]^\perp$ and $w_1 \in [C]$. Thus, $\langle y, w\rangle = 0$, so y is indeed in the image of $I - P_{/C}$, then $P_{[D]}y$ is in the image of $P_{[D]}(I-P_{/C})$. Using that C and D are disjoint $P_{[D]}y = P_{[D]}P_{[C]^\perp}(I-P)x = P_{[D]}(I-P)x = r$. □

Assume for a moment that E is finite, then $|B^P| = \dim \operatorname{Im} P$ with probability 1. If (C, D) is a permitted pair, then the distribution of $B^{P_{/C-D}}$ is the same as that of B^P conditioned on the event that $B^P \cap (C \cup D) = C$. So $|B^{P_{/C-D}}| = \dim \operatorname{Im} P$ with probability 1. In particular, $\mathbb{E}|B^P| = \mathbb{E}|B^{P_{/C-D}}|$. The next lemma extends this statement to the more general unimodular setting.

Lemma 3.11. *Let (G, o, P, C, D) be a unimodular random decorated RGPC where P is an orthogonal projection and the pair (C, D) is permitted with probability* 1. *Then*

$$\operatorname{Tr}(G, o, P) = \operatorname{Tr}(G, o, P_{/C-D}) = \operatorname{Tr}(G, o, P_{-D/C}).$$

This can be obtained from combining Proposition 3.10 and the following lemma.

Lemma 3.12. *Let (G, o, P, C) be a unimodular random decorated RGPC where P is an orthogonal projection and C is independent with probability* 1. *Then*

$$\operatorname{Tr}(G, o, P) = \operatorname{Tr}(G, o, P_{/C}).$$

CEU eTD Collection

We also have the corresponding dual statement, that is, let (G, o, P, D) be a unimodular random decorated RGPC where P is an orthogonal projection and D is dually independent with probability 1. Then

$$\mathrm{Tr}(G, o, P) = \mathrm{Tr}(G, o, P_{-D}).$$

Proof. We only need to prove the first statement, because the second one can be obtained by applying the first statement to $I - P$.

Observe that $\ker(P_{[C]} \restriction \operatorname{Im} P) = \operatorname{Im} P_{\times C}$ from the definition of $P_{\times C}$, moreover, $\overline{\operatorname{Im}(P_{[C]} \restriction \operatorname{Im} P)} = [C]$, because C is independent. Applying the rank nullity theorem (Lemma 3.3.3) and then using the fact $P_{/C} = P_{\times C} + P_{[C]}$ from Proposition 3.4 we get that

$$\mathrm{Tr}(G, o, P) = \mathrm{Tr}(G, o, P_{\times C}) + \mathrm{Tr}(G, o, P_{[C]}) = \mathrm{Tr}(G, o, P_{\times C} + P_{[C]}) = \mathrm{Tr}(G, o, P_{/C}).$$

□

The next lemma gives an extension of Lemma 3.6.

Lemma 3.13. *Let $F \subset E$, and assume that*

$$\langle P_{/B^P \cap F - F \setminus B^P} e, e\rangle = \langle P_{-F \setminus B^P / B^P \cap F} e, e\rangle$$

for all $e \in E$ with probability 1. Then for any finite $A \subset E$ we have

$$\mathbb{P}(A \subset B^P | B^P \restriction F) = \mathbb{P}(A \subset B^{P_{/B^P \cap F - F \setminus B^P}}).$$

Proof. Let $F_1, F_2, \dots$ be an increasing sequence of finite sets such that their union is F. The crucial step in the proof is the following lemma.

Lemma 3.14. *Let (C, D) be a permitted pair, such that $C \cup D = F$. Then $\langle P_{/C-D} e, e\rangle \le \langle P_{-D/C} e, e\rangle$ for all $e \in E$. Now assume that $\langle P_{/C-D} e, e\rangle = \langle P_{-D/C} e, e\rangle$ for all $e \in E$. Let us define $P_n = P_{/C \cap F_n - D \cap F_n}$. Then $B^{P_{/C-D}}$ is the weak limit of B^{P_n}.*

Proof. Let A be a finite set such that, $A \cap F = \emptyset$, moreover let $\mathcal{A}$ be an upwardly closed subset of 2^A, i.e. if $X \subset Y \subset A$ and $X \in \mathcal{A}$, then $Y \in \mathcal{A}$. Using that determinantal measures have negative associations ([42, Theorem 6.5]) we get the following inequality for $m > n$

$$\mathbb{P}[B^{P_n} \cap A \in \mathcal{A}] = \mathbb{P}[B^{P_{/C \cap F_n - D \cap F_n}} \cap A \in \mathcal{A}] \ge \mathbb{P}[B^{P_{/C \cap F_m - D \cap F_n}} \cap A \in \mathcal{A}].$$

Tending to infinity with m, we get that

$$\mathbb{P}[B^{P_n} \cap A \in \mathcal{A}] \ge \mathbb{P}[B^{P_{/C-D \cap F_n}} \cap A \in \mathcal{A}]. \tag{3.1}$$

To justify this last statement, let $\mathcal{U}$ be the set of orthogonal projections R such that $D \cap F_n$ is dually independent with respect to R. Combining Proposition 3.9 and Proposition 3.10, we obtain

CEU eTD Collection

that $P_{/C\cap F_m}$ and $P_{/C}$ are all contained in $\mathcal{U}$. For $R\in\mathcal{U}$, the probability $\mathbb{P}[B^{R_{-D\cap F_n}}\cap A\in\mathcal{A}]$ is a continuous function of $(\langle Re,f\rangle)_{e,f\in A\cup(D\cap F_n)}$. As we proved in Proposition 3.4, $P_{/C\cap F_m}$ tends to $P_{/C}$ in the strong operator topology. Thus,

$$\lim_{m\to\infty}\mathbb{P}[B^{P_{/C\cap F_m-D\cap F_n}}\cap A\in\mathcal{A}]=\mathbb{P}[B^{P_{/C-D\cap F_n}}\cap A\in\mathcal{A}].$$

This gives us Inequality (3.1).

Tending to infinity with n we get that

$$\liminf_{n\to\infty}\mathbb{P}[B^{P_n}\cap A\in\mathcal{A}]\geq\lim_{n\to\infty}\mathbb{P}[B^{P_{/C-D\cap F_n}}\cap A\in\mathcal{A}]=\mathbb{P}[B^{P_{/C-D}}\cap A\in\mathcal{A}].$$

A similar argument gives that

$$\limsup_{n\to\infty}\mathbb{P}[B^{P_n}\cap A\in\mathcal{A}]\leq\mathbb{P}[B^{P_{-D/C}}\cap A\in\mathcal{A}]$$

Therefore,

$$\begin{aligned}\mathbb{P}[B^{P_{-D/C}}\cap A\in\mathcal{A}]&\geq\limsup_{n\to\infty}\mathbb{P}[B^{P_n}\cap A\in\mathcal{A}]\\&\geq\liminf_{n\to\infty}\mathbb{P}[B^{P_n}\cap A\in\mathcal{A}]\geq\mathbb{P}[B^{P_{/C-D}}\cap A\in\mathcal{A}].\end{aligned}\tag{3.2}$$

These inequalities are in fact true without the assumption $A\cap F=\emptyset$. Indeed, let $A\subset E$ finite and $\mathcal{A}$ be an upwardly closed subset of 2^A. We define $A'=A\backslash F$ and

$$\mathcal{A}'=\{X\subset A'|X\cup(A\cap C)\in\mathcal{A}\}.$$

Note that $\mathcal{A}'$ is upwardly closed subset of $2^{A'}$.

Then $\mathbb{P}[B^{P_{/C-D}}\cap A\in\mathcal{A}]=\mathbb{P}[B^{P_{/C-D}}\cap A'\in\mathcal{A}']$. Moreover, for any large enough n, we have $\mathbb{P}[B^{P_n}\cap A\in\mathcal{A}]=\mathbb{P}[B^{P_n}\cap A'\in\mathcal{A}']$. Clearly $A'\cap F=\emptyset$, so we reduced the problem to the already established case.

Choosing $A=\{e\}$ and $\mathcal{A}=\{\{e\}\}$ in (3.2), we get that $\langle P_{/C-D}e,e\rangle\leq\langle P_{-D/C}e,e\rangle$ for all $e\in E$. Inequality (3.2) tells us that $B^{P_{-D/C}}$ stochastically dominates $B^{P_{/C-D}}$. But if $\langle P_{/C-D}e,e\rangle=\langle P_{-D/C}e,e\rangle$ for all $e\in E$, then the distribution of $B^{P_{/C-D}}$ and $B^{P_{-D/C}}$ must be the same. Then inequality (3.2) gives the statement. □

Let A be any finite set. We define the martingale X_n by

$$X_n=\mathbb{P}[A\subset B^P|B^P\restriction F_n]=\mathbb{P}[A\subset B^{P_{/B^P\cap F_n-F_n\backslash B^P}}].$$

Combining the previous lemma with our assumptions on B^P we get that with probability 1 we have $\lim X_n=\mathbb{P}[A\subset B^{P_{/B^P\cap F-F\backslash B^P}}]$. On the other hand we have

$$\lim X_n=\mathbb{P}[A\subset B^P|B^P\restriction F].$$

CEU eTD Collection

The statement follows.

□

Lemma 3.15. *Let (G, o, P, F) be a unimodular random decorated RGPC where P is an orthogonal projection with probability* 1. *Then with probability* 1*, we have that for any finite set $A \subset V(G) \times K$*

$$\mathbb{P}(A \subset B^P | B^P \restriction F) = \mathbb{P}(A \subset B^{P_{/B^P \cap F - F \setminus B^P}}).$$

Proof. From Lemma 3.14, we have that for all $e \in V(G) \times K$ we have

$$\langle P_{/B^P \cap F - F \setminus B^P} e, e \rangle \leq \langle P_{-F \setminus B^P / B^P \cap F} e, e \rangle.$$

From Lemma 3.11, we have $\mathrm{Tr}(G, o, P_{/B^P \cap F - F \setminus B^P}) = \mathrm{Tr}(G, o, P_{-F \setminus B^P / B^P \cap F})$, which imply that with probability 1 we have $\langle P_{/B^P \cap F - F \setminus B^P} e, e \rangle = \langle P_{-F \setminus B^P / B^P \cap F} e, e \rangle$ for any $e \in \{o\} \times K$, but then it is true for any e from unimodularity. (See [4, Lemma 2.3 (Everything Shows at the Root)].) Therefore, Lemma 3.13 can be applied to get the statement.

□

The lemma above establishes Conjecture 9.1 of [42] in the special unimodular case. Note that this conjecture is false in general as it was pointed out to the author by Russel Lyons. Indeed, it follows from the results of Heicklen and Lyons [31] that for the WUSF on certain trees, conditioning on all edges but one does not (a.s.) give a measure corresponding to an orthogonal projection, because the probability of the remaining edge to be present is in $(0, 1)$ a.s.

3.3 Limit of conditional determinantal processes

Theorem 3.16. *Let $(G_n, o_n, P_n, C_n, D_n)$ be a convergent sequence of unimodular random decorated RGPCs with limit (G, o, P, C, D). Assume that P_n and P are orthogonal projections and (C_n, D_n) and (C, D) are all permitted with probability* 1. *Then $(G_n, o_n, (P_n)_{/C_n - D_n})$ converges to $(G, o, P_{/C-D})$.*

This will follow from applying the next lemma twice, first for the sequence P_n, then for $I - (P_n)_{/C}$ with D_n in place of C_n. At the second time we need to use Proposition 3.10 to show that the conditions of the lemma are satisfied.

Lemma 3.17. *Let $(G_n, o_n, P_n, C_n, D_n)$ be a convergent sequence of unimodular random decorated RGPCs with limit (G, o, P, C, D). Assume that P_n and P are orthogonal projections and C_n, C are all independent with probability* 1. *Then $(G_n, o_n, (P_n)_{/C_n}, D_n)$ converges $(G, o, P_{/C}, D)$.*

Proof. The presence of D_n does not not add any extra difficulty to the problem, so for simplicity of notation we will prove the following statement instead:

CEU eTD Collection

Let (G_n, o_n, P_n, C_n) be a convergent sequence of unimodular random decorated RGPCs with limit (G, o, P, C). Assume that P_n and P are orthogonal projections, C_n and C are all independent with probability 1*. Then $(G_n, o_n, (P_n)_{/C_n})$ converges to $(G, o, P_{/C})$.*

We start by the following lemma.

Lemma 3.18. *Let (G_n, o_n, P_n, C_n) be a convergent sequence of decorated RGPCs with limit (G, o, P, C). Assume that P_n and P are orthogonal projections, C_n and C are all independent, and there is an r such that $C_n \subset V(B_r(G_n, o_n)) \times K$ and $C \subset V(B_r(G, o)) \times K$. Then $(G_n, o_n, (P_n)_{\times C_n})$ converges to $(G, o, P_{\times C})$.*

Proof. Let us choose an orthogonal projection Π from a small neighborhood U of P. If this neighborhood is small enough, then C is independent with respect to Π. For $c \in C$, we have $\Pi_{\times\{c\}} e = \Pi e - \frac{\langle \Pi e, c\rangle}{\langle \Pi c, c\rangle} \Pi c$. Indeed, clearly $\Pi e - \frac{\langle \Pi e, c\rangle}{\langle \Pi c, c\rangle} \Pi c \in \operatorname{Im}\Pi \cap [\{c\}]^\perp$, moreover with the notation $\alpha = \frac{\langle \Pi e, c\rangle}{\langle \Pi c, c\rangle}$ for any $w \in \operatorname{Im}\Pi \cap [\{c\}]^\perp$ we have

$$\langle w, e - (\Pi e - \alpha \Pi c)\rangle = \langle w, (I - \Pi)e\rangle + \langle w, \alpha \Pi c\rangle = \langle \Pi w, \alpha c\rangle = \langle w, \alpha c\rangle = 0.$$

By induction we get that

$$\Pi_{\times C} e = \Pi e - \sum_{c \in C} \alpha_{c,e} \Pi c.$$

Here $\alpha_{c,e}$ is a continuous function of $(\langle \Pi x, y\rangle)_{x,y \in C \cup \{e\}}$ in the neighborhood U. The statement can be deduced using this. □

From compactness every subsequence of $(G_n, o_n, P_n, (P_n)_{/C_n}, C_n)$ has a convergent subsequence, so it is enough to prove the following lemma.

Lemma 3.19. *Let (G_n, o_n, P_n, C_n) be a convergent sequence of unimodular random decorated RGPCs with limit (G, o, P, C). Assume that P_n and P are orthogonal projections, C_n and C are all independent with probability* 1*. If $(G_n, o_n, P_n, (P_n)_{/C_n}, C_n)$ converges to (G, o, P, Q, C), then (G, o, Q) has the same distribution as $(G, o, P_{/C})$.*

Proof. Using Skorokhod's representation theorem we can find a coupling of $(G_n, o_n, P_n, (P_n)_{/C_n}, C_n)$ and (G, o, P, Q, C) such that $\lim_{n\to\infty}(G_n, o_n, P_n, (P_n)_{/C_n}, C_n) = (G, o, P, Q, C)$ with probability 1. By definition there is a random sequence $r_1, r_2, \dots$ such that $\lim_{n\to\infty} r_n = \infty$ with probability 1, and there is a root preserving graph isomorphism ψ_n from $B_{r_n}(G, o)$ to $B_{r_n}(G_n, o_n)$ such that $\bar\psi_n(C \cap (B_{r_n}(G, o) \times K)) = C_n \cap (B_{r_n}(G_n, o_n) \times K)$, where $\bar\psi_n(v, k) = (\psi_n(v), k)$ and with probability 1 for each $e, f \in V(G) \times K$ we have

$$\lim_{n\to\infty} \langle P_n \bar\psi_n e, \bar\psi_n f\rangle = \langle Pe, f\rangle,$$

and

$$\lim_{n\to\infty} \langle (P_n)_{/C_n} \bar\psi_n e, \bar\psi_n f\rangle = \langle Qe, f\rangle.$$

Of course, $\bar\psi_n e$ only makes sense if n is large enough.

CEU eTD Collection

Let us define $C_n(r) = C_n \cap (B_r(G_n, o_n) \times K)$ and $C(r) = C \cap (B_r(G, o) \times K)$.

Lemma 3.18 gives us that for any r we have

$$\lim_{n\to\infty} \langle (P_n)_{\times C_n(r)} \bar{\psi}_n(e), \bar{\psi}_n(f) \rangle = \langle P_{\times C(r)} e, f \rangle. \tag{3.3}$$

Note that $\operatorname{Im} P_{\times C(r)}$ is a decreasing sequence of subspaces with intersection $\operatorname{Im} P_{\times C}$. So $P_{\times C(r)}$ converges to $P_{\times C}$ in the strong operator topology.

In particular, for any $e, f \in V(G) \times K$, we have

$$\lim_{r\to\infty} \langle P_{\times C(r)} e, f \rangle = \langle P_{\times C} e, f \rangle, \tag{3.4}$$

and

$$\lim_{r\to\infty} \langle (P_n)_{\times C_n(r)} \bar{\psi}_n(e), \bar{\psi}_n(f) \rangle = \langle (P_n)_{\times C_n} \bar{\psi}_n(e), \bar{\psi}_n(f) \rangle. \tag{3.5}$$

We need the following elementary fact.

Lemma 3.20. *Let $a(r, n)$ be non-negative real numbers, such that for any fixed n, the sequence $a(r, n)$ is monotone decreasing in r. Let $A_n = \lim_{r\to\infty} a(r, n)$, assume that for any fixed r the limit $B_r = \lim_{n\to\infty} a(r, n)$ exists. Then $\lim_{n\to\infty} A_n \le \lim_{r\to\infty} B_r$ if these limits exist.*

Note that if $e = f$ then the limits in (3.4) and (3.5) are decreasing limits as we observed in Proposition 3.4. So the previous lemma combined with equation (3.3) gives us that for any $e \in V(G) \times K$ we have

$$\lim_{n\to\infty} \langle (P_n)_{\times C_n} \bar{\psi}_n e, \bar{\psi}_n e \rangle \le \langle P_{\times C} e, e \rangle.$$

Combining this with Proposition 3.4, we get that

$$\langle Qe, e \rangle = \lim_{n\to\infty} \langle (P_n)_{/C_n} \bar{\psi}_n e, \bar{\psi}_n e \rangle \le \langle P_{/C} e, e \rangle. \tag{3.6}$$

On the other hand, from Lemma 3.12, we know that

$$\begin{aligned}
\mathbb{E} \sum_{k\in K} \langle Q(o,k), (o,k) \rangle &= \operatorname{Tr}(G, o, Q) = \lim_{n\to\infty} \operatorname{Tr}(G_n, o_n, (P_n)_{/C_n}) \\
&= \lim_{n\to\infty} \operatorname{Tr}(G_n, o_n, P_n) = \operatorname{Tr}(G, o, P) = \operatorname{Tr}(G, o, P_{/C}) \\
&= \mathbb{E} \sum_{k\in K} \langle P_{/C}(o,k), (o,k) \rangle.
\end{aligned}$$

From this and inequality (3.6) we get that $\langle Q(o,k), (o,k) \rangle = \langle P_{/C}(o,k), (o,k) \rangle$ for all $k \in K$ with probability 1, so from unimodularity ([4, Lemma 2.3 (Everything shows at the

CEU eTD Collection

root)]) it follows that

$$\langle Qe, e\rangle = \lim_{n\to\infty} \langle (P_n)_{/C_n}\bar{\psi}_n e, \bar{\psi}_n e\rangle = \langle P_{/C}e, e\rangle \tag{3.7}$$

for all $e \in V(G) \times K$ with probability 1.

Now we prove that with probability 1 for every $e, f \in V(G) \times K$ we have $\langle Qe, f\rangle = \langle P_{/C}e, f\rangle$. This is clear if $e \in C$, because in that case $P_{/C}e = Qe = e$. So assume that $e \notin C$, then

$$\begin{aligned}
|\langle P_{/C}e, f\rangle - \langle Qe, f\rangle| &= |\langle P_{\times C}e, f\rangle - \langle Qe, f\rangle| \\
&\le |\langle P_{\times C}e, f\rangle - \langle P_{\times C(r)}e, f\rangle| \\
&\quad + |\langle P_{\times C(r)}e, f\rangle - \langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n f\rangle| \\
&\quad + |\langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n f\rangle - \langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n f\rangle| \\
&\quad + |\langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n f\rangle - \langle Qe, f\rangle|.
\end{aligned}$$

Pick any $\varepsilon > 0$. If we choose a large enough r, then $|\langle P_{\times C}e, f\rangle - \langle P_{\times C(r)}e, f\rangle| < \varepsilon$ and $|\langle P_{\times C(r)}e, e\rangle - \langle P_{\times C}e, e\rangle| < \varepsilon$ from equation (3.4). Fix such an r. Then if n is large enough $|\langle P_{\times C(r)}e, f\rangle - \langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n f\rangle| < \varepsilon$ from equation (3.3), and also $|\langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n f\rangle - \langle Qe, f\rangle| < \varepsilon$, because of Proposition 3.4 and the fact that $e \notin C$. Finally, observing that $(P_n)_{\times C_n(r)} - (P_n)_{\times C_n}$ is an orthogonal projection, we have

$$\begin{aligned}
&|\langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n f\rangle - \langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n f\rangle| \\
&\qquad \le \|(P_n)_{\times C_n(r)}\bar{\psi}_n e - (P_n)_{\times C_n}\bar{\psi}_n e\|_2 \\
&\qquad = \sqrt{\langle (P_n)_{\times C_n(r)}\bar{\psi}_n e - (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n e\rangle} \\
&\qquad \le \Big(|\langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n e\rangle - \langle P_{\times C(r)}e, e\rangle| \\
&\qquad\qquad + |\langle P_{\times C(r)}e, e\rangle - \langle P_{\times C}e, e\rangle| \\
&\qquad\qquad + |\langle P_{\times C}e, e\rangle - \langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n e\rangle| \Big)^{\frac{1}{2}}
\end{aligned}$$

Now, for a large enough n we have $|\langle (P_n)_{\times C_n(r)}\bar{\psi}_n e, \bar{\psi}_n e\rangle - \langle P_{\times C(r)}e, e\rangle| < \varepsilon$ from equation (3.3) and $|\langle P_{\times C}e, e\rangle - \langle (P_n)_{\times C_n}\bar{\psi}_n e, \bar{\psi}_n e\rangle| = |\langle P_{/C}e, e\rangle - \langle (P_n)_{/C_n}\bar{\psi}_n e, \bar{\psi}_n e\rangle| < \varepsilon$ from line (3.7). Finally, $|\langle P_{\times C(r)}e, e\rangle - \langle P_{\times C}e, e\rangle| < \varepsilon$ follows from the choice of r. Putting everything together, $|\langle P_{/C}e, f\rangle - \langle Qe, f\rangle| < 3\varepsilon + \sqrt{3\varepsilon}$, so Lemma 3.19 follows. □

This completes the proof of Lemma 3.17 and Theorem 3.16. □

4 The proof of Theorem 2.4

First we observe that we may assume that $|V(G_n)| \to \infty$. If not, then we can take a large $m = m(n)$ and replace G_n with m disjoint copies of G_n, and P_n with the m fold direct sum of copies of P_n.

CEU eTD Collection

Let (G,P) be a finite graph-positive-contraction, where P is an orthogonal projection. Let $m = |V(G) \times L|$. Fix an ordering $e_1, e_2, \dots, e_m$ of the element of $V(G) \times L$. Let $E_i = \{e_1, e_2, \dots, e_i\}$. For $e \in V(G) \times L$ let $I(e)$ be the indicator of the event that $e \in B^P$. Let $g(x) = -x \log x - (1-x)\log(1-x)$. Using the chain rule for the conditional entropy and Lemma 3.6 we obtain that

$$\begin{aligned}
h_L(G,P) &= H(I(e_1), I(e_2), \dots, I(e_m)) \\
&= \sum_{i=0}^{m-1} H(I(e_{i+1})|I(e_1), I(e_2), \dots, I(e_i)) \\
&= \sum_{i=0}^{m-1} \sum_{C \subset E_i} \mathbb{P}[B^P \cap E_i = C] g(\mathbb{P}[e_{i+1} \in B^P | B^P \cap E_i = C]) \\
&= \sum_{i=0}^{m-1} \mathbb{E} g(\mathbb{P}[e_{i+1} \in B^{P_{/(E_i \cap B^P) - (E_i \backslash B^P)}}]) \\
&= \sum_{i=0}^{m-1} \mathbb{E} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e_{i+1}, e_{i+1} \rangle).
\end{aligned}$$

Here expectation is over the random choice of B^P.

Instead of a fixed ordering of $V(G) \times L$ we can choose a uniform random ordering. Taking expectation we get that

$$h_L(G,P) = \sum_{i=0}^{m-1} \mathbb{E} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e_{i+1}, e_{i+1} \rangle),$$

where expectation is over the random choice of $E_i = \{e_1, e_2, \dots, e_i\}$ and B^P. Note that $g(0) = g(1) = 0$, so

$$g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e, e \rangle) = 0$$

whenever $e \in E_i$. Also note that e_{i+1} is a uniform random element of $(V(G) \times L) \backslash E_i$. From these it follows that if e is a uniform random element of $V(G) \times L$ independent of E_i, then

$$\frac{m}{m-i} \mathbb{E} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e, e \rangle) \quad = \quad \mathbb{E} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e_{i+1}, e_{i+1} \rangle) \quad \leq \quad \log 2. \qquad (4.1)$$

Thus,

$$h_L(G,P) = \sum_{i=0}^{m-1} \frac{m}{m-i} \mathbb{E} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} e, e \rangle).$$

Let $(G,o,P) = U(G,P)$. Then

$$h_L(G,P) = \sum_{i=0}^{m-1} \frac{m}{m-i} \frac{1}{|L|} \mathbb{E} \sum_{\ell \in L} g(\langle P_{/(E_i \cap B^P) - (E_i \backslash B^P)} (o,\ell), (o,\ell) \rangle).$$

CEU eTD Collection

So

$$\frac{h_L(G,P)}{|V(G)|} = \sum_{i=0}^{m-1} \frac{1}{m-i}\mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_i\cap B^P)-(E_i\setminus B^P)}(o,\ell),(o,\ell)\rangle).$$

For $t\in[0,1)$ we define

$$H_t(G,P) = \mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_i\cap B^P)-(E_i\setminus B^P)}(o,\ell),(o,\ell)\rangle),$$

where $i=\lfloor tm\rfloor$, and E_i is a uniform random i element subset of $V(G)\times L$ independent of B^P and o. For $i=0,1,\dots,m-1$, we have

$$\frac{1}{m-i}\mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_i\cap B^P)-(E_i\setminus B^P)}(o,\ell),(o,\ell)\rangle) = \int_{i/m}^{(i+1)/m} \frac{m}{m-\lfloor tm\rfloor} H_t(G,P)dt.$$

Therefore

$$\frac{h_L(G,P)}{|V(G)|} = \int_0^1 \frac{m}{m-\lfloor tm\rfloor} H_t(G,P)dt. \tag{4.2}$$

Let $m_n = |V(G_n)\times L|$. Recall that we observed at the beginning of the proof that we may assume that $|V(G_n)|\to\infty$. So we assume this.

Lemma 4.1. *Let (G_n,P_n) be the sequence given in the statement of the theorem. For any $t\in[0,1)$ we have*

$$\lim_{n\to\infty} H_t(G_n,P_n) = \mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_t\cap B^P)-(E_t\setminus B^P)}(o,\ell),(o,\ell)\rangle),$$

where E_t is a Bernoulli(t) percolation of the set $V(G)\times L$ independent of B^P. Consequently,

$$\lim_{n\to\infty} \frac{m_n}{m_n-\lfloor tm_n\rfloor} H_t(G_n,P_n) = \frac{1}{1-t}\mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_t\cap B^P)-(E_t\setminus B^P)}(o,\ell),(o,\ell)\rangle).$$

Proof. From Proposition 2.1 we have $(G_n,o_n,P_n,B^{P_n})\to(G,o,P,B^P)$. It is straightforward to show that $(G_n,o_n,P_n,E_{\lfloor tm_n\rfloor})\to(G,o,P,E_t)$, here $m_n=|V(G)\times L|$ and $E_{\lfloor tm_n\rfloor}$ is a uniform $\lfloor tm_n\rfloor$ element subset of $V(G)\times L$ independent of B^{P_n}. Then it follows that $(G_n,o_n,P_n,E_{\lfloor tm_n\rfloor},B^{P_n})\to(G,o,P,E_t,B^P)$. But then with the notations $C_n=E_{\lfloor tm_n\rfloor}\cap B^{P_n}$, $C=E_t\cap B^P$, $D_n=E_{\lfloor tm_n\rfloor}\setminus B^{P_n}$ and $D=E_t\setminus B^P$ we have $(G_n,o_n,P_n,C_n,D_n)\to(G,o,P,C,D)$. It follows from Theorem 3.8 and Proposition 3.9, that (C_n,D_n) and (C,D) are all permitted with probability 1. It is also clear that (G_n,o_n,P_n,C_n,D_n) are unimodular. Thus applying Theorem 3.16 we get that $(G_n,o_n,(P_n)_{/C_n-D_n})$ converge to $(G,o,P_{/C-D})$. We define the continuous map $f:\mathcal{RGPC}\to\mathbb{R}$ as $f(G,o,P)=\sum_{\ell\in L} g(\langle P(o,\ell),(o,\ell)\rangle)$. Then from the definition of weak* convergence we get that

$$\lim_{n\to\infty}\mathbb{E}f(G_n,o_n,(P_n)_{/C_n-D_n}) = \mathbb{E}f(G,o,P_{/C-D})$$

and this is exactly what we needed to prove. ☐

CEU eTD Collection

From (4.1) we have $\frac{m_n}{m_n-\lfloor m_n \rfloor} H_t(G,P) \le \log 2$ for any n and t. So combining equation (4.2) and Lemma 4.1 with the dominated convergence theorem we get that

$$\begin{aligned}
\lim_{n\to\infty} \frac{h_L(G_n,P_n)}{|V(G_n)|} &= \lim_{n\to\infty} \int_0^1 \frac{m_n}{m_n-\lfloor tm_n\rfloor} H_t(G_n,P_n)dt \qquad (4.3)\\
&= \int_0^1 \lim_{n\to\infty} \frac{m_n}{m_n-\lfloor tm_n\rfloor} H_t(G_n,P_n)dt\\
&= \int_0^1 \frac{1}{1-t}\mathbb{E}\sum_{\ell\in L} g(\langle P_{/(E_t\cap B^P)-(E_t\backslash B^P)}(o,\ell),(o,\ell)\rangle)dt\\
&= \int_0^1 \frac{1}{1-t}\sum_{\ell\in L} \mathbb{P}[(o,\ell)\notin E_t]\mathbb{E}\left[g(\langle P_{/(E_t\cap B^P)-(E_t\backslash B^P)}(o,\ell),(o,\ell)\rangle)\middle|(o,\ell)\notin E_t\right] dt\\
&= \int_0^1 \sum_{\ell\in L} \mathbb{E}\left[g(\langle P_{/(E_t\cap B^P)-(E_t\backslash B^P)}(o,\ell),(o,\ell)\rangle)\middle|(o,\ell)\notin E_t\right] dt.
\end{aligned}$$

Here we used the law of total expectation and the fact that $g(\langle B^{P_{/(E_t\cap B^P)-(E_t\backslash B^P)}}(o,\ell),(o,\ell)\rangle) = 0$ whenever $(o,\ell)\in E_t$. Let c be an i.i.d. uniform $[0,1]$ labeling of $V(G)\times L$. Observe that conditioned on the event $(o,\ell)\notin E_t$ the distribution of E_t is the same as the distribution of $\{e\in V(G)\times L | c(e) < c(o,\ell)\}$ conditioned on $c(o,\ell)=t$. Let $I(e)$ be the indicator of the event $e\in B^{\mathrm{rest}_L P}$. From Lemma 3.15 we get for $\ell\in L$

$$\begin{aligned}
&\int_0^1 \mathbb{E}\left[g(\langle P_{/(E_t\cap B^P)-(E_t\backslash B^P)}(o,\ell),(o,\ell)\rangle)\middle|(o,\ell)\notin E_t\right] dt\\
&\quad= \int_0^1 \mathbb{E}\left[g(\mathbb{E}(I(o,\ell)|\{I(f)|f\in E_t\}))\middle|(o,\ell)\notin E_t\right] dt\\
&\quad= \int_0^1 \mathbb{E}\left[g(\mathbb{E}(I(o,\ell)|\{I(f)|c(f)<c(o,\ell)\}))\middle|c(o,\ell)=t\right] dt\\
&\quad= \mathbb{E}\left[g(\mathbb{E}(I(o,\ell)|\{I(f)|c(f)<c(o,\ell)\}))\right] = \mathbb{E}\bar{h}((o,\ell),\mathrm{rest}_L P).
\end{aligned}$$

Combining this with equation (4.3) we get Theorem 2.4.

5 Extension of Theorem 2.4 to positive contractions

To state the extension of Theorem 2.4 we need another tightness notion. Let $K_0 \supset K$ be finite. A random RGPC (G_0,o_0,T_0) with support set K_0 is called an K_0-*extension* of the random RGPC (G,o,T) with support set K, if $(G_0,o_0,\mathrm{rest}_K(T_0))$ has the same distribution as (G,o,T). We say that the extension is *tight* if T_0 is an orthogonal projection with probability 1. A finite graph-positive-contraction (G_0,T_0) with support set K_0 is called an K_0-*extension* of the finite graph-positive-contraction (G,T) with support set K, if $G=G_0$ and $\mathrm{rest}_K T_0 = T$. We say that the extension is *tight*, if T_0 is an orthogonal projection.

Given a sequence of finite graph-positive-contractions (G_n,T_n) with support K and a random RGPC (G,o,T) with support set K, we say that $\lim U(G_n,T_n) = (G,o,T)$ *p-tightly*, if there is a

CEU eTD Collection

finite $K_0 \supset K$ and there are tight K_0-extensions (G_n, P_n) of (G_n, T_n) and a tight K_0-extension (G, o, P) of (G, o, T) such that $\lim U(G_n, P_n) = (G, o, P)$.

With these definitions we have the following extension of Theorem 2.4.

Theorem 5.1. *Let (G_n, T_n) be a sequence of finite graph-positive-contractions such that $\lim U(G_n, T_n) = (G, o, T)$ p-tightly for some random RGPC (G, o, T). Then*

$$\lim_{n\to\infty} \frac{h_L(G_n, T_n)}{|V(G_n)|} = \bar{h}_L(G, o, T).$$

Proof. By the definition of tight convergence, there is a finite $K_0 \supset K$ and there are tight K_0-extensions (G_n, P_n) of (G_n, T_n) and a tight K_0-extension (G, o, P) of (G, o, T) such that $\lim U(G_n, P_n) = (G, o, P)$. Note that the distribution of B^{T_n} is the same as $B^{P_n} \cap (V(G) \times K)$. So $h_L(G_n, T_n) = h_L(G_n, P_n)$. Similarly, $\bar{h}_L(G, o, T) = \bar{h}_L(G, o, P)$. So from Theorem 2.4

$$\lim_{n\to\infty} \frac{h_L(G_n, T_n)}{|V(G_n)|} = \lim_{n\to\infty} \frac{h_L(G_n, P_n)}{|V(G_n)|} = \bar{h}_L(G, o, P) = \bar{h}_L(G, o, T).$$

□

We do not know whether the condition of p-tightness can be replaced with tightness in the theorem above.

Later we will need the following proposition.

Proposition 5.2. *Let $K \subset K_0$, such that $|K_0| = 2|K|$. Any finite graph-positive-contraction (G, T) has a tight K_0-extension (G, P).*

Proof. This is well known, see for example [42, Chapter 9]. We include the proof for the reader's convenience. Let $q(x) = \sqrt{x(1-x)}$ on the interval $[0, 1]$ and 0 otherwise. Using functional calculus we can define $q(T)$, for every positive contraction. Then the block matrix

$$P = \begin{pmatrix} T & q(T) \\ q(T) & I - T \end{pmatrix}$$

gives the desired operator. □

The K_0-extension given in the previous lemma will be called the *standard K_0-extension* of (G, T). The standard K_0-extension of a random RGPC is defined in the analogous way.

CEU eTD Collection

6 Sofic entropy: The proof of Theorem 2.6

Note that for any graph G the set of random $\{0,1\}^K$ colorings of $V(G)$ can be identified with the set of random subsets of $V(G)\times K$. In this proof we use the random subset terminology.

As we mentioned in Subsection 2.7, the inequality $h'(B^T)\le \bar{h}(G_\Gamma, e_\Gamma, T)$ is well known, but we give the proof for completeness.

Let G be a graph, and F be a random subset of $V(G)\times K$. Let c be a $[0,1]$ labeling of $V(G)\times K$. For $e\in V(G)\times K$ let $I(e)$ be the indicator of the event that $e\in F$. For $(v,k)\in V(G)\times K$ we define

$$\bar{h}((v,k),c,F) = H(I(v,k)|\{I(v',k')|c(v',k')<c(v,k)\}).$$

We also define

$$\bar{h}((v,k),F) = \mathbb{E}\bar{h}((v,k),c,F),$$

where c is an i.i.d. uniform $[0,1]$ labeling of $V(G)\times K$.

Moreover, if r is an integer, then we define

$$\bar{h}_r((v,k),c,F) = H(I(v,k)|\{I(v',k')|c(v',k')<c(v,k) \text{ and } (v',k')\in B_r(G,v)\times K\})$$

and

$$\bar{h}_r((v,k),F) = \mathbb{E}\bar{h}_r((v,k),c,F),$$

where c is an i.i.d. uniform $[0,1]$ labeling of $V(G)\times K$.

Comparing these definitions with the definitions given in Subsection 2.7, we see that if $F=B^T$ for some positive contraction T, then $\bar{h}((v,k),F)=\bar{h}((v,k),T)$. Thus, it is justified the use the same symbol in both cases.

If c is a $[0,1]$-labeling such that the labels are pairwise distinct and G is finite, the chain rule of conditional entropy gives us

$$H(F) = \sum_{(v,k)\in V(G)\times K} \bar{h}((v,k),c,F).$$

Taking expectation over c we get that

$$H(F) = \sum_{(v,k)\in V(G)\times K} \bar{h}((v,k),F).$$

Or, alternatively,

$$\frac{H(F)}{|V(G)|} = \mathbb{E}\sum_{k\in K}\bar{h}((o,k),F)$$

where o is a uniform random vertex of $V(G)$.

CEU eTD Collection

Combining this with the well known monotonicity properties of conditional entropies, for any integer r, we have

$$\frac{H(F)}{|V(G)|} = \mathbb{E}\sum_{k\in K}\bar{h}((o,k),F) \le \mathbb{E}\sum_{k\in K}\bar{h}_r((o,k),F).$$

Note that $\bar{h}_r((o,k),F)$ only depends on the distribution of $F\cap(B_r(G,o)\times K)$. Therefore, if F is an (ε,r) approximation, then we have

$$\frac{H(F)}{|V(G)|} \le \mathbb{E}\sum_{k\in K}\bar{h}_r((o,k),F) \le \sum_{k\in K}\bar{h}_r((e_\Gamma,k),B^T)+\eta_r(\varepsilon),$$

where $\eta_r(\varepsilon)$ does not depend on G, and $\eta_r(\varepsilon)\to 0$ as $\varepsilon\to 0$. In particular,

$$H(\varepsilon,r) \le \sum_{k\in K}\bar{h}_r((e_\Gamma,k),B^T)+\eta_r(\varepsilon)$$

tending to 0 with ε we obtain that

$$\inf_{\varepsilon} H(\varepsilon,r) \le \sum_{k\in K}\bar{h}_r((e_\Gamma,k),B^T).$$

But we have

$$\lim_{r\to\infty}\sum_{k\in K}\bar{h}_r((e_\Gamma,k),B^T) = \sum_{k\in K}\bar{h}((e_\Gamma,k),B^T).$$

Thus tending to infinity with r we get

$$h'(B^T) \le \sum_{k\in K}\bar{h}((e_\Gamma,k),B^T) = \bar{h}(G_\Gamma,e_\Gamma,T).$$

Now let $G_1,G_2,\dots$ be a sequence of finite S-labeled Schreier graphs Benjamini-Schramm converging to (G_Γ,e_Γ). Let $K\subset K_0$, such that $|K_0|=2|K|$. Let P be the standard K_0-extension of T. Then it is clear that P is an invariant operator on $\ell^2(V(G_\Gamma)\times K_0)$.

Lemma 6.1. *There is a sequence of positive contractions R_n on $\ell^2(V(G_n)\times K_0)$ such that $\lim_{n\to\infty}U(G_n,R_n)=(G_\Gamma,e_\Gamma,P)$. Moreover, the spectral measures $\mu_n=\mu_{U(G_n,R_n)}$ weakly converge to $\mu=\mu_{(G_\Gamma,e_\Gamma,P)}=|K|(\delta_0+\delta_1)$.*

Proof. One can easily define a metric d' on $\mathcal{P}(\mathcal{RGPC})$ such that for any sequence of positive contractions R_n on $\ell^2(V(G_n)\times K_0)$, we have that $\lim_{n\to\infty}d'(U(G_n,R_n),(G_\Gamma,e_\Gamma,P))=0$ if and only if $\lim_{n\to\infty}U(G_n,R_n)=(G_\Gamma,e_\Gamma,P)$ and μ_n weakly converge to μ.

Thus if the required sequence does not exist, then there is an $\varepsilon>0$ and an infinite sequence $n_1<n_2<\dots$ such that $d'(U(G_{n_i},R_{n_i}),(G_\Gamma,e_\Gamma,P))\ge\varepsilon$ for any i and any positive contractions R_{n_i} on $\ell^2(V(G_{n_i})\times K_0)$.

We will now use the results of Lyons and Thom [43]. In their paper they are using ultralimits. However, by passing to a subsequence we may replace ultralimits by actual limits.

CEU eTD Collection

Thus [43, Proposition 4.4, Lemma 4.7 and Remark 4.3] provide us a subsequence (m_i) of (n_i) and positive contractions R_{m_i} on $\ell^2(V(G_{m_i}) \times K_0)$, such that $\lim_{i\to\infty} U(G_{m_i}, R_{m_i}) = (G_\Gamma, e_\Gamma, P)$ and μ_{m_i} weakly converge to μ. Indeed, [43, Proposition 4.4] gives us the convergence $\lim_{i\to\infty} U(G_{m_i}, R_{m_i}) = (G_\Gamma, e_\Gamma, P)$ and [43, Proposition 4.7] is used to make sure R_{m_i} is indeed a positive contraction. Finally, the convergence of spectral measures follows from [43, Remark 4.3].

Then $\lim_{i\to\infty} d'(U(G_{m_i}, R_{m_i}), (G_\Gamma, e_\Gamma, P)) = 0$, which contradicts to the choice of the subsequence (n_i).

Finally, observe that

$$\mathrm{Tr}(G_\Gamma, e_\Gamma, P) = \mathrm{Tr}(G_\Gamma, e_\Gamma, T) + \mathrm{Tr}(G_\Gamma, e_\Gamma, I - T) = |K|,$$

so the spectral measure μ is indeed equal to $|K|(\delta_0 + \delta_1)$. $\square$

Note that R_n is not necessary an orthogonal projection. Now we modify R_n slightly to get an orthogonal projection. Let us define

$$w(x) = \begin{cases} x & \text{for } 0 \le x < \frac{1}{2}, \\ x - 1 & \text{for } \frac{1}{2} \le x \le 1 \end{cases}$$

Note that w is not continuous, but w^2 is continuous. Let $(v_i)_{i=1}^{|V(G_n)\times K_0|}$ be an orthonormal basis of $\ell^2(V(G_n) \times K_0)$ consisting of eigenvectors of R_n, such that $R_n v_i = \lambda_i v_i$. Let $w(R_n)$ be the unique operator, such that $w(R_n)v_i = w(\lambda_i)v_i$ for $i = 1, 2, \ldots, |V(G_n) \times K_0|$.

Then $P_n = R_n - w(R_n)$ will be the orthogonal projection to the span of $\{v_i | \lambda_i \ge \frac{1}{2}\}$. Moreover,

$$\begin{aligned} \lim_{n\to\infty} \mathbb{E} \sum_{k\in K_0} \|w(R_n)(o,k)\|_2^2 &= \lim_{n\to\infty} \mathbb{E} \sum_{k\in K_0} \langle w(R_n)^2(o,k), (o,k)\rangle \\ &= \lim_{n\to\infty} \int_0^1 w^2 d\mu_n = \int_0^1 w^2 d\mu \\ &= |K|(w^2(0) + w^2(1)) = 0 \end{aligned} \tag{6.1}$$

Here the expectation is over a uniform random vertex o of $V(G_n)$. This easily implies that $U(G_n, R_n)$ and $U(G_n, P_n)$ have the same limit, that is, $\lim U(G_n, P_n) = (G_\Gamma, e_\Gamma, P)$. (Note that in the language of [43] the vanishing limit in (6.1) means that (R_n) and (P_n) represent the same operator.) Now using Theorem 2.4 we get that

$$\begin{aligned} \lim_{n\to\infty} \frac{H(B^{\mathrm{rest}_K(P_n)})}{|V(G_n)|} &= \lim_{n\to\infty} h_K(G_n, P_n) \\ &= \bar{h}(G_\Gamma, e_\Gamma, \mathrm{rest}_K(P)) = \bar{h}(G_\Gamma, e_\Gamma, T). \end{aligned}$$

CEU eTD Collection

Now for any ε and r for large enough n we have that $B^{\mathrm{rest}_K(P_n)}$ is an (ε, r)-approximation of B^T, because $\lim_{n\to\infty} U(G_n, \mathrm{rest}(P_n)) = (G_\Gamma, e_\Gamma, T)$. So $\bar{h}(G_\Gamma, e_\Gamma, T) \leq h(B^T)$ follows.

Putting everything together we get that $\bar{h}(G_\Gamma, e_\Gamma, T) \leq h(B^T) \leq h'(B^T) \leq \bar{h}(G_\Gamma, e_\Gamma, T)$. So Theorem 2.6 follows.

7 Tree entropy

Let $G = (V, E)$ be a locally finite connected graph. Choose an orientation of each edge to obtain the oriented graph $\vec{G}$. The *vertex-edge incidence matrix* $A = (a_{ve})$ of $\vec{G}$ is a $V \times E$ matrix such that

$$a_{ve} = \begin{cases} 1 & \text{if } e \text{ enters } v, \\ -1 & \text{if } e \text{ leaves } v, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\bigstar = \bigstar(\vec{G})$ be the closed subspace of $\ell^2(E)$ generated by the rows of A, and let $P_\bigstar$ be the orthogonal projection from $\ell^2(E)$ to $\bigstar$. If G is finite, then the determinantal measure corresponding to $P_\bigstar$ is the uniform measure on the spanning trees of G [17]. Let $\tau(G)$ be the number of spanning trees of G, then $H(B^{P_\bigstar}) = \log \tau(G)$. If G is infinite, the corresponding determinantal measure is the so-called *wired uniform spanning forest*(WUSF) [52, 29, 9, 40]. Note that in both cases, the resulting measure does not depend on the chosen orientation of G.

Given a rooted graph (G, o) and a non-negative integer k, let $p_k(G, o)$ be the probability that a simple random walk starting at o is back at o after k steps.

The following theorem was proved by Lyons [41].

Theorem 7.1. *Let G_n be a sequence of finite connected graphs, such that $|V(G_n)| \to \infty$ and their Benjamini-Schramm limit is a random rooted graph (G, o). Then*

$$\lim_{n\to\infty} \frac{\log \tau(G_n)}{|V(G_n)|} = \mathbb{E}\left(\log \deg(o) - \sum_{k=1}^{\infty} \frac{1}{k} p_k(G, o)\right).$$

Using our results we can give another expression for the limiting quantity. Let G be a connected locally finite infinite graph, let $\mathfrak{F}$ be the WUSF of G. For $e \in E(G)$ let $I(e)$ be the indicator of the event that $e \in \mathfrak{F}$. Given a $[0,1]$ labeling c of $E(G)$ and an edge $e \in E(G)$ we define

$$\bar{h}(G, e, c) = H(I(e)|\{I(f)|c(f) < c(e)\}),$$

and

$$\bar{h}(G, e) = \mathbb{E}\bar{h}(G, e, c),$$

where the expectation is over the i.i.d. uniform random $[0,1]$ labeling of G. Now we state our version of the tree entropy theorem.

CEU eTD Collection

Theorem 7.2. *Let G_n be a sequence of finite connected graphs, such that $|V(G_n)| \to \infty$ and their Benjamini-Schramm limit is a random rooted graph (G, o). Then*

$$\lim_{n\to\infty} \frac{\log \tau(G_n)}{|V(G_n)|} = \frac{1}{2}\mathbb{E}\sum_{e\sim o} \bar{h}(G, e),$$

where the summation is over the edges e incident to the root o.

Proof. Let $(\vec{G}, o)$ be the random rooted oriented graph obtained from (G, o) by orienting each edge independently and uniformly to one of the two possible directions. Let $L(\vec{G})$ be the line graph of $\vec{G}$, that is the vertex set of $L(\vec{G})$ is $V(\vec{G})$ and two vertices of $L(G)$ are connected if the corresponding edges in $\vec{G}$ are adjacent. Let $(\vec{G}', o')$ be obtained from $(\vec{G}, o)$ by biasing by the degree of the root. Let e be a uniform random edge incident to o'. Then $(L(\vec{G}'), e, P_{\bigstar(\vec{G}')})$ will be a random RGPC, which we denote by (L, e, P). (Here the support set K of (L, e, P) is a one element set.) Now there is an orientation $\vec{G}_n$ of G_n such that the Benjamini-Schramm limit of $\vec{G}_n$ is $(\vec{G}, o)$. This can be proved by choosing random orientations, and using concentration results. We omit the details. Let (L_n, P_n) be the finite-graph-contraction $(L(\vec{G}_n), P_{\bigstar(\vec{G}_n)})$. We have the following lemma.

Lemma 7.3. *We have* $\lim_{n\to\infty} U(L_n, P_n) = (L, e, P)$.

Proof. This can be proved by slightly modifying the argument of the proof of [4, Proposition 7.1]. □

The proof can be finished using Theorem 2.4. □

Both Lyons's and our theorem can be extended to edge weighted graphs, but in this case they are about two different quantities. However, these two quantities are closely related as we explain now. Let G be a connected finite graph, and assume that each edge e has a positive weight $w(e)$. The weight of a spanning tree T is defined as $w(T) = \prod_{e\in T} w(T)$. Let

$$Z(G, w) = \sum_{T \text{ is a spanning tree}} w(T)$$

be the sum of the weights of the spanning trees of G. Let $\mathfrak{F}$ be a random spanning tree of G, such that for any spanning tree T we have $\mathbb{P}(\mathfrak{F} = T) = Z(G, w)^{-1} w(T)$. This is again a determinantal process, the only difference compared to the uniform case is that for each edge e we need to multiply the corresponding column of the vertex-edge incidence matrix by $\sqrt{w(e)}$. In fact, this is the way we define the weighted version of the WUSF for infinite graphs. The Shannon entropy $H(\mathfrak{F})$ of $\mathfrak{F}$ is related to $Z(G, w)$ by the identity

$$H(\mathfrak{F}) = \log Z(G, w) - \mathbb{E} \log w(\mathfrak{F}). \tag{7.1}$$

Let (G_n, w_n) be a Benjamini-Schramm convergent sequence of weighted connected graphs, such that $|V(G_n)| \to \infty$ and their Benjamini-Schramm limit is a random rooted weighted graph

CEU eTD Collection

(G,o,w). Assume that the weights are uniformly bounded away from zero and infinity, that is, there are $0 < C_1 < C_2 < \infty$ such that all the weight are from the interval $[C_1, C_2]$. Then the generalization of Lyons's theorem states that

$$\lim_{n\to\infty} \frac{\log Z(G_n, w_n)}{|V(G_n)|} = \mathbb{E}\left(\log \pi(o) - \sum_{k=1}^{\infty} \frac{1}{k} p_{k,w}(G,o)\right),$$

where $\pi(v)$ is total weight of the edges incident to v, and $p_{k,w}(G,o)$ is defined using the random walk with transition probabilities $p(x,y) = \pi(x)^{-1} w(xy)$ instead of the simple random walk. On the other hand our theorem states that

$$\lim_{n\to\infty} \frac{H(\mathfrak{F}_n)}{|V(G_n)|} = \frac{1}{2}\mathbb{E}\sum_{e\sim o} \bar{h}(G,e,w),$$

where $\bar{h}(G,e,w)$ is defined as above, but using the weighted version of the WUSF.

These two statements above together with equation (7.1) of course imply that $\lim_{n\to\infty} |V(G_n)|^{-1}\mathbb{E}\log w(\mathfrak{F}_n)$ exists. However, there is a more direct proof. It is based on the observation that

$$\begin{aligned}\frac{\mathbb{E}\log w(\mathfrak{F}_n)}{|V(G_n)|} &= \frac{1}{|V(G_n)|}\sum_{e\in E(G_n)} \mathbb{P}(e\in\mathfrak{F}_n)\log w(e)\\ &= \frac{1}{2}\mathbb{E}\sum_{e\sim o}\mathbb{P}(e\in\mathfrak{F}_n)\log w(e),\end{aligned}$$

where the last expectation is over a uniform random $o \in V(G_n)$. Since we know that the limit of $\mathfrak{F}_n$ is $\mathfrak{F}$, where $\mathfrak{F}$ is the WUSF of the random rooted weighted graph (G,o,w) (see [4, Proposition 7.1]) we get that

$$\lim_{n\to\infty} \frac{\mathbb{E}\log w(\mathfrak{F}_n)}{|V(G_n)|} = \frac{1}{2}\mathbb{E}\sum_{e\sim o}\mathbb{P}(e\in\mathfrak{F})\log w(e).$$

Using equation (7.1), this provides us another formula for the limit $\lim_{n\to\infty} |V(G_n)|^{-1}\log Z(G_n, w_n)$. Namely,

$$\lim_{n\to\infty} \frac{\log Z(G_n, w_n)}{|V(G_n)|} = \frac{1}{2}\mathbb{E}\sum_{e\sim o}\left(\mathbb{P}(e\in\mathfrak{F})\log w(e) + \bar{h}(G,e,w)\right).$$

Question 7.4. *We have seen that if (G,o) is an infinite random rooted graph which is the limit of finite connected graphs, then*

$$\mathbb{E}\left(\log \deg(o) - \sum_{k=1}^{\infty}\frac{1}{k}p_k(G,o)\right) = \frac{1}{2}\mathbb{E}\sum_{e\sim o}\bar{h}(G,e).$$

Is this true for any infinite unimodular random rooted graph?

CEU eTD Collection

8 Matchings on trees

Given a finite graph G, let $\mathrm{mm}(G)$ be the number of maximum size matchings of G. In this section, we explain how to use Theorem 2.4 to prove the following theorem.

Theorem 8.1. *Let $G_1, G_2, \ldots$ be a Benjamini-Schramm convergent sequence of finite trees with maximum degree at most D. Then*

$$\lim_{n\to\infty} \frac{\log \mathrm{mm}(G_n)}{|V(G_n)|}$$

exists.

Note that without the assumption that the graphs G_i are trees, the limit above might not exist, even if the sequence converges to an amenable graph like $\mathbb{Z}^2$. Indeed, Figure 3.1 shows a graph which is locally close to $\mathbb{Z}^2$ and it has a unique perfect matching. On the other hand one can see that a $2n \times 2n$ box in $\mathbb{Z}^2$ has exponentially many perfect matchings. More results on the number of perfect matchings in subgraphs of $\mathbb{Z}^2$ can be found in [37, 56, 23]. See also [2], for an example of a Benjamini-Schramm convergent sequence of bipartite d-regular graphs such that the limit above does not exist. However, if we restrict our attention to vertex transitive bipartite graphs, the limit above exists for convergent graph sequences, as it was proved by Csikvári [22].

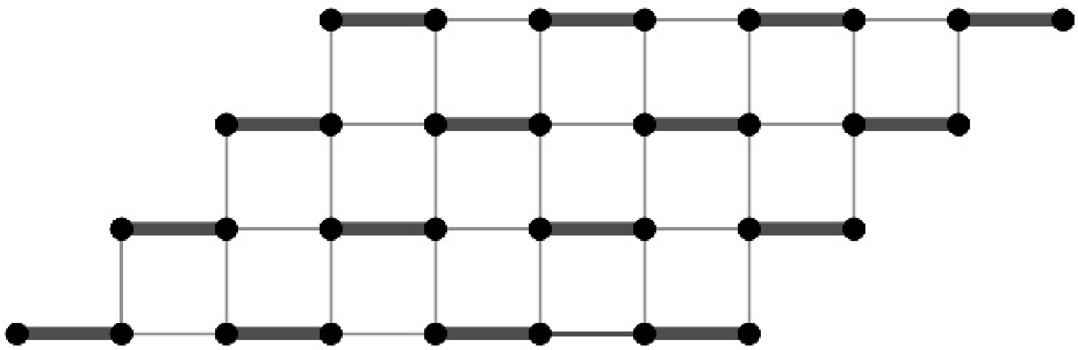

Figure 3.1: A subgraph of $\mathbb{Z}^2$ with a unique perfect matching

We only give the outline of the proof, the interested reader should consult the paper [47] for more details.

Given a matching M, let $U(M)$ be the vertices uncovered by M. The first step in the proof of Theorem 8.1 is the following simple observation.

Proposition 8.2. *Let G be a finite tree. Then any matching M of G can be uniquely reconstructed from $U(M)$.*

CEU eTD Collection

Consider a finite tree G. Let $\mathcal{M}$ be a uniform random maximum size matching of G. It follows from Proposition 8.2 that $\log \mathrm{mm}(G) = H(U(\mathcal{M}))$, where H denotes the Shannon entropy. Let $\bar{P}_G$ be the orthogonal projection to the kernel of the adjacency operator of G. The next theorem shows that $U(\mathcal{M})$ is a determinantal process.

Theorem 8.3. *Let G be a finite tree. Then $U(\mathcal{M})$ is the determinantal process corresponding to the orthogonal projection $\bar{P}_G$.*

Next we show that in the settings of Theorem 8.1, the finite graph positive contractions $(G_n, \bar{P}_{G_n})$ converge to $(G, o, \bar{P}_G)$, where (G, o) in the Benajamini-Schramm limit of G_n. Thus, Theorem 2.4 can be applied to deduce Theorem 8.1.

9 Measurability of the polar decomposition

We need the following characterisation of the polar decomposition.

Lemma 9.1. *Let T be a bounded operator, and let $T = UP$, be it polar decomposition. Then $P = (T^*T)^{\frac{1}{2}}$. Moreover, $U = \lim_{\varepsilon\to 0+} T(\varepsilon I + T^*T)^{-\frac{1}{2}}$ in the strong operator topology.*[1]

Proof. The formula for P is well-known. To verify the formula for U, we need to prove three three things. (1) The limit indeed exists. (2) $\|Ux\| = \|x\|$ for any $x \in (\ker T)\perp$ and $\ker T \subset \ker U$. (3) $T = UP$.

To prove (1), fix an element x of the Hilbert-space, and consider $\varepsilon_1, \varepsilon_2 > 0$, then

$$\begin{aligned}
&\|T(\varepsilon_1 I + T^*T)^{-\frac{1}{2}}x - T(\varepsilon_2 I + T^*T)^{-\frac{1}{2}}x\|^2\\
&\quad= \left\langle T\left((\varepsilon_1 I + T^*T)^{-\frac{1}{2}} - (\varepsilon_2 I + T^*T)^{-\frac{1}{2}}\right)x, T\left((\varepsilon_1 I + T^*T)^{-\frac{1}{2}} - (\varepsilon_2 I + T^*T)^{-\frac{1}{2}}\right)x\right\rangle\\
&\quad= \left\langle\left((\varepsilon_1 I + T^*T)^{-\frac{1}{2}} - (\varepsilon_2 I + T^*T)^{-\frac{1}{2}}\right)T^*T\left((\varepsilon_1 I + T^*T)^{-\frac{1}{2}} - (\varepsilon_2 I + T^*T)^{-\frac{1}{2}}\right)x, x\right\rangle\\
&\quad= \int_0^{\|T^*T\|} \mu_{T^*T,x}(t),
\end{aligned}$$

where $h_{\varepsilon_1,\varepsilon_2}(t) = t\left((\varepsilon_1+t)^{-\frac{1}{2}} - (\varepsilon_2+t)^{-\frac{1}{2}}\right)^2$, and $\mu_{T^*T,x}(t)$ is the spectral measure corresponding to T^*T and x. Note that for any $t \geq 0$, and $\varepsilon_1, \varepsilon_2 > 0$, we have

$$h_{\varepsilon_1,\varepsilon_2}(t) = \left(\sqrt{\frac{t}{t+\varepsilon_1}} - \sqrt{\frac{t}{t+\varepsilon_2}}\right)^2 \leq 1.$$

Also for any fixed $t \geq 0$, we have $\lim h_{\varepsilon_1,\varepsilon_2}(t) = 0$, as $(\varepsilon_1, \varepsilon_2)$ tends to 0. Thus, form the dominated convergence theorem, we see that $\|T(\varepsilon_1 I + T^*T)^{-\frac{1}{2}}x - T(\varepsilon_2 I + T^*T)^{-\frac{1}{2}}x\|^2$ converges to 0, as $(\varepsilon_1, \varepsilon_2)$ tends to 0. Therefore, $\lim_{\varepsilon\to 0+} T(\varepsilon I + T^*T)^{-\frac{1}{2}}x$ indeed exists.

[1] Note that the spectrum of $\varepsilon I + T^*T$ is contained in $[\varepsilon, \varepsilon + \|T^*T\|]$, so $(\varepsilon I + T^*T)^{-\frac{1}{2}}$ is well defined by functional calculus.

CEU eTD Collection

To prove (2) observe that

$$\left\|T(\varepsilon I+T^*T)^{-\frac{1}{2}}x\right\|^2=\langle(\varepsilon I+T^*T)^{-\frac{1}{2}}T^*T(\varepsilon I+T^*T)^{-\frac{1}{2}}x,x\rangle=\int_0^{\|T^*T\|}g_\varepsilon(t)\mu_{T^*T,x}(t)$$

where $g_\varepsilon(t)=\frac{t}{t+\varepsilon}$. Note that $\lim_{\varepsilon\to 0}g_\varepsilon(0)=0$ and $\lim_{\varepsilon\to 0}g_\varepsilon(t)=1$ for any $t>0$. Moreover $|g_\varepsilon(t)|\leq 1$ for any $t,\varepsilon>0$. Thus, from the dominated convergence theorem, we have

$$\lim_{\varepsilon\to 0}\left\|T(\varepsilon I+T^*T)^{-\frac{1}{2}}x\right\|^2=\mu_{T^*T,x}\left((0,\|T^*T\|]\right).$$

Therefore, $\|Ux\|=\|x\|$ for any $x\in(\ker T)^\perp=\ker(T^*T)^\perp$ and $\ker T\subset\ker U$.

To prove (3) observe that

$$\begin{aligned}&\left\|T\left((\varepsilon I+T^*T)^{-\frac{1}{2}}(T^*T)^{\frac{1}{2}}-I\right)x\right\|^2\\&=\left\langle\left((\varepsilon I+T^*T)^{-\frac{1}{2}}(T^*T)^{\frac{1}{2}}-I\right)T^*T\left((\varepsilon I+T^*T)^{-\frac{1}{2}}(T^*T)^{\frac{1}{2}}-I\right)x,x\right\rangle\\&=\int f_\varepsilon(t)\mu_{T^*T,x}(t),\end{aligned}$$

where $f_\varepsilon(t)=t((\frac{t}{t+\varepsilon})^{\frac{1}{2}}-1)^2$. Note that $\lim_{\varepsilon\to 0}f_\varepsilon(t)=0$ for any t, moreover, $|f_\varepsilon(t)|<\|T^*T\|$ for any $t,\varepsilon>0$. Thus, the statement again follows from the dominated convergence theorem. □

Now it is clear that for any polynomial f, the map $(G,o,T)\mapsto(G,o,f(T))$ is measurable. Thus, by functional calculus, the map $(G,o,T)\mapsto(\varepsilon I+T^*T)^{-\frac{1}{2}}$ is also measurable. Therefore, the polar decomposition is also measurable.

CEU eTD Collection

CEU eTD Collection

Bibliography

[1] Miklos Abért, Andreas Thom, and Balint Virág. "Benjamini-Schramm convergence and pointwise convergence of the spectral measure". In: *preprint* (2013).

[2] Miklós Abért, Péter Csikvári, Péter Frenkel, and Gábor Kun. "Matchings in Benjamini–Schramm convergent graph sequences". In: *Transactions of the American Mathematical Society* 368.6 (2016), pp. 4197–4218.

[3] Miklós Abért and Benjamin Weiss. In: *In preparation* ().

[4] David Aldous and Russell Lyons. "Processes on unimodular random networks". In: *Electronic Journal of Probability* 12 (2007), pp. 1454–1508.

[5] Tim Austin. "Additivity properties of sofic entropy and measures on model spaces". In: *Forum of Mathematics, Sigma*. Vol. 4. Cambridge University Press. 2016.

[6] Tim Austin and Moumanti Podder. "Gibbs measures over locally tree-like graphs and percolative entropy over infinite regular trees". In: *Journal of Statistical Physics* 170.5 (2018), pp. 932–951.

[7] Ágnes Backhausz and Balázs Szegedy. "On large-girth regular graphs and random processes on trees". In: *Random Structures & Algorithms* 53.3 (2018), pp. 389–416.

[8] Rémi Bardenet and Odalric-Ambrym Maillard. "Concentration inequalities for sampling without replacement". In: *Bernoulli* 21.3 (2015), pp. 1361–1385.

[9] Itai Benjamini, Russell Lyons, Yuval Peres, and Oded Schramm. "Special invited paper: uniform spanning forests". In: *Annals of probability* (2001), pp. 1–65.

[10] Itai Benjamini and Oded Schramm. "Recurrence of distributional limits of finite planar graphs". In: *Electron. J. Probab.* 6 (2000), pp. 1–13.

[11] Manjul Bhargava, Daniel M Kane, Bjorn Poonen, and Eric Rains. "Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves". In: *arXiv preprint arXiv:1304.3971* (2013).

[12] Rajendra Bhatia. "Matrix analysis, volume 169 of". In: *Graduate texts in mathematics* (1997).

[13] Béla Bollobás. "A probabilistic proof of an asymptotic formula for the number of labelled regular graphs". In: *European Journal of Combinatorics* 1.4 (1980), pp. 311–316.

[14] Béla Bollobás. "The independence ratio of regular graphs". In: *Proceedings of the American Mathematical Society* (1981), pp. 433–436.

[15] Christian Borgs, Jennifer Chayes, Jeff Kahn, and László Lovász. "Left and right convergence of graphs with bounded degree". In: *Random Structures & Algorithms* 42.1 (2013), pp. 1–28.

[16] Lewis Bowen. "Measure conjugacy invariants for actions of countable sofic groups". In: *Journal of the American Mathematical Society* 23.1 (2010), pp. 217–245.

[17] Robert Burton and Robin Pemantle. "Local characteristics, entropy and limit theorems for spanning trees and domino tilings via transfer-impedances". In: *The Annals of Probability* (1993), pp. 1329–1371.

[18] Julien Clancy, Nathan Kaplan, Timothy Leake, Sam Payne, and Melanie Matchett Wood. "On a Cohen–Lenstra heuristic for Jacobians of random graphs". In: *Journal of Algebraic Combinatorics* 42.3 (2015), pp. 701–723.

[19] Julien Clancy, Timothy Leake, and Sam Payne. "A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs". In: *Experimental Mathematics* 24.1 (2015), pp. 1–7.

CEU eTD Collection

[20] Henri Cohen and Hendrik W Lenstra. "Heuristics on class groups of number fields". In: *Number Theory Noordwijkerhout 1983*. Springer, 1984, pp. 33–62.

[21] Thomas M Cover. *Elements of information theory*. John Wiley & Sons, 1999.

[22] Péter Csikvári. "Matchings in vertex-transitive bipartite graphs". In: *Israel Journal of Mathematics* 215.1 (2016), pp. 99–134.

[23] Noam Elkies, Greg Kuperberg, Michael Larsen, and James Propp. "Alternating-sign matrices and domino tilings (Part I)". In: *Journal of Algebraic Combinatorics* 1.2 (1992), pp. 111–132.

[24] Jordan S Ellenberg, Akshay Venkatesh, and Craig Westerland. "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields". In: *annals of Mathematics* (2016), pp. 729–786.

[25] Matthew Farrell and Lionel Levine. "CoEulerian graphs". In: *Proceedings of the American Mathematical Society* 144.7 (2016), pp. 2847–2860.

[26] William Feller. *An Introduction to Probability Theory and its Applications (Volume 1)*. John Wiley & Sons.

[27] Eduardo Friedman and Lawrence C Washington. "On the distribution of divisor class groups of curves over a finite field". In: *Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin* (1989), pp. 227–239.

[28] Alan Frieze. "Random structures and algorithms". In: *Proceedings of the International Congress of Mathematicians-Seoul 2014. Vol. 1* (2014), pp. 311–340.

[29] Olle Häggström. "Uniform and minimal essential spanning forests on trees". In: *Random Structures & Algorithms* 12.1 (1998), pp. 27–50.

[30] David R Heath-Brown. "The size of Selmer groups for the congruent number problem, II". In: (1994).

[31] Deborah Heicklen and Russell Lyons. "Change intolerance in spanning forests". In: *Journal of Theoretical Probability* 16.1 (2003), pp. 47–58.

[32] Alexander E Holroyd, Lionel Levine, Karola Mészáros, Yuyal Peres, James Propp, and David B Wilson. "Chip-firing and rotor-routing on directed graphs". In: *In and out of equilibrium 2*. Springer, 2008, pp. 331–364.

[33] Jiaoyang Huang. "Invertibility of adjacency matrices for random d-regular graphs". In: *arXiv preprint arXiv:1807.06465* (2018).

[34] Jiaoyang Huang. "Invertibility of adjacency matrices for random d-regular directed graphs". In: *arXiv preprint arXiv:1806.01382* (2018).

[35] Svante Janson. "Random regular graphs: asymptotic distributions and contiguity". In: *Combinatorics, Probability and Computing* 4.4 (1995), pp. 369–405.

[36] Antal A Járai. "Sandpile models". In: *Probability Surveys* 15 (2018), pp. 243–306.

[37] PW Kasteleyn. "The statistics of dimers on a lattice: I. The number of dimer arrangements on a quadratic lattice". In: *Physica* 27.12 (1961), pp. 1209–1225.

[38] Shaked Koplewitz. "Sandpile groups and the coeulerian property for random directed graphs". In: *Advances in Applied Mathematics* 90 (2017), pp. 145–159.

[39] Lionel Levine. "What is... a sandpile". In: *Notices Amer. Math. Soc.* Citeseer. 2010.

[40] Russell Lyons. "A bird's-eye view of uniform spanning trees and forests". In: *Microsurveys in discrete probability* 41 (1998), pp. 135–162.

[41] Russell Lyons. "Asymptotic enumeration of spanning trees". In: *Combinatorics, Probability and Computing* 14.4 (2005), pp. 491–522.

[42] Russell Lyons. "Determinantal probability measures". In: *Publications Mathématiques de l'IHÉS* 98 (2003), pp. 167–212.

[43] Russell Lyons and Andreas Thom. "Invariant coupling of determinantal measures on sofic groups". In: *Ergodic Theory and Dynamical Systems* 36.2 (2016), pp. 574–607.

[44] Jessie MacWilliams. "Orthogonal matrices over finite fields". In: *The American Mathematical Monthly* 76.2 (1969), pp. 152–164.

CEU eTD Collection

[45] Brendan D McKay. “Spanning trees in regular graphs”. In: *European Journal of Combinatorics* 4.2 (1983), pp. 149–160.

[46] András Mészáros. “Limiting entropy of determinantal processes”. In: *Annals of Probability* 48.5 (2020), pp. 2615–2643.

[47] András Mészáros. “Matchings on trees and the adjacency matrix: A determinantal viewpoint”. In: *arXiv preprint arXiv:2011.04012* (2020).

[48] András Mészáros. “The distribution of sandpile groups of random regular graphs”. In: *Transactions of the American Mathematical Society* 373.9 (2020), pp. 6529–6594.

[49] Michael S. O. Molloy, Hanna Robalewska, Robert W. Robinson, and Nicholas C. Wormald. “1-Factorizations of random regular graphs”. In: *Random Structures & Algorithms* 10.3 (1997), pp. 305–321.

[50] Hoi H Nguyen and Melanie Matchett Wood. “Cokernels of adjacency matrices of random r-regular graphs”. In: *arXiv preprint arXiv:1806.10068* (2018).

[51] Serguei Norine and Peter Whalen. “Jacobians of nearly complete and threshold graphs”. In: *European Journal of Combinatorics* 32.8 (2011), pp. 1368–1376.

[52] Robin Pemantle. “Choosing a spanning tree for the integer lattice uniformly”. In: *The Annals of Probability* (1991), pp. 1559–1574.

[53] Walter Rudin. *Principles of mathematical analysis*. McGraw-hill New York, 1976.

[54] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[55] Brandon Seward. “Weak containment and Rokhlin entropy”. In: *arXiv preprint arXiv:1602.06680* (2016).

[56] Harold NV Temperley and Michael E Fisher. “Dimer problem in statistical mechanics – an exact result”. In: *Philosophical Magazine* 6.68 (1961), pp. 1061–1063.

[57] Van Vu. “Random discrete matrices”. In: *Horizons of combinatorics*. Springer, 2008, pp. 257–280.

[58] Melanie Wood. “The distribution of sandpile groups of random graphs”. In: *Journal of the American Mathematical Society* 30.4 (2017), pp. 915–958.

[59] Melanie Matchett Wood. “personal communication”. In: (2018).

[60] Melanie Matchett Wood. “Random integral matrices and the Cohen-Lenstra heuristics”. In: *American Journal of Mathematics* 141.2 (2019), pp. 383–398.

CEU eTD Collection