The distribution of sandpile groups of random regular graphs

András Mészáros

June 26, 2018

Abstract

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 probability that the $p$-Sylow subgroup of the sandpile group is a given $p$-group $P$, is proportional to $|\text{Aut}(P)|^{-1}$. For finitely many primes, these events get independent in limit. Similar results hold for undirected random regular graphs, there for odd primes the limiting distributions are the ones given by Clancy, Leake and Payne.

Our results extends a recent theorem of Huang saying that the adjacency matrices of random $d$-regular directed graphs are invertible with high probability to the undirected case. It also gives an alternate proof of a theorem of Backhausz and Szegedy.

1 Introduction

Fix $d \geq 3$. We consider two random $d$-regular graph models. The graph of a permutation $\pi$ 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 $\{1, 2, \ldots, n\}$. Thus, the adjacency matrix $A_n$ of $D_n$ is just obtained as $A_n = P_1 + P_2 + \ldots + P_d$, where $P_1, P_2, \ldots P_d$ 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 $\Delta_n$ 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 $\Delta_n$ is denoted by $\text{RowSpace}(\Delta_n)$. The group $\Gamma_n = \mathbb{Z}^{n-1}/\text{RowSpace}(\Delta_n)$ is called the sandpile group of $D_n$. If $D_n$ is strongly connected (which happens with high probability as $n \to \infty$), then $\Gamma_n$ 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 an eulerian directed graph. 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 result is the following.

*Central European University, Budapest

e-mail: Meszaros_Andras@phd.ceu.edu
Theorem 1. Let $p_1, p_2, \ldots, p_s$ be distinct primes. Let $\Gamma_n$ be the sandpile group of $D_n$. Let $\Gamma_{n,i}$ be the $p_i$-Sylow subgroup of $\Gamma_n$. For $i = 1, 2, \ldots, s$ let $G_i$ be a finite abelian $p_i$-group. Then

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

(1)

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

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

(2)

Assume that $d$ is even and $p_1 = 2$. There is a probability distribution $\nu$ on the set (of isomorphism classes) of finite abelian 2-groups, which is supported on groups with odd rank$^1$, such that

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

We were not able to give an explicit formula for $\nu$. See Section 8 for characterizations of this distribution.

The distribution appearing in equation (1) is called the Cohen-Lenstra heuristics. Given a prime $p$, it is a probability distribution on the set (of isomorphism classes) of finite abelian $p$-groups, such that the probability of a group $G$ is proportional to $|\text{Aut}(G)|^{-1}$. It was introduced by Cohen and Lenstra [6] in a conjecture on the distribution of class groups of quadratic number fields. The distribution appearing in equation (2) is a modified version of the Cohen-Lenstra heuristics that was introduced by Clancy et al [4, 5].

A recent, deep paper of Wood [20] shows that the sandpile group of dense Erdős-Rényi random graphs satisfies the latter heuristic. That is, Theorem 1 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 4 for our model.

We will 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 $\Gamma$ and a fixed finite abelian group $V$, we call the expectation $\mathbb{E}[\text{Sur}(\Gamma, V)]$ the surjective $V$-moment of $\Gamma$. Our next theorem determines the limits of the surjective moments of the sandpile groups for our random graph models. The convergence of these moments then implies Theorem 1 using the work of Wood [20].

Theorem 2. Let $\Gamma_n$ be the sandpile group of $D_n$. For any finite Abelian group $V$ we have

$$\lim_{n \to \infty} \mathbb{E}[\text{Sur}(\Gamma_n, V)] = 1.$$

$^1$The rank of a group is the minimum number of generators.
Let $\Gamma_n$ be the sandpile group of $H_n$. Let $V$ be a finite Abelian group. If $d$ is odd, then

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

if $d$ is even, then

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

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

This theorem is proved by using the fact that the adjacency matrices $A_n$ and $C_n$ both exhibit strong mixing properties, when they are acting on $V^n$. To state these results, we need a few definitions. Let $V$ be a finite abelian group. For $q = (q_1, q_2, \ldots, q_n) \in V^n$ the minimal coset in $V$ containing $q_1, q_2, \ldots, q_n$ is denoted by $\text{MinC}_q$, the sum of the components of $q$ is denoted by $s(q) = \sum_{i=1}^n q_i$, and we define

$$R(q, d) = \{r \in (d \cdot \text{MinC}_q)^n \mid s(r) = ds(q)\}.$$ 

It is straightforward to check that $A_n q \in R(q, d)$ with probability 1. 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 $d_\infty(X, Y) = \max_{r \in \mathcal{R}} |P(X = r) - P(Y = r)|$. We prove that the distribution of $A_n q$ is close to that of $U_{q,d}$ in the following sense.

**Theorem 3.** 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 $<q \otimes w> = \sum_{i=1}^n q_i \otimes w_i$. Let $I_2 = I_2(V)$ be the subgroup of $V \otimes V$ generated by the set $\{a \otimes b + b \otimes a \mid a, b \in V\}$. Let $\text{Rank}_2(V)$ 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 subgroup of $I$ of index $2^{\text{Rank}_2(V)}$. 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

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

It is clear from what is written above that $C_n q \in R^S(q, d)$ with probability 1. Similarly before let $U_{q,d}^S$ be a uniform random element of $R^S(q, d)$. Then we have

**Theorem 4.** For $d \geq 3$ we have

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

Note that the limits in Theorem 2, Theorem 3 and Theorem 4 are uniform in $d$. See Section 6 for further discussion.

Recently, Huang [13] considered a slightly different random $d$-regular directed graph model on $n$ vertices, the so-called configuration model. 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

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

---

[2] By definition $d \cdot \text{MinC}_q = \{g_1 + g_2 + \cdots + g_d | g_1, g_2, \ldots, g_d \in \text{MinC}_q\}$. 

3
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

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

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

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

This solves an open problem of Frieze [10] and Vu [19] for random regular bipartite graphs.

Using Theorem 4 we can extend these results of Huang for the random regular graphs \( H_n \).

**Proposition 5.** For the adjacency matrix \( C_n \) of \( H_n \) we have

\[
P(C_n \text{ is singular in } \mathbb{R}) = o(1).
\]

Indeed, from Theorem 4 with the choice of \( V = \mathbb{F}_p \) it is straightforward to prove that for a prime \( p \) such that \( \gcd(p, d) = 1 \), we have

\[
\mathbb{E}\{0 \neq x \in \mathbb{F}_p^m \mid C_n x = 0\} = 1 + o(1).
\]

Therefore, the statement follows as above.

Theorem 1 describes the local behavior of the sandpile group \( \Gamma_n \) of \( H_n \). Now we try to gain some global information on these groups. The next statement is about the asymptotic order of \( \Gamma_n \). This is a special case of the theorem of Lyons [17]. Let us choose \( H_2, H_4, \ldots \) independently.

The torsion part of \( \Gamma_n \) is denoted by \( \text{tors}(\Gamma_n) \).

**Theorem 6** (Lyons). There is a \( 0 < \tau_d < \infty \) such that with probability 1 we have

\[
\lim_{n \to \infty} \frac{\log |\text{tors}(\Gamma_n)|}{n} = \tau_d.
\]

Theorem 2 leads to the following statement on the rank of \( \Gamma_n \).

**Theorem 7.** With probability 1 we have

\[
\lim_{n \to \infty} \frac{\text{Rank}(\Gamma_n)}{n} = 0.
\]

Observe that \( \text{Rank}(\text{tors}(\Gamma_n)) = \max_p \text{ a prime } \text{ Rank}_p(\text{tors}(\Gamma_n)) \), where \( \text{Rank}_p(\text{tors}(\Gamma_n)) \) is the rank of the \( p \)-Sylow subgroup of \( \text{tors}(\Gamma_n) \). Therefore, this theorem means that many primes contribute to reach the growth described in Theorem 6.

A conjecture of Abért and Szegedy [11] states that if \( G_1, G_2, \ldots \) 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 \( \text{co-rank}_p G_n = \dim \ker A_n \), where \( A_n \) 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-Schramm 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 the lines of Theorem 7 one can prove that

\[
\lim_{n \to \infty} \frac{\max_p \text{ a prime } \text{ co-rank}_p(H_n)}{n} = 0.
\]
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 [2].

Theorem 1 follows from Theorem 2 using the results of Wood [20] 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 $X_1, X_2, \ldots$ 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 [7] proved that the answer is affirmative for both questions in the special case when each surjective moment of $X$ is 1. In this case $X$ follows the Cohen-Lenstra heuristic. Later, it was proved by Wood [20] that the answer is yes for both questions if the moments do not grow too fast, namely if $E|\text{Sur}(X,V)| \leq |\land^2 V|$ for any finite abelian $p$-group $V$. The proof generalizes the ideas of Heath-Brown [11]. In [20] this is stated only in the special case, when the limiting surjective $V$-moments of $X$ are exactly $|\land^2 V|$, but in a later paper of Wood [21] 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 [20] 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 5.

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 $\text{RowSpace}(M) = \{ xM | x \in \mathbb{Z}_p^n \}$. The cokernel of $M$ is defined as $\text{cok}(M) = \mathbb{Z}_p^m/\text{RowSpace}(M)$. Freidman and Washington [9] proved that if $M_n$ is an $n \times n$ random matrix over $\mathbb{Z}_p$, with respect to the Haar-measure, then $\text{cok}(M_n)$ asymptotically follows the Cohen-Lenstra heuristic, that is, for any finite abelian $p$-group $G$ we have

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

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 [21]. Her paper also contains similar results for non-square matrices.

Bhargava, Kane, Lenstra, Poonen and Rains [3] 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 [5]. Let $M_n$ be a Haar-uniform symmetric random matrix over $\mathbb{Z}_p$. Then for any finite abelian $p$-group $G$ we have

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

This is exactly the distribution appearing in Theorem 1. Note that this is not the original formula given in [5], but it can be easily deduced from it, see [20]. 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 [20]. If $G = \bigoplus_i \mathbb{Z}/p^{\lambda_i} \mathbb{Z}$ with $\lambda_1 \geq \lambda_2 \geq \cdots$ and $\mu$ is the transpose of the partition $\lambda$, then

$$
\frac{|\phi : G \times G \to \mathbb{C}^* \text{ symmetric, bilinear, perfect}|}{|G| |\text{Aut}(G)|} = p^{-\sum_i \mu_i(\mu_i + 1)} \prod_{i=1}^{\lambda_1} \prod_{j=1}^{\lambda_i - \lambda_{i-1}} (1 - p^{-2j})^{-1}. \quad (3)
$$
The structure of the paper

Section 2 contains the basic definitions that we need, including the notion of typical vectors. Moreover, it also contains a brief summary of results on distribution of sandpile groups. In Section 3 we investigate the distribution of $A_n q$, where $q$ is a typical vector. These theorems 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 3, 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 paper 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 7. At many points of the paper we need to estimate the probabilities of certain non-typical events, the proofs of these lemmas are collected in Section 10.

2 Preliminaries

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

Consider a vector $q = (q_1, q_2, \ldots, q_n) \in V^n$. For a permutation $\pi$ of the set $[n] = \{1, 2, \ldots, n\}$ the vector $q_\pi = (q_{\pi(1)}, q_{\pi(2)}, \ldots, q_{\pi(n)})$ 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 $q_\pi$, where $\pi$ is chosen uniformly from the set of all permutations, or equivalently, as a uniform random element of $S(q)$.

Let $S_{q,h} = \sum_{i=1}^{n} q^{(i)}$, where $q^{(1)}, q^{(2)}, \ldots, q^{(n)}$ are independent random permutations of $q$. Here we repeat our earlier observation that $S_{q,h} \in R(q, h)$. 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

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

so $m_q$ can be considered as a vector in $\mathbb{R}^{V}$. 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 8.** A vector $q \in V^n$ is called $\alpha$-typical if $\|m_q - \frac{n}{|V|} 1\|_\infty < n^\alpha$. Here $1$ is the all 1 vector and $\|\cdot\|_\infty$ is the maximum norm.

Note that if $\alpha > \frac{1}{2}$ then a uniform element of $|V|^n$ will be $\alpha$-typical with probability $1 - o(1)$.

One of the key steps towards Theorem 3 is the following.

**Theorem 9.** For $d \geq 3$ and $\frac{1}{2} < \alpha < \frac{2}{3}$ we have

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

This will be an easy consequence of the following theorem.

**Theorem 10.** Fix $\frac{1}{2} < \alpha < \beta < \frac{2}{3}$ and $h \geq 2$, then we have

$$ \lim_{n \to \infty} \sup_{q \in V^n} \sup_{\alpha\text{-typical}} \sup_{\beta\text{-typical}} |P(S_{q,h} = r)|V|^{n-1} - 1| = 0. $$
In the proofs we often need to consider \( h \)-tuples \( Q = (q^{(1)}, q^{(2)}, \ldots, q^{(h)}) \) where each \( q^{(i)} \) is a permutation of a fixed \( q \in V^n \). Such \( h \)-tuples will be called \((q,h)\)-tuples. Let \( Q_{q,h} \) be the set of \((q,h)\)-tuples. A random \((q,h)\)-tuple is \( \bar{Q} = (\bar{q}^{(1)}, \bar{q}^{(2)}, \ldots, \bar{q}^{(h)}) \), where \( \bar{q}^{(1)}, \bar{q}^{(2)}, \ldots, \bar{q}^{(h)} \) 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 \( Q = (Q_1, Q_2, \ldots, Q_n) \) in \((V^h)^n \), where \( Q_i = (q_i^{(1)}, q_i^{(2)}, \ldots, q_i^{(h)}) \). 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

\[
m_Q(t) = |\{i \mid Q_i = t\}|.
\]

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, \( m_Q(\{t \in V^h \mid t_1 = c\}) \) stands for \( m_Q(\{t \in V^h \mid t_1 = c\}) \).

Fix a \( \gamma \) such that \( \frac{2}{7} < \alpha < \beta < \gamma < \frac{2}{3} \).

**Definition 11.** A \((q,h)\)-tuple \( Q \) or \( m_Q \) itself will be called \( \gamma \)-typical if \( \|m_Q - \frac{n}{|V|^n} I\|_\infty < n^\gamma \).

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

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

**Definition 12.** Let \( X_1, X_2, \ldots \) and \( Y_1, Y_2, \ldots \) 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 [10] then can be reformulated as \( P(\Sigma = r) \sim \frac{1}{|V|^{n-1}} \) uniformly for any \( \alpha \)-typical \( q \in V^n \) and \( \beta \)-typical \( r \in R(q,h) \).

**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 \( \Delta \) 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 \( \Delta_s \) is obtained from \( \Delta \) by deleting the row and column corresponding to \( s \). The group \( \Gamma_s = \mathbb{Z}^{n-1}/\text{RowSpace}(\Delta_s) \) is called the sandpile group at vertex \( s \). The order of \( \Gamma_s \) is the number of spanning trees in \( D \) oriented towards \( s \). Let \( \mathbb{Z}_0^n = \{ x \in \mathbb{Z}^n \mid \sum_{i=1}^{n} x_i = 0 \} \). Note that every row of \( \Delta \) is in \( \mathbb{Z}_0^n \). Thus the following definition makes sense. The group \( \Gamma = \mathbb{Z}_0^n/\text{RowSpace}(\Delta) \) 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 [8].
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 [15] [16] [12] for more information on sandpile groups.

We already mentioned the result of Wood [20] on Erdős-Rényi random graphs. Here we give more details. For $0 \leq q \leq 1$, the Erdős-Rényi random graph $G(n, q)$ is a graph on the vertex set $\{1, 2, \ldots, n\}$, such that for each pair of vertices they are connected with probability $q$ independently. Let $p_1, p_2, \ldots, p_s$ be distinct primes. Fix $0 < q < 1$. Let $Γ_n$ be the sandpile group of $G(n, q)$. Let $Γ_{n,i}$ be the $p_i$-Sylow subgroup of $Γ_n$, and for $i = 1, 2, \ldots, s$ let $G_i$ be a finite abelian $p_i$-group. Then

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

See equation (3) for an even more explicit formula.

Koplewitz [14] proved the analogous result for directed graphs. For $0 \leq q \leq 1$, the random directed graph $D(n, q)$ is a graph on the vertex set $\{1, 2, \ldots, n\}$, such that for each ordered pair of vertices they are connected with a directed edge with probability $q$ independently. Let $p_1, p_2, \ldots, p_s$ be distinct primes. Fix $0 < q < 1$. Let $Γ_n$ be the total sandpile group of $D(n, q)$. Let $Γ_{n,i}$ be the $p_i$-Sylow subgroup of $Γ_n$, and for $i = 1, 2, \ldots, s$ let $G_i$ be a finite abelian $p_i$-group. Then

$$\lim_{n \to \infty} P\left(\bigoplus_{i=1}^{s} Γ_{n,i} \cong \bigoplus_{i=1}^{s} G_i\right) = \prod_{i=1}^{s} \prod_{j=2}^{∞}(1 - p_i^{-j}).$$

Note that, unlike what we would expect knowing the undirected case, this distribution is not the same as the one given in Theorem 10 for the random directed $d$-regular graph $D_n$. A quick explanation is that $D_n$ is eulerian, while $D(n, q)$ is not.

3 Behavior of typical vectors

3.1 The proof of Theorem 10

The proofs of the lemmas stated in this subsection are postponed to the next subsection.

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

$$\mathcal{M}(q, r) = \{m_Q \mid Q \in \mathcal{Q}_{q,h}, Σ(Q) = r\}$$

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

$$P(Σ(\tilde{Q}) = r) = \sum_{m \in \mathcal{M}(q, r)} P((Σ(\tilde{Q}) = r) \land (m_\tilde{Q} = m)).$$

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 $Σ(Q) = r$ for a $(q, h)$-tuple $Q = (q^{(1)}, q^{(2)}, \ldots, q^{(h)})$, we have $m_{q^{(i)}} = m_q$ for every $i = 1, 2, \ldots, h$ and $m_{Σ(Q)} = m_r$ as the following lemma shows.

\[\text{Here we omitted from the notation the dependence on } h, \text{ later we will do this several times without mentioning it.}\]
Lemma 13. Consider \( q, r \in V^n \). Let \( m \in \mathcal{M}(q, r) \). Then \( m \) is a non-negative integral vector satisfying the following linear equations.

For \( i = 1, 2, \ldots, h \) and \( c \in V \)
\[
m(t_i) = c = m_q(c),
\]
and for \( c \in V \)
\[
m(t_\Sigma) = c = m_r(c).
\]

Now assume that \( m \) is a nonnegative integral vector satisfying the equations above, then
\[
P((\Sigma(Q) = r_1) \land (m_Q = m)) = \frac{\prod_{t \in V} m_r(c)!}{\prod_{t \in V^d} m(t)!} \cdot \left(\frac{n!}{\prod_{t \in V} m_q(c)}\right)^h
\]
\[
= \frac{\prod_{t \in V} m(t_\Sigma)!}{\prod_{t \in V^d} m(t)!} \cdot \left(\frac{n!}{\prod_{t \in V} m_q(c)}\right)^h.
\]

In particular, \( P((\Sigma(Q) = r_1) \land (m_Q = m)) > 0 \) 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.

The left hand sides of the equations (4) and (5) in Lemma 13 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 \( A(q, r_2) \). Of course the are many such translations, we will use the one given in the next lemma.

Lemma 14. For any \( r_1, r_2 \in V^n \) we define the vector \( v = v_{r_1, r_2} \) by
\[
v(t) = \frac{m_{r_2}(t_\Sigma) - m_{r_1}(t_\Sigma)}{|V|^{h-1}}
\]
for every \( t \in V^h \). Then for any \( q \in V^h \) we have
\[
A(q, r_1) + v_{r_1, r_2} = A(q, r_2).
\]

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 \( \|x - y\|_\infty < D \).

Lemma 15. If \( r \in R(q, h) \) then \( A(q, r) \) contains an integral point.

Now 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 \( \alpha \)-typical \( q \in V^n \) fix an arbitrary \( \beta \)-typical \( r_0 = r_0(q) \in R(q, h) \). Set
\[
\mathcal{M}^*(q, r_0) = \{m \in \mathcal{M}(q, r_0) \mid \|m - \frac{n}{|V|^h}1\|_\infty < 2n^\gamma\}.
\]

For any other \( \beta \)-typical \( r \in R(q, h) \) we define
\[
\mathcal{M}^*(q, r) = \{m + \hat{v}_{r_0, r} \mid m \in \mathcal{M}^*(q, r_0)\} \subset \mathcal{M}(q, r).
\]

Observe that for large enough \( n \), if both \( r_0 \) and \( r \) are \( \beta \)-typical, then
\[
\|\hat{v}_{r_0, r}\|_\infty < D + \frac{2n^\beta}{|V|^{|h-1|}} < n^\gamma.
\]
Thus, using that the map $m \mapsto m + \hat{v}_{\gamma_{\xi,\eta}}$ 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 $\alpha$-typical $q \in V^n$ and $\beta$-typical $r \in R(q, h)$ we have

$$\{m \in \mathcal{M}(q, r) \mid \|m - \frac{n}{|V|^n} \mathbf{1}_\infty < n\} \subset \mathcal{M}^*(q, r).$$

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

The crucial point of our argument is the next lemma.

**Lemma 16.** For an $\alpha$-typical $q \in V^n$, a $\beta$-typical $r \in R(q, h)$, $r_0 = r_0(q)$ and $m \in \mathcal{M}^*(q, r_0)$ we have that

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

uniformly in the sense of Definition 12.

From this it follows immediately that for an $\alpha$-typical $q$ and $\beta$-typical $r_1, r_2 \in R(q, h)$ we have

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

uniformly, or equivalently

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

uniformly.

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

**Lemma 17.** We have

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

2. For an $\alpha$-typical $q \in V^n$ we have $P(\bar{Q} \text{ is } \gamma \text{ - typical}) \sim 1$ uniformly in the sense of Definition 12.

3. For an $\alpha$-typical $q \in V^n$ we have $P(\Sigma(\bar{Q}) \text{ is } \beta \text{ - typical}) \sim 1$ uniformly in the sense of Definition 12.

4. The following holds

$$\lim_{n \to \infty} \sup_{q \in V^n} P((\Sigma(\bar{Q}) = r) \land (\bar{Q} \text{ is not } \gamma \text{ - typical}) \mid |V|^{n-1} = 0.$$

Fix an $\alpha$-typical $q \in V^n$. For every $\beta$-typical $r \in R(q, h)$ consider the events $(\Sigma(\bar{Q}) = r) \land (m_{\bar{Q}} \in \mathcal{M}^*(q, r))$. These events are pairwise disjoint. Moreover, from (7) above we see that their union contains the event $(\Sigma(\bar{Q}) \text{ is } \beta \text{ - typical}) \land (\bar{Q} \text{ is } \gamma \text{ - typical})$ for large enough $n$. So for large enough $n$ we have

$$P((\Sigma(\bar{Q}) \text{ is } \beta \text{ - typical}) \land (\bar{Q} \text{ is } \gamma \text{ - typical})) \leq \sum_{r \in R(q, h)} P((\Sigma(\bar{Q}) = r) \land (m_{\bar{Q}} \in \mathcal{M}^*(q, r))) \leq 1.$$
From Lemma 17.2 and 17.3 we get that
\[ P((\Sigma(Q) \text{ is } \beta \text{-typical}) \land \tilde{Q} \text{ is } \gamma \text{-typical}) \sim 1. \]

Thus
\[ \sum_{r \in R(q,h)} P((\Sigma\bar{Q}) = r) \land (m \in \mathcal{M}^*(q,r))) \sim 1 \]
for every \( \alpha \)-typical \( q \in V^n \). Combining this with (8) we obtain that for every \( \alpha \)-typical \( q \in V^n \)
\[ P((\Sigma\bar{Q}) = r) \land (m \in \mathcal{M}^*(q,r))) \sim |\{r \in R(q,h) \mid r \text{ is } \beta \text{-typical}\}|^{-1} \sim |R(q,h)|^{-1} = |V|^{-(n-1)}. \]
for all \( \alpha \)-typical \( q \in V^n \) and \( \beta \)-typical \( r \in R(q,h) \). Here in the second line we use Lemma 17.1.

Finally, using Lemma 17.4 we get Theorem 10.

### 3.2 Details of the proof of Theorem 10

**Proof.** (Lemma 14) 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 the equations (4) and (5) in Lemma 13 above for \( r = r_1 \), then \( m' = m + v_{r_1, r_2} \) satisfies the equations (4) and (5) for \( r = r_2 \). Observe that for any \( i = 1, 2, \ldots, h \) and \( c, s \in V \) we have
\[ |\{t \in V^h \mid t_i = c, t_\Sigma = s\}| = |V|^{h-2}. \]
(Here we need to use that \( h \geq 2 \).) So we have
\[ \sum_{t \in V^h \atop t_i = c} m'(t) = \sum_{t \in V^h \atop t_i = c} m(t) + \sum_{t \in V^h \atop t_i = c} v_{r_1, r_2}(t) = \]
\[ m_q(c) + \sum_{s \in V} |\{t \in V^h \mid t_i = c, t_\Sigma = s\}| \frac{m_{r_2}(s) - m_{r_1}(s)}{|V|^{h-1}} = \]
\[ m_q(c) + \frac{1}{|V|} \left( \sum_{s \in V} m_{r_2}(s) - \sum_{s \in V} m_{r_1}(s) \right) = m_q(c) + \frac{1}{|V|} (n - n) = m_q(c), \]
that is equation (4) is satisfied. Furthermore, for any \( c \in V \) we have
\[ \sum_{t \in V^h \atop t_\Sigma = c} m'(t) = \sum_{t \in V^h \atop t_\Sigma = c} m(t) + \sum_{t \in V^h \atop t_\Sigma = c} v_{r_1, r_2}(t) = \]
\[ m_{r_1}(c) + |V|^{h-1} \frac{m_{r_2}(c) - m_{r_1}(c)}{|V|^{h-1}} = m_{r_2}(c), \]
that is equation (5) is satisfied. \( \square \)

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 \( i = 1, 2, \ldots, h \) 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.

**Proof.** (Lemma 15) We need to show that the system of linear equations given by equations (4) and (5) admits an integral solution. Using the integral analogue of Farkas’ lemma 13. Corollary 4.1a] we obtain that there exists an integral solution if and only if for every rational number \( 0 \leq \gamma(i, c) < 1 \) (\( i = 1, 2, \ldots, h, \quad c \in V \)) and \( 0 \leq \delta(c) < 1 \) (\( c \in V \)) such that
\[ \sum_{i=1}^h \sum_{c \in V} \gamma(i, c) u_{i,c} + \sum_{c \in V} \delta(c) w_c \text{ is an integral vector} \quad (10) \]
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 (11) translates as follows. For every \( t \in V^h \)
\[
\sum_{i=1}^{h} \gamma(i, t_i) + \delta(t_\Sigma) = 0
\]
(11)
in the group \( S^1 \). If we define \( \gamma'(i, c) = \gamma(i, c) - \gamma(i, 0) \) and \( \delta'(c) = \delta(c) + \sum_{i=1}^{h} \gamma(i, 0) \), then clearly \( \gamma'(i, 0) = 0 \) and from equation (11) with \( t = 0 \) we get that \( \delta'(0) = 0 \). Equation (11) can be rewritten as
\[
\sum_{i=1}^{h} \gamma'(i, t_i) + \delta'(t_\Sigma) = 0.
\]

For every \( i \) and \( c \), if \( t \) is such that \( t_i = c \) and \( t_j = 0 \) if \( i \neq j \) we obtain that \( \gamma'(i, c) = -\delta'(c) \). Therefore, equation (11) can be once again rewritten as
\[
\sum_{i=1}^{h} \delta'(t_i) = \delta'(t_\Sigma) = \delta'(\sum_{i=1}^{h} t_i),
\]
which means that \( \delta \) is a group homomorphism between \( V \) and \( \mathbb{Q}/\mathbb{Z} \). Thus, we get that
\[
\sum_{i=1}^{h} \sum_{c \in V} \gamma(i, c)m_q(c) + \sum_{c \in V} \delta(c)m_r(c) =
\sum_{i=1}^{h} \sum_{c \in V} (\gamma'(i, c) + \gamma(i, 0))m_q(c) + \sum_{c \in V} (\delta'(c) - \sum_{i=1}^{h} \gamma(i, 0))m_r(c) =
\sum_{i=1}^{h} \sum_{c \in V} \delta'(c)m_q(c) + \sum_{c \in V} \delta'(c)m_r(c) =
-h \sum_{c \in V} \delta'(c)m_q(c) + \sum_{c \in V} \delta'(c)m_r(c) =
-h \sum_{i=1}^{n} \delta'(q_i) + \sum_{i=1}^{n} \delta'(r_i) = \delta'(\sum_{i=1}^{n} (\delta(q_i) + \delta(r_i))) = \delta'(0) = 0
\]
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. \( \square \)

The following approximation will be useful for Lemma 19.

**Lemma 18.** Let \( K(n) = o\left(\frac{n^2}{n^2}\right) \), then for any \( |k| < K(n) \) we have
\[
(n + k)! \sim n! \exp(k \log n + \frac{k^2}{2n}).
\]

**Lemma 19.** For \( q, r \in V^n \) and \( m \in \mathcal{M}(q, r) \) such that \( \|m - \frac{n}{|V|^h} 1\|_\infty < 3n^7 \) we have
\[
P((\Sigma(\bar{Q}) = r_1) \land (mQ = m)) \sim f(q) \exp(\frac{1}{2n}B(m - \frac{n}{|V|^h} 1, m - \frac{n}{|V|^h} 1))
\]
uniformly, where \( f(q) \) is a function depending only on \( q \), and \( B : \mathbb{R}^{V^h} \times \mathbb{R}^{V^h} \to \mathbb{R} \) is bilinear form defined as
\[
B(x, y) = |V| \sum_{c \in V} \left( \sum_{t \in V^h \mid t_\Sigma = c} x(t) \right) \left( \sum_{t \in V^h \mid t_\Sigma = c} y(t) \right) - |V|^h \sum_{t \in V^h} x(t)y(t).
\]
Proof. Recall that $\gamma < \frac{2}{3}$, so Lemma 13 can be applied to obtain the approximations

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

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

Substituting these approximations in equation (6) we obtain the statement. \hfill \Box

Proof. (Lemma 16) 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 the proof of Lemma 15) Since $v_{r_0,r} \in \text{Span}_{c \in V} w_c$, we get that $v_{r_0,r}$ is also in the radical. Observe that if $n$ is large enough $\|v_{r_0,r}\|_\infty < D + \frac{2n^\gamma}{|V|^h} < n^\gamma$, so both $m$ and $m + \hat{v}_{r_0,r}$ satisfies the conditions of Lemma 19. It is also clear that $B(x,y) = O(||x||_\infty ||y||_\infty)$. We have

$$\frac{1}{2n}B(m + \hat{v}_{r_0,r}, - \frac{n}{|V|^h} 1, m + \hat{v}_{r_0,r} - \frac{n}{|V|^h} 1) =$$

$$\frac{1}{2n}B(m + (\hat{v}_{r_0,r} - v_{r_0,r}) + v_{r_0,r} - \frac{n}{|V|^h} 1, m + (\hat{v}_{r_0,r} - v_{r_0,r}) + v_{r_0,r} - \frac{n}{|V|^h} 1) =$$

$$\frac{1}{2n} \left(B(m - \frac{n}{|V|^h} 1, m - \frac{n}{|V|^h} 1) + 2B(m - \frac{n}{|V|^h} 1, \hat{v}_{r_0,r} - v_{r_0,r}) + B(\hat{v}_{r_0,r} - v_{r_0,r}, \hat{v}_{r_0,r} - v_{r_0,r})\right) =$$

$$\frac{1}{2n} \left(B(m - \frac{n}{|V|^h} 1, m - \frac{n}{|V|^h} 1) + O(4Dn^\gamma + D^2)\right) =$$

$$\frac{1}{2n}B(m - \frac{n}{|V|^h} 1, m - \frac{n}{|V|^h} 1) + O(n^{\gamma-1}).$$

Then the statement follows from Lemma 19. \hfill \Box

The statements of Lemma 17 easily follow from the next lemmas. For the proof of Lemma 20 and 22 see Section 10. Lemma 21 can be proved using Lemma 18

Lemma 20. There is a $C_1 > 0$ such that for every $\alpha$-typical $q \in V^n$ we have

$$P(\tilde{Q} \text{ is not } \gamma\text{-typical}) < C_1 \exp\left(-n^{2\gamma-1}/C_1\right).$$

Lemma 21. There is a $C_2 > 0$ such that for every $\beta$-typical $r \in V^n$ if we consider the number of permutations of $r$, i. e. the cardinality of the set $S(r) = \{r' \text{ is a permutation of } r\}$ we have

$$|S(r)| \geq |V|^n \exp\left(-C_2 n^{2\beta-1}\right).$$

Lemma 22. If $q$ is $\alpha$-typical, then

$$\lim_{n \to \infty} P(\Sigma(\tilde{Q}) \text{ is } \beta\text{-typical}) = 1$$

uniformly.

From these two lemmas we obtain the following lemma.
Lemma 23. For every $\alpha$-typical $q \in V^n$, $\beta$-typical $r \in V^n$ and a random $(q,h)$-tuple $Q$ we have
\[ P(\Sigma(\bar{Q}) = r \text{ and } \bar{Q} \text{ is not } \gamma\text{-typical}) < \frac{C_1 \exp \left( -n^{2\gamma - 1}/C_1 + C_2 n^{2\beta - 1} \right)}{|V|^n}. \]
Here the numerator $C_1 \exp \left( -n^{2\gamma - 1}/C_1 + C_2 n^{2\beta - 1} \right)$ on the right hand side goes to 0 as $n$ goes to infinity.

Proof. For every $r' \in S(r)$ consider the event $\Sigma(\bar{Q}) = r'$ and $\bar{Q}$ is not $\gamma$-typical. These events are disjoint and by symmetry they have the same probability. Moreover, they are all contained by the event that $Q$ is not $\gamma$-typical. Thus,
\[ P(\Sigma(\bar{Q}) = r \text{ and } \bar{Q} \text{ is not } \gamma\text{-typical}) \leq \frac{P(\bar{Q} \text{ is not } \gamma\text{-typical})}{|S(r)|}. \]
The statement then follows from Lemma 20 and 21.

3.3 The proof of Theorem 9

We start by a simple lemma.

Lemma 24. For $q, r \in V^n$, and $h \geq 2$ we have $P(S_{q,h} = r) \leq |S(q)|^{-1}$

Proof. It follows from the facts that
\[ P(S_{q,h} = r \mid r - (q^{(1)} + \cdots + q^{(h-1)}) \sim q) = |S(q)|^{-1} \]
and
\[ P(S_{q,h} = r \mid r - (q^{(1)} + \cdots + q^{(h-1)}) \not\sim q) = 0. \]

Now we prove Theorem 9 from Theorem 10.

Proof. We have $P(S_{q,d} = r) = EP(S_{q,d-1} = r - q')$ where $q'$ is a uniform random permutation of $q$. There is a $c > 0$ such that $r - q'$ is not $\beta$-typical with probability at most $\exp(-cn^{2\beta - 1})$, see Section 10. Observe that $r - q' \in R(q,d-1)$ for every $q' \sim q$. Applying Theorem 10 if $r - q'$ is $\beta$-typical, then $P(S_{q,d-1} = r - q') \sim |V|^{-(n-1)}$ uniformly, otherwise $0 \leq P(S_{q,d-1} = r - q') \leq |S(q)|^{-1}$ from the previous lemma. From the law of total probability we have
\[ P(S_{q,d}) = P(S_{q,d-1} = r - q' \mid r - q' \text{ is } \beta\text{-typical}) P(r - q' \text{ is } \beta\text{-typical}) + P(S_{q,d-1} = r - q' \mid r - q' \text{ is not } \beta\text{-typical}) P(r - q' \text{ is not } \beta\text{-typical}). \]
Inserting the above inequalities into this, we obtain that
\[ (1 + o(1))|V|^{-(n-1)} \left( 1 - \exp(-cn^{2\beta - 1}) \right) \leq P(S_{q,d} = r) \leq |V|^{-(n-1)} + \frac{\exp(-cn^{2\beta - 1})}{|S(q)|}. \]
Since there is $c'$ such that $|S(q)| \geq |V|^n \exp(-c'n^{2\alpha - 1})$ for every $\alpha$-typical $q \in V^n$, we get that $\exp(-cn^{2\beta - 1})/|S(q)| = o(|V|^n)$. The theorem follows.
4 Only the typical vectors matter

The aim of this section to prove Theorem 3. Let \( \text{Cos}(V) \) 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 \( \sum_{c \in W} m_q(c) \leq f(n) \). In the previous section we used the term \( \alpha \)-typical for \((V, 0)\) typical vectors.

We start by a simple corollary of Theorem 2.

**Lemma 25.** We have

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

**Proof.** If \( W \) is a subgroup of \( V \), then from Theorem 2 we know that \( d_\infty(A_n q, U_{q,d}) = o(|W|^{-n}) \) uniformly for all \((W, 0)\)-typical \( q \). On the other hand the number of \((W, 0)\)-typical vectors are at most \(|W|^n\). Thus,

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

Consider a coset \( W \in \text{Cos}(V) \) 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

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

using the already established case. Since \( \text{Cos}(V) \) is finite the statement follows. \( \Box \)

For \( q \in V^n \) choose \( r_q \) such that \( P(A_n q = r_q) = \max_{r \in V^n} P(A_n q = r) \). For \( W \in \text{Cos}(V) \) we define \( I(W^n) = \{ q \in W^n \mid \text{MinC}_q = W \} \). Note that \( V = \bigcup_{W \in \text{Cos}(V)} I(W^n) \), where this is a disjoint union. For \( q \in I(W^n) \) we have \( d_\infty(A_n q, U_{q,d}) \leq |W|^{-(n-1)} + P(A_n q = r_q) \) from the triangle inequality. Moreover, \( \{ q \in I(W^n) \mid q \text{ is not typical} \} = o(|W|^n) \). Combining these with Lemma 25 we obtain that

\[
\limsup_{n \to \infty} \sum_{q \in V^n} d_\infty(A_n q, U_{q,d}) = \limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \in I(W^n)} d_\infty(A_n q, U_{q,d}) =
\]

\[
\limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \text{ is typical} (W, 0)} d_\infty(A_n q, U_{q,d}) + \limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \in I(W^n) \text{ is not typical} (W, 0)} d_\infty(A_n q, U_{q,d}) \leq
\]

\[
\limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \in I(W^n) \text{ is not typical} (W, 0)} (|W|^{-(n-1)} + P(A_n q = r_q)) =
\]

\[
\limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \text{ is not typical} (W, 0)} \{ q \in I(W^n) \mid q \text{ is not typical} \} |W|^{-(n-1)} +
\]

\[
\limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \text{ is not typical} (W, 0)} P(A_n q = r_q) =
\]

\[
\limsup_{n \to \infty} \sum_{W \in \text{Cos}(V)} \sum_{q \text{ is not typical} (W, 0)} P(A_n q = r_q).
\]
So in order to prove Theorem 3 it is enough to prove that

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

We establish this in three steps, namely we prove that

$$\limsup_{n \to \infty} \sum_{W \in \Cos(V)} \sum_{q \in I(W^n) \text{ is not } (W,n^n)\text{-typical}} P(A_nq = r_q) = 0,$$  \hfill (12)

$$\limsup_{n \to \infty} \sum_{W \in \Cos(V)} \sum_{q \in (W,n^n)\text{-typical,}} P(A_nq = r_q) = 0,$$  \hfill (13)

$$\limsup_{n \to \infty} \sum_{W \in \Cos(V)} \sum_{q \in (W,C \log n)\text{-typical,}} P(A_nq = r_q) = 0,$$  \hfill (14)

where \( C \) is a constant to be chosen later.

The equalities (12), (13) and (14) are proved in subsections 4.1, 4.3 and 4.4 respectively.

### 4.1 Proof of Equality (12)

Due to symmetry if \( q_1 \sim q_2 \), then \( P(A_nq_1 = r_{q_1}) = P(A_nq_2 = r_{q_2}) \). So

$$\sum_{q' \sim q} P(A_nq' = r_{q'}) = |S(q)| P(S_q = r_q) =$$

$$|S(q)| \sum_{q' \sim q} P(S_{q,d-1} = r_q - q') P(q^{(d)} = q') = \sum_{q' \sim q} P(S_{q,d-1} = r_q - q') = P(r_q - S_{q,d-1} \sim q).$$

Let \( T_n \subset V^n \) be such that it contains exactly one element of each equivalence class. Then

$$\sum_{W \in \Cos(V)} \sum_{q \in I(W^n) \text{ is not } (W,n^n)\text{-typical}} P(A_nq = r_q) = \sum_{W \in \Cos(V)} \sum_{q \in I(W^n) \cap T_n \text{ is not } (W,n^n)\text{-typical}} P(r_q - S_{q,d-1} \sim q)$$

Note that \( |T_n| \leq n^L \) for a sufficiently large \( L \), therefore

$$\sum_{P(S_{q,d-1} \sim -q) < n^{-(L+1)}} P(S_{q,d-1} \sim -q) \leq |T_n| n^{-(L+1)} = o(1).$$

This means that to establish Equality (12) it is enough to show that for a large enough \( n \) if \( P(S_{q,d-1} \sim -q) \geq n^{-(L+1)} \) then \( q \) is \((W,n^n)\)-typical for some coset \( W \in \Cos(V) \).

The following terminology will be useful for us. With every \((q,d-1)\)-tuple \( Q = (Q_1, Q_2, \ldots, Q_n) \) we associate the random variables \( Z \in V \) and \( X^Q = (X_1^Q, X_2^Q, \ldots, X_{d-1}^Q) \in V^{d-1} \), such that \( Z = r_q(i) \) and \( X^Q = Q_i \), where \( i \) is a uniform random element of the set \( \{1,2,\ldots,n\} \). Note that the joint distribution of \( Z \) and \( X^Q \) is well defined because we use the same random \( i \) in their definition. Each \( X_j^Q \) has the same distribution as \( q_i \) where \( i \) is chosen uniformly from \( \{1,2,\ldots,n\} \). The random variable \( X_{q,d-1}^Q \in V \) is defined as \( X_{q,d-1}^Q = \sum_{i=1}^{d-1} X_i^Q \). With this terminology the event \( r_q - \Sigma(Q) \sim q \) is the same as \( Z - X_{q,d-1}^Q \sim X_1^Q \). Here \( \sim \) means that the two random variables have the same distribution. Thus, \( P(r_q - S_{q,d-1} \sim q) = P(Z - X_{q,d-1}^Q \sim X_1^Q) \). We call
the random variables \( Z, X_1, X_2, \ldots, X_{d-1} \in V \) \( \varepsilon \)-independent if for every \( z, x_1, x_2, \ldots, x_{d-1} \in V \) we have

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

Fix \( \frac{1}{2} < \eta < \alpha \). Then we have the following lemma. See Section [10] for the proof.

**Lemma 26.** For large enough \( n \) we have that for any \( q \in V^n \)

\[
P(Z, X_1^q, X_2^q, \ldots, X_{d-1}^q) \text{ are not } n^{n-1} \text{-independent} < n^{-(L+1)}.
\]

Therefore for large enough \( n \), if \( P(r_q - S_{q,d-1} \sim q) = P(Z - X_\Sigma^q \sim X_1^q) \geq n^{-(L+1)} \), we have

\[
P(Z, X_1^q, X_2^q, \ldots, X_{d-1}^q) \text{ are } n^{n-1} \text{-independent and } Z - X_\Sigma^q \sim X_1^q > 0,
\]

so there exist \( n^{n-1} \) independent random variables \( Z, X_1, X_2, \ldots, X_{d-1} \) 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 \( \{1, 2, \ldots, n\} \).

Now the following lemma gives us equality [12]

**Lemma 27.** 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 \( Z, X_1, X_2, \ldots, X_{d-1} \) are \( \varepsilon \)-independent \( V \)-valued random variables, for some \( 0 < \varepsilon < \varepsilon_0 \). Let \( X_\Sigma = X_1 + X_2 + \cdots + X_{d-1} \). Assume that \( X_1, X_2, \ldots, X_{d-1} \) and \( Z - X_\Sigma \) have the same distribution \( \pi \). Then there is a coset \( W \) in \( V \) such that \( d_{\infty}(\pi, \pi_W) < C\varepsilon \).

Here \( \pi_W \) is the uniform distribution on \( W \). For two distribution \( \pi \) and \( \mu \) on the same finite set \( \mathcal{R} \) their distance \( d_{\infty}(\pi, \mu) \) is defined as \( d_{\infty}(\pi, \mu) = \max_{r \in \mathcal{R}} |\pi(r) - \mu(r)| \).

The next subsection is devoted to the proof of this lemma.

### 4.2 The proof of Lemma [27]

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 28.** Let \( Z, X_1, X_2, \ldots, X_{d-1} \) 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 \( \pi \). Then \( \pi = \pi_W \) for some coset \( W \) in \( V \).

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

\[
\hat{\pi}(\varrho) = \sum_{v \in V} \pi(v) \varrho(v).
\]

and

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

The assumptions of the lemma imply that

\[
\hat{\mu}(\varrho) \left( \frac{1}{\hat{\pi}(\varrho)} \right)^{d-1} = \hat{\pi}(\varrho)
\]

for every \( \varrho \in \hat{V} \). In particular \( |\hat{\mu}(\varrho)|, |\hat{\pi}(\varrho)|^{d-1} = |\hat{\pi}(\varrho)| \) 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 \( \varrho \in V \). Let us define \( \hat{V}_1 = \{ \varrho \in V \mid |\hat{\pi}(\varrho)| = 1 \} \).

Note that \( \hat{V}_1 \) always contains the trivial character. Then for every \( \varrho \in \hat{V}_1 \) the character \( \varrho \) is
constant on the support of \( \pi \), or in other words the support of \( \pi \) is contained in \( W_\varepsilon = g^{-1}(\hat{\pi}(g)) \), which is a coset of \( \ker g \). Therefore the support of \( \pi \) is contained in the coset \( W = \bigcap_{g \in \tilde{V}_1} W_\varepsilon \).

Now we prove that \( \hat{\pi}(g) = \hat{\pi}_W(g) \) for every \( g \in \tilde{V} \), which implies that \( \pi = \pi_W \). This is clear for \( g \in \tilde{V}_1 \), so assume that \( g \not\in \tilde{V}_1 \), that is, \( \hat{\pi}(g) = 0 \). This implies that \( g \) is not constant on \( W \). So there is \( w_1, w_2 \in W \) such that \( \varrho(w_1) \neq \varrho(w_2) \). For \( w = w_1 - w_2 \) we have \( \varrho(w) \neq 1 \) and \( W = wW \). Thus

\[
\hat{\pi}_W(g) = \frac{1}{|W|} \sum_{v \in W} \varrho(v) = \frac{1}{|W|} \sum_{v \in W} \varrho(wv) = \frac{1}{|W|} \varrho(w) \sum_{v \in W} \varrho(v) = \varrho(w) \hat{\pi}_W(g).
\]

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

Now we turn to the proof of Lemma \( \ref{lemma28} \).

**Proof.** Using the notations of the proof of Lemma \( \ref{lemma28} \), the conditions of the lemma imply that

\[
\left| \hat{\pi}(g) - \hat{\mu}(g) \left( \frac{1}{|W|} \sum_{v \in W} \varrho(v) \right)^{d-1} \right| \leq |V|^{d \varepsilon}
\]

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

\[
\left| \hat{\pi}(g) - \hat{\mu}(g) \left( \frac{1}{|W|} \sum_{v \in W} \varrho(v) \right)^{d-1} \right| \geq |\hat{\pi}(g)| - |\hat{\mu}(g)| \cdot |\hat{\pi}(g)|^{d-1} \geq |\hat{\pi}(g)| - |\hat{\pi}(g)|^{d-1},
\]

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

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. If for \( x \in [0, 1] \) we have \( x - x^{d-1} \leq |V|^{d \varepsilon} \), then either \( x \leq C_1 \varepsilon \) or \( x > 1 - C_1 \varepsilon \). In the rest of the proof we assume that \( \varepsilon < \varepsilon_1 \). Then for every \( g \in \tilde{V} \) we have either \( |\hat{\pi}(g)| < C_1 \varepsilon \) or \( |\hat{\pi}(g)| > 1 - C_1 \varepsilon \).

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

\[
z = \frac{\pi(g)}{|\hat{\pi}(g)|}.
\]

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

\[
|\hat{\pi}(g)| = z \hat{\pi}(g) = \Re z \hat{\pi}(g) = \sum_{\xi \in R(g)} \pi(g^{-1}(\xi)) \Re z \xi \leq 1 - (1 - \pi(g^{-1}(\xi_0))) \delta.
\]

Thus, \( |\hat{\pi}(g)| > 1 - C_1 \varepsilon \) implies that for the coset \( W_\varepsilon = g^{-1}(\xi_0) \) we have \( \pi(W_\varepsilon) > 1 - C_1 \delta^{-1} \varepsilon \).

So the coset \( W = \bigcap_{g \in \tilde{V}_1} W_\varepsilon \) satisfies \( \pi(W) > 1 - C_1 \delta^{-1} |V| \varepsilon \). For any \( g \in \tilde{V}_1 \) we have

\[
|\hat{\pi}(g) - \hat{\pi}_W(g)| \leq 2(1 - \pi(W_\varepsilon)) \leq 2C_1 \delta^{-1} \varepsilon.
\]

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

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

provided that \( \varepsilon_0 \) is small enough, which gives us a contradiction. So the argument in the proof of Lemma \( \ref{lemma28} \) gives us \( \hat{\pi}_W(g) = 0 \). Thus

\[
|\hat{\pi}(g) - \hat{\pi}_W(g)| = |\hat{\pi}(g)| \leq C_1 \varepsilon.
\]

This gives us \( |\hat{\pi}(g) - \hat{\pi}_W(g)| \leq 2C_1 \delta^{-1} \varepsilon \) for any \( g \in \tilde{V} \). The map \( \pi \mapsto \hat{\pi} \) is an invertible linear map, so there is an \( L = L_V \) such that \( d_\infty(\pi, \pi_W) \leq L \max_{\varepsilon \in V} |\hat{\pi}(g) - \hat{\pi}_W(g)| \). This gives the statement. \qed
4.3 Proof of Equality \[13\]

Recall that in subsection \[4.1\] we have chosen an \(L\), such that \(|T_n| \leq n^L\). The same argument that was given there shows that to establish Equality \[13\] it is enough to prove the following lemma.

**Lemma 29.** There is a \(C\) such that if \(W \in \text{Cos}(V)\) and \(q \in V^n\) is \((W,n^\alpha)\)-typical, but not \((W,C \log n)\)-typical, then for a random \((q,d-1)\)-tuple \(Q\) we have \(P(r_q - \Sigma(Q) \sim q) \leq n^{-(L+1)}\).

**Proof.** Let \(E = \sum_{c \notin W} m_q(c)\). Since \(q\) is \((W,n^\alpha)\)-typical we have \(E \leq n^\alpha\). Assume that \(r = \sum_{i=1}^d q^{(i)}\), where \(q^{(i)} \sim q\). Note that \(\{j | r_j \notin \text{dW}\} \subseteq \cup_{i=1}^d \{j | q^{(i)}(j) \notin W\}\), so \(\sum_{c \notin \text{dW}} m_r(c) \leq dE\). In particular this is true for \(r_q\), that is \(\sum_{c \notin \text{dW}} m_r(c) \leq dE\).

Let \(H_0 = \{j | r_q(j) \notin \text{dW}\}\). For \(i = 1,2,...,d-1\) we define the random subset \(H_i\) of \(\{1,2,...,n\}\) using the random \((q,d-1)\)-tuple \(Q = (\bar{q}^{(1)}, \bar{q}^{(2)}, \ldots, \bar{q}^{(d-1)})\) as \(H_i = \{j | q^{(i)}(j) \notin W\}\), and let the random subset \(H^* \subset \{1,2,...,n\}\) be defined as \(H^* = \{j | r_q(j) - \Sigma(Q)(j) \notin W\}\). Then \(0 \leq |H_0| \leq dE\) and \(|H_1| = |H_2| = \ldots = |H_{d-1}| = E\). Let \(B\) be the set of such \(j\)'s, which are contained in exactly one of the sets \(H_0, H_1, H_2, ..., H_{d-1}\). Then \(B \subset H^*\), therefore we have

\(P(r_q - \Sigma(Q) \sim q) \leq P(|H^*| = E) \leq P(|B| \leq E)\).

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. 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,

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

The following lemma finishes the proof. (See Section \[10\] for its proof.)

**Lemma 30.** 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 \(\{n\} = \{1,2,...,n\}\) of size \(a\) and \(b\) respectively chosen independently and uniformly, then

\[P\left(|A \cap B| \geq \frac{(d - 2)E}{d(d-1)}\right) < n^{-(L+1)} / \binom{d}{2}\] \(\square\)

4.4 Proof of Equality \[14\]

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

\[\lim_{n \to \infty} \sum_{q \in D^*_W} |S(q)|P(\Sigma(Q) = r_q) = 0,\]

where \(D^*_W = \{q \in T_n | q\) is \((W,C \log n)\)-typical, but not \((W,0)\)-typical\} and \(\bar{Q}\) is a random \((q,d)\)-tuple. (Recall that \(S(q)\) is the set of permutations of \(q\).)

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

\[\frac{1 + m_{S(Q)}(u)}{1 + m_Q(u)} \leq \log^2 n,\]

19
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

\[
\frac{1 + m(t_\Sigma = u_\Sigma)}{1 + m(u)} \leq \log^4 n,
\]

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

**Lemma 31.** For any coset \( W \in \text{Cos}(V) \) we have

\[
\limsup_{n \to \infty} \sum_{q \in D_n^W} |S(q)| P(\Sigma(\bar{Q}) = r_q) = \limsup_{n \to \infty} \sum_{q \in D_n^W} |S(q)| P(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is } W \text{ decent}).
\]

**Proof.** The same argument as in the beginning of Subsection 4.1 show that it is enough to show that \( |S(q)| P(\Sigma(\bar{Q}) = r_q \text{ and } \bar{Q} \text{ is not } W \text{ decent}) < n^{-(L+1)} \) for every \((W, C \log n)\)-typical vector \( q \in V^n \) if \( n \) is large enough. 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 \( d - 1 \) tuple \( Q^{d-1} = (q^{(1)}, q^{(2)}, \ldots, q^{(d-1)}) \) such that \( r - \Sigma(Q^{d-1}) \sim q \), the tuple \( (q^{(1)}, q^{(2)}, \ldots, q^{(d-1)}, r_q - \Sigma(Q^{d-1})) \) will be a \((q, d)\)-tuple and it is denoted by \( \text{Ext}(Q^{d-1}) \). It is also clear that \( \Sigma(\text{Ext}(Q^{d-1})) = r_q \), 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 \( Q^d = \text{Ext}(Q^{d-1}) \). Also note that \( P(\bar{Q}^{d-1} = Q^{d-1}) = |S(q)| P(\bar{Q}^d = Q^d) \). Moreover \( \text{Ext}(Q^{d-1}) \) is \( W \)-decent, if \( Q_{d-1} \) satisfies the property that

for any \( t \in W^{d-1} \) and \( c \in dW \) we have

\[
\frac{1 + m_{r_q}(c)}{1 + |\{i \in [k] \ | \ r_q(i) = c \text{ and } Q^{d-1}(i) = t\}|} \leq \log^2 n. \tag{15}
\]

A random \((q, d - 1)\)-tuple will satisfy the property above with probability at least \( 1 - n^{-(L+1)} \) for every \((W, C \log n)\)-typical vector \( q \in V^n \) if \( n \) is large enough. Indeed, if \( m_{r_q}(c) < \log^2 n \) this is clear. Otherwise, with high probability

\[
|\{i \ | \ r_q(i) = c \text{ and } Q^{d-1}(i) = t\}| > \frac{1}{2} m_{r_q}(c)
\]

for any \( t \in W^{d-1} \), as it follows from Lemma 70 of Section 10. \( \square \)

As before we define

\[
\mathcal{M}(q, r) = \{m_Q \ | \ Q \in Q_{d, d}, \Sigma(Q) = r\}.
\]

Now let

\[
\mathcal{M}^d(q, r) = \{m \in \mathcal{M}(q, r) \ | \ m \text{ is } W \text{ decent}\}
\]

From the previous lemma we need to prove that

\[
\lim_{n \to \infty} \sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^d(q, r_q)} |S(q)| P((\Sigma(\bar{Q}) = r_q) \land (m_{\bar{Q}} = m)) = 0.
\]

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

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

\[
m(t_i = c) = m(t_1 = c)
\]

20
for every \( c \in V \) and \( i = 1, 2, \ldots, d \).

In other words, \( \mathcal{M} \) consists of the integer points of a rational polyhedral cone. From [18, Theorem 16.4] we know that this cone is generated by an integral Hilbert basis, i.e. we have the following lemma.

**Lemma 32.** There are finitely many vectors \( m_1, m_2, \ldots, m_\ell \in \mathcal{M} \), such that

\[
\mathcal{M} = \{ c_1 m_1 + c_2 m_2 + \cdots + c_\ell m_\ell \mid c_1, c_2, \ldots, c_\ell \text{ are non-negative integers} \}.
\]

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 \( m_{h+1}, m_{h+2}, \ldots, m_\ell \) are not contained in \( W^d \).

**Definition 33.** Given a vector \( m \in \mathcal{M} \) write \( m = \sum_{i=1}^{\ell} c_i m_i \), where \( c_1, c_2, \ldots, c_\ell \) 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 \( \|m\|_{WC} = m(t \not\in W^d) \), we have \( \|m\|_{WC} = \|\Delta(m)\|_{WC} \) and \( \|m - \Delta(m)\|_{WC} = 0 \).

For any non-negative integral vector \( m \in \mathbb{R}^d \) we define

\[
E(m) = \frac{\prod_{t \in V} m(t) = c!}{\prod_{t \in V^d} m(t)!} \left( \prod_{i=1}^{d} \frac{\prod_{t \in V} m(t_i = c)!}{m(V^d)!} \right)^{d-1}
\]

then for every \( q, r \in V^n \) and \( m \in \mathcal{M}(q, r) \) we have

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

Here in the last equality we used the fact that \( m \in \mathcal{M}(q, r) \). Of course there are many other equivalent ways to express this probability and each of them suggests a way to extend the formula to all non-negative integral vectors, but the formula given in line (16) will be useful for us later.

**Lemma 34.** Consider a non-negative integral half-decent vector \( m_0 \in \mathbb{R}^V \), such that \( \|m_0\|_{WC} = O(\log n) \), where \( n = \sum_{t \in V} m(t) \). For \( u \in V^d \) let \( \chi_u \in \mathbb{R}^V \) 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 \( u \not\in W^d \) then

\[
E(m_0 + \chi_u)/E(m_0) = O(n^{-(d-2)/d} \log^2 n).
\]

There is a \( D \), such that for any \( i \in \{ h + 1, h + 2, \ldots, \ell \} \) we have

\[
E(m_0 + m_i)/E(m_0) = O \left( \left( n^{-(d-2)/d} \log^D n \right)^{\|m_i\|_{WC}} \right).
\]

**Proof.** Let \( g = \frac{1 + m_0(t \not\in u)}{1 + m_0(u)} \) and \( f_i = \frac{1 + m_0(t_i = u)}{n+1} \).

Note that

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

If \( u \in W^d \), then since \( W \)-half-decent we have \( g \leq \log^4 n \), and clearly \( f_i \leq 1 \), so the statement follows.
If \( u \not\in W^d \), we consider the following two cases, if \( u_\Sigma \not\in dW \), then \( m_0(t_\Sigma = u_\Sigma) \leq \|m_0\|_{W^c} = O(\log n) \), and there is an \( i \) such that \( u_i \not\in W \), this imply that \( f_i = O(\log n) \) so \( E(m_0 + \chi_u)/E(m_0) = O\left(\frac{\log^2 n}{n}\right) \). If \( u_\Sigma \in W^d \), there are at least two indices \( i \) such that \( u_i \not\in W \), for such an index \( i \) we have \( f_i = O(\log n) \), clearly \( g = O(n) \), so \( E(m_0 + \chi_u)/E(m_0) = O\left(n\left(\frac{\log n}{n}\right)^{2(d-1)/d}\right) = O(n^{-\frac{d-2}{d}} \log^2 n) \).

The last statement of the lemma follows from the previous ones.

The following estimate will be crucial later.

**Lemma 35.** There is a \( K \) such that for any \((W,C \log n)\)-typical \( q \in V^n \) and \( m \in \mathcal{M}^2(q, r_q) \) we have

\[
E(m) \leq \left(Kn^{-(d-2)/d} \log^D n\right)\|\Delta(m)\|_{W^c} E(m - \Delta(m)).
\]

**Proof.** This follows from repeated application of the previous lemma and the observation that \( m - \Delta(m) \) and all other \( m_0 \) we need to apply that lemma is \( W \)-half-decent.

Now we made all the necessary preparation to prove Equality \(^{14}\) With our new notations we have to prove that

\[
\lim_{n \to \infty} \sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^2(q, r_q)} E(m) = 0.
\]

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 \(|W| < |V|\), then from the induction hypothesis we can use Theorem \(^3\) to get that that

\[
\sum_{q \in W^n \cap T_n} |S(q)|P(S_{q,d} = r_q) = \sum_{q \in W^n} P(S_{q,d} = r_q) = \sum_{q \in W^n} P(U_{q,d} = r_q) + o(1) = \sum_{K \in \operatorname{Cos}(W)} |K| + o(1),
\]

in particular there is a finite \( B \) such that for every \( n \) we have that \( \sum_{q \in W^n \cap T_n} |S(q)|P(S_{q,d} = r_q) < B \). This is clear if the coset \( W \) is a subgroup, if the coset \( W \) is not a subgroup we need to use the bijection given in the proof of Lemma \(^{25}\).

We need a few notations

\[
\mathcal{M}_n^\Delta = \bigcup_{q \in D_n^W} \{\Delta(m) \mid m \in \mathcal{M}^2(q, r_q)\}.
\]

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

\[
\Delta_n^{-1}(m_\Delta) = \bigcup_{q \in D_n^W} \{m \in \mathcal{M}^2(q, r_q) \mid \Delta(m) = m_\Delta\}.
\]

Using Lemma \(^{35}\) we obtain that

\[
\sum_{q \in D_n^W} \sum_{m \in \mathcal{M}^2(q, r_q)} E(m) = \sum_{m_\Delta \in \mathcal{M}_n^\Delta} \sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m) \leq \sum_{m_\Delta \in \mathcal{M}_n^\Delta} \left(\frac{K n^{-(d-2)/d} \log^D n}{\|m_\Delta\|_{W^c}}\right) \sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta). \quad (17)
\]

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 \( \mathcal{M}^2(q, r_q) \cap \Delta_n^{-1}(m_\Delta) \) 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 $m_{q'}(c) = m_q(c) - m_\Delta(t_1 = c)$ and a unique $w_q \in W^\prime \cap T'$ such that for every $c \in V$ we have $m_{w_q}(c) = m_{r_q}(c) - m_\Delta(t_\Sigma = c)$. Note that for any $m \in M^\Delta(q, r_q) \cap \Delta_n^{-1}(m_\Delta)$ we have $m - m_\Delta \in M(q', w_q)$. Moreover $E(m - m_\Delta) = |S(q')||P(\Sigma(Q) = w_q) \land (m_Q = m - m_\Delta))$, where $\tilde{Q}$ is a random $(q', d)$-tuple. So it follows that $\sum_{m \in M^\Delta(q, r_q) \cap \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) \leq |S(q')|P(S_{q', d} = w_q)$. Also note that the maps $q \mapsto q'$ and $m \mapsto m - m_\Delta$ are injective. Therefore

$$\sum_{m \in \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) = \sum_{q \in X} \sum_{m \in M(q, r_q) \cap \Delta_n^{-1}(m_\Delta)} E(m - m_\Delta) \leq
\sum_{q \in X} |S(q')|P(S_{q', d} = w_q) \leq \sum_{q' \in W^\prime \cap T'} |S(q')|P(S_{q', d} = r_q) < B$$

Thus continuing line (17)

$$\sum_{q \in D^\prime} \sum_{m \in M(q, r_q)} E(m) \leq B \sum_{m_\Delta \in M^\Delta_n} \left(K_n^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{w^C}}.$$

There is an $F$ such that $|M^\Delta_n| \leq n^F$, choose a constant $G$ such that for large enough $n$ we have $(K_n^{-(d-2)/d} \log^{d-1} n)^{\|m_\Delta\|_{w_C}} < n^{-(F+1)}$, whenever $\|m_\Delta\|_{w_C} \geq G$. Let

$$H = |\{m \mid m = \sum_{i=h+1}^\ell c_i m_i, \quad c_{h+1}, c_{h+2}, \ldots, c_\ell \text{ non-negative integers, } \|m\|_{w^*} < G\}| \leq G^{\ell-h},$$

finally observe that $\|m_\Delta\|_{w_C} \geq 1$ for all $m_\Delta \in M^\Delta_n$. So for large enough $n$

$$B \sum_{m_\Delta \in M^\Delta_n} \left(K_n^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{w_C}} =
B \sum_{m_\Delta \in M^\Delta_n} \left(K_n^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{w_C}} + B \sum_{m_\Delta \in M^\Delta_n \mid \|m_\Delta\|_{w_C} < G} \left(K_n^{-(d-2)/d} \log^D n\right)^{\|m_\Delta\|_{w_C}} \leq
Bn^F n^{-(F+1)} + BHK_n^{-(d-2)/d} \log^D n = o(1)$$

Thus we have proved Equality (14).

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

The random $(n-1) \times (n-1)$ matrix $A'_q$ is obtained from $A_n$ by deleting its last row and last column. For $q \in V^{n-1}$ the subgroup generated by $q_1, q_2, \ldots, q_{n-1}$ is denoted by $G_q$. Let $U_q$ be a uniform random element of $G_q^{-1}$. The next corollary of Theorem 3 states that the distribution of $A'_q q$ is close to that of $U_q$.

**Corollary 36.** We have

$$\lim_{n \to \infty} \sum_{q \in V^{n-1}} d_{\infty}(A'_q q, U_q) = 0.$$
Proof. For \( q \in V^{n-1} \) and \( r \in G_{q}^{n-1} \) we define \( \bar{q} = (q_{1}, q_{2}, \ldots, q_{n-1}, 0) \in V^{n} \) and \( \bar{r} = (r_{1}, r_{2}, \ldots, r_{n-1}, d \cdot s(q) - s(r)) \in G_{q}^{n} \).

Note that \( s(\bar{r}) = d \cdot s(q) = d \cdot s(\bar{q}) \) and \( \text{MinC}_{\bar{q}} = G_{q} \), so \( \bar{r} \in R(\bar{q}, d) \). Moreover, \( A'_{n} q = r \) if and only if \( A_{n} \bar{q} = \bar{r} \), so \( P(A'_{n} q = r) = P(A_{n} \bar{q} = \bar{r}) \). 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 is straightforward.

Recall that the reduced Laplacian \( \Delta_{n} \) of \( D_{n} \) was defined as \( \Delta_{n} = A'_{n} - dI \). The next well-known proposition connects \( \text{Hom}(\Gamma_{n}, V) \) and \( \text{Sur}(\Gamma_{n}, V) \) with the kernel of \( \Delta_{n} \) when \( \Delta_{n} \) acts on \( V^{n-1} \).

**Proposition 37.** For any finite abelian group \( V \) we have

\[
|\text{Hom}(\Gamma_{n}, V)| = |\{ q \in V^{n-1} \mid \Delta_{n} q = 0 \}|
\]

and

\[
|\text{Sur}(\Gamma_{n}, V)| = |\{ q \in V^{n-1} \mid \Delta_{n} q = 0, \ G_{q} = V \}|
\]

Proof. There is an obvious bijection between \( \text{Hom}(S_{n}, V) \) and

\[
\{ \varphi \in \text{Hom}(Z^{n-1}, V) \mid \text{RowSpace}(\Delta_{n}) \subset \ker \varphi \}.
\]

Moreover, any \( \varphi \in \text{Hom}(Z^{n-1}, V) \) is uniquely determined by the vector \( q = (\varphi(e_{1}), \varphi(e_{2}), \ldots, \varphi(e_{n-1})) \in V^{n-1} \), where \( e_{1}, e_{2}, \ldots, e_{n-1} \) is the standard generating set of \( Z^{n-1} \). Furthermore, \( \text{RowSpace}(\Delta_{n}) \subset \ker \varphi \) if and only if \( \Delta_{n} q = 0 \), so the first statement follows. The second one can be proved similarly. \( \square \)

Combining Proposition 37 with with Corollary 36 we obtain

\[
\lim_{n \to \infty} \mathbb{E}|\text{Sur}(\Gamma_{n}, V)| = \lim_{n \to \infty} \sum_{q \in V^{n-1}} P(\Delta_{n} q = 0) = \lim_{n \to \infty} \sum_{q \in V^{n-1}} P(A'_{n} q = dq) = \lim_{n \to \infty} \sum_{q \in V^{n-1}} P(U_{q} = dq) = \lim_{n \to \infty} |\{ q \in V^{n-1} \mid G_{q} = V \}| \cdot |V|^{-(n-1)} = 1
\]

This proves the first statement Theorem 12.

This implies that the distribution of \( \Gamma_{n} \) follows the Cohen-Lenstra heuristic. See [21][Theorem 3.1 and Lemma 3.2.] or [20][Theorem 8.3]. Thus we obtained the first statement of Theorem 11. The proofs of the corresponding statements about the sandpile group of \( H_{n} \) are postponed to Section 4 and 8.

### 6 Uniform convergence in \( d \)

We state our results for the directed random graph model, but the arguments can be repeated for the other 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 38.** 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 random uniform element of \( S(q) \), then

\[
|P(A_n^{(d)} q = r) - P(U_{q,d} = r)| = |\mathbb{E}P(A_n^{(d-1)} q = r - q') - |U_{q,d-1}|^{-1}| \leq \mathbb{E}|P(A_n^{(d-1)} q = r - q') - |U_{q,d-1}|^{-1}| \leq d_{\infty}(A_n^{(d-1)} q, U_{q,d-1}),
\]

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 3.

Corollary 39. We have

\[
\limsup_{n \to \infty} \sup_{d \geq 3} \sum_{q,d} d_{\infty}(A_n^{(d)} q, U_{q,d}) = 0.
\]

This also implies a uniform version of Corollary 36. Therefore the limits in Theorem 2 are uniform in \( d \). Consequently, Theorem 1 remains true if we allow \( d \) to vary with \( n \).

7 Sum of m-matrices: Modifications of the proofs

A fixed point free permutation of order 2 is called a matching permutation, which we abbreviate as m-permutation. The permutation matrix of an m-permutation is called m-matrix. Then \( C_n = M_1 + M_2 + \cdots + M_d \), where \( M_1, M_2, \ldots, M_d \) are independent uniform random \( n \times n \) m-matrices.

Consider a vector \( q = (q_1, q_2, \ldots, q_n) \in V^n \). For an m-permutation \( \pi \) of the set \([n] = \{1, 2, \ldots, n\}\) the vector \( q_{\pi} = (q_{\pi(1)}, q_{\pi(2)}, \ldots, q_{\pi(n)})\) is called an m-permutation of \( q \). A random m-permutation of \( q \) is defined as the random variable \( \xi_q \), where \( \pi \) is chosen uniformly from the set of all m-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 m-permutations of \( q \). A random \((q, 1, h)\)-tuple is \( Q = (q^{(0)}, q^{(1)}, \ldots, q^{(h)})\), where \( q^{(0)}, q^{(2)}, \ldots, q^{(h)} \) are independent random m-permutations of \( q \). Similarly 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

\[
m_Q(t) = |\{i \mid Q_i = t\}|.
\]

In this section the components of a vector \( t \in V^{1+h} \) are indexed from 0 to \( h \), i.e. \( t = (t_0, t_1, \ldots, t_h) \). For \( t \in V^{1+h} \) we define \( t_{\Sigma} = \sum_{i=1}^h t_i \). 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

\[
\mathcal{M}^\Sigma(q, r) = \{m_Q \mid Q \text{ is a } (q, 1, h)\text{-tuple such that } \Sigma(Q) = r\}.
\]

A \((q, 1, h)\)-tuple \( Q \) is \( \gamma \)-typical if \( \|m_Q - \frac{n}{V^2} \mathbf{1}\|_{\infty} < n^\gamma \).

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

\[
m_{q,r}(a, b) = |\{i \mid q_i = a \text{ and } r_i = b\}|,
\]

so \( m_{q,r} \) can be considered as a vector in \( \mathbb{R}^{V^2} \). The vector \( r \) is called \((q, \beta)\)-typical if

\[
\|m_{q,r} - \frac{n}{V^2} \mathbf{1}\|_{\infty} < n^\beta.
\]

With these notations we have the following analogue of Theorem 10.
Theorem 40. Fix $\frac{1}{2} < \alpha < \beta < \frac{2}{3}$ and $h \geq 2$, then we have

$$\lim_{n \to \infty} \sup_{q \in V^n, r \in R^S(q,h)} \left| P(S_{q,h} = r) / \left( \frac{2^{\text{rank}_2(V)}}{|V|^{n-1}} \right) - 1 \right| = 0.$$  

Proof. The proof is analogous with the proof of Theorem [10]. We need to replace the notion of $(q,h)$-tuple with the notion of $(q,1,h)$-tuple, the notion of $\beta$-typical vector with the notion of $(q,\beta)$ 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 41. Let $q \in V^n$ such that $\text{MinC}_q = V$, then

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

Proof. We define the homomorphism $\varphi : V^n \to (V \otimes V) \times V$ by $\varphi(r) = (q \otimes r, s(q))$ for every $r \in V^n$. We claim that it is surjective. First, take any $a, b \in V$. The condition $\text{MinC}_q = V$ implies that $q_1 - q_n, q_2 - q_n, \ldots, q_{n-1} - q_n$ generate $V$. In particular, there are integers $c_1, c_2, \ldots, c_{n-1}$ such that $a = \sum_{i=1}^{n-1} c_i(q_i - q_n)$. Let us define $r = (c_1 b, c_2 b, \ldots, c_{n-1} b, -\sum_{i=1}^{n-1} c_i b) \in V^n$. Then

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

and $s(r) = 0$, that is, $\varphi(r) = (a \otimes b, 0)$. Thus, $V \otimes V \times \{0\}$ is contained in the range of $\varphi$. Clearly, for any $v \in V$ we can choose $r$ such that $s(r) = v$. This implies that $\varphi$ is indeed surjective. Since $R^S(q,h) = \varphi^{-1}(I_2 \times \{h \cdot s(q)\})$, we have

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

Lemma 42. Consider $q, r \in V^n$. Let $m \in M^S(q,r)$. Then $m$ is a nonnegative integral vector with the following properties.

For $c \in V$

$$m(t_0 = c) = m_q(c), \quad (18)$$

for $i = 1, 2, \ldots, h$ and $a, b \in V$

$$m(t_0 = a \text{ and } t_i = b) = m(t_0 = b \text{ and } t_i = a), \quad (19)$$

and for $a, b \in V$

$$m(t_0 = a \text{ and } t = b) = m_{q,r}(a,b). \quad (20)$$

Moreover, for $i = 1, 2, \ldots, h$ and $c \in V$.

$$m(t_0 = c \text{ and } t_i = c) \text{ is even.} \quad (21)$$

Now assume that $m$ is a nonnegative integral vector satisfying the conditions above. Then
\[ P(\Sigma(Q) = r \text{ and } m_Q = m) = \]
\[ \left( \frac{n!}{2^{n/2} (n/2)!} \right)^{-h} \prod_{a,b \in V} m(t_0 = a, t_\Sigma = b)! \prod_{t \in V^{1+h}} m(t)! \]
\[ \prod_{i=1}^{h} \left( \prod_{a \in V} \frac{m(t_i = a, t_0 = a)!}{\sqrt{2^{m(t_i = a, t_0 = a)/2} (m(t_i = a, t_0 = a)/2)!}} \right) \left( \prod_{a \neq b \in V} \sqrt{m(t_0 = a, t_i = b)!} \right). \] (22)

In particular, \( P((\Sigma(Q) = r_1) \wedge (m_Q = m)) > 0 \) so \( m \in M^S(q, r) \). Let \( A^S(q, r) \) be the affine subspace given by the linear equations (18), (19) and (21) above. Then \( M^S(q, r) \) is the set of non-negative integral points of the affine subspace \( A^S(q, r) \) satisfying the parity constraints in (21) above.

**Lemma 43.** For any \( q, r_1, r_2 \in V^n \) we define the vector \( v = v_{q, r_1, r_2} \) 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 44.** Assume that \( n \) is large enough. For an \( \alpha \)-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 (21) of Lemma 43.

To prove this 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 45.** 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
\[ \sum_{k=1}^{n} q_k(i) r_k(j) \equiv \sum_{k=1}^{n} q_k(j) r_k(i) \pmod{o_i} \] (23)
and whenever \( o_i \) is even we have
\[ \sum_{k=1}^{n} q_k(i) r_k(i) \text{ is even.} \] (24)

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

27
Now assume that
\[ a \]

Let
\[ \text{Lemma 46.} \]

Now we modify
\[ \text{Clearly } \]
\[ z \]

there is an
\[ m \]

and
\[ \sum \]

\[ o \]

even using the condition (24) above. If
\[ 1 \]

\[ a \]

direction. Since
\[ \text{Proof.} \]

It is clear that the conditions are indeed necessary, so we only need to prove the other
\[ \text{follows that there is a symmetric matrix } \]
\[ A \]

entries of
\[ A \]

Since
\[ is even for every \]
\[ a, b \]

\[ w = Aq. \]

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
\[ w_i = \sum_{h=1}^{\ell} \sum_{j=1}^{n} a_{ij}q_j(h)v_h = \sum_{h=1}^{\ell} \left( a_{ih}v_h + \sum_{j=\ell+1}^{n} r_j(i)q_j(h)v_h \right) = \]

\[ \sum_{h=1}^{\ell} \left( r_i(h) + r_h(i) - \sum_{k=1}^{n} q_k(h)r_k(i) + \sum_{j=\ell+1}^{n} r_j(i)q_j(h) \right) v_h = \]

\[ \sum_{h=1}^{\ell} \left( r_i(h) + r_h(i) - \sum_{k=1}^{n} q_k(h)r_k(i) \right) v_h = \sum_{h=1}^{\ell} r_i(h)v_h = r_i. \]

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
\[ a_i \]

is even, then
\[ a_{ii} = 2r_i(i) - \sum_{k=1}^{n} q_k(i)r_k(i), \]

which is even using the condition (24) above. If
\[ 1 \leq i \leq \ell, \]

\[ a_i \]

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
\[ o_iq_i = o_i v_i = 0. \]

For
\[ c \in V \]

we define
\[ z_{q,w}(c) = \sum_{1 \leq i \leq n} w_i. \]

Clearly,
\[ z_{q,w} \]

can be considered as a vector in
\[ V^V. \]

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

Lemma 46. 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
\[ m \]-permutation
\[ w \]

of
\[ q \]

such that
\[ z_{q,w} = z, \]

if and only if
\[ \sum_{c \in V} z(c) = s(q) \]

(25)

and
\[ \sum_{c \in V} c \otimes z(c) \in I_2. \]

(26)

Proof. It is clear that the conditions are indeed necessary, so we only need to prove the other
direction. Since
\[ m_q(c) > 0 \]

we can find a
\[ w_0 \]

such that
\[ z_{q,w_0} = z. \]

(Of course
\[ w_0 \]

is not necessarily
\[ an \]

m-permutation of
\[ q. \]

Condition (26) gives us that
\[ < q \otimes w_0 > \in I_2. \]

Using Lemma 45 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
\[ m_0(a,b) = \sum_{1 \leq i,j \leq n} a_{ij} \]

\[ q_i = a, \]

\[ q_j = b. \]

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 \( \ell \) is an integer chosen such that \( 0 \leq m(a,b) - 2\ell|V| < 2|V| \). Now for every \( 0 \neq a \in V \) we do the following procedure. We find the unique integer \( \ell \) such that for
\[
\Delta = m_q(a) - \sum_{b \in V} m(a,b) - \ell 2|V|,
\]
we have \( 0 \leq \Delta < 2|V| \). Now increase \( m(a,a) \) by \( \ell 2|V| \). (Note that \( \ell \) is non-negative because of the condition \( m_q(a) > 10|V|^2 \).) Increase both \( m(a,0) \) and \( m(0,a) \) by \( \Delta \). Finally, let \( \Delta_0 = m_q(0) - \sum_{b \in V} m(0,b) \), and increase \( m(0,0) \) by \( \Delta_0 \). (Once again \( \Delta_0 \) 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
\[
m(0,0) = \sum_{a,b \in V} m(a,b) - 2 \sum_{\{a,b\} \neq \{a,0\}} m(a, b) - \sum_{0 \neq a \in V} m(a,a) = n - 2 \sum_{\{a,b\} \neq \{a,0\}} m(a, b) - \sum_{0 \neq a \in V} m(a,a).
\]

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 \( m \)-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
\[
z_{q,w}(a) = \sum_{1 \leq i \leq n, q_i = a} w_i = \sum_{b \in V} m_{q,w}(a,b) b = \sum_{b \in V} m_0(a,b) b = \sum_{b \in V, 1 \leq i,j \leq n} a_{ij} b = \sum_{b \in V} \sum_{1 \leq i,j \leq n} a_{ij} q_j = \sum_{b \in V} a_{ij} q_j = \sum_{1 \leq i,j \leq n} w_0(i) = z_{q,w_0}(a) = z(a).
\]

Finally
\[
z_{q,w}(0) = \sum_{a \in V} z_{q,w}(a) - \sum_{0 \neq a \in V} z_{q,w}(a) = \sum_{i=1}^n a_i - \sum_{0 \neq a \in V} z_{q,w}(a)
\]
\[
s(q) - \sum_{0 \neq a \in V} z(a) = \sum_{a \in V} z(a) - \sum_{0 \neq a \in V} z(a) = z(0),
\]

using condition \([25]\).

The proof of Lemma \([13]\) also gives us the following statement.

**Lemma 47.** Let \( q_1, q_2, \ldots, q_h \in V^n \) and \( r \in V^n \). Assume that \( \sum_{i=1}^n s(q_i) = s(r_i) \). Then there is an integral vector \( m \) indexed by \( V^h \) such that\(^4\)
\[
m(t_i = b) = m_{q_i}(b)
\]
for every \( i = 1, 2, \ldots, h \) and \( b \in V \), and
\[
m(t_{\Sigma} = b) = m_{r}(b)
\]
for every \( b \in V \).

\(^4\)Unlike in the rest of this section, here the components of a \( t \in V^h \) are indexed from 1 to \( h \).
Now we are ready to prove Lemma 44.

**Proof.** Fix an $\alpha$-typical $q$, and $r \in R^S(q, h)$. Let $W$ be the set of $z \in V^V$ satisfying the conditions (25) and (26) of Lemma 46. 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 $z_1, z_2, \ldots, z_h \in W$ such that $z_{q,r} = \sum_{i=1}^h z_i$. If $n$ is large enough then for an $\alpha$-typical $q$, we have $m_q(c) > 10|V|^2$. By using Lemma 46 for each $i \in \{1, 2, \ldots, h\}$ we can find an $m$-permutation $\hat{w}_i$ of $q$ such that $z_{q,\hat{w}_i} = z_i$. 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 $\{t \mid q_i = a\}$. Similarly, $r^a$ is obtained from $r$ by projecting to the same set of coordinates. Observe that $\sum_{i=1}^h s(w_i^a) = \sum_{i=1}^h z_i(a) = z_{q,r}(a) = s(r^a)$ so from Lemma 47 we obtain an integral vector $m^a$ indexed by $V^h$ such that

$$m^a(t_i = b) = m_{w_i^a}(b) = m_{q,\hat{w}_i}(a, b)$$

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

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

for every $b \in V$.

Then the vector $m$ defined by

$$m((t_0, 1_1, \ldots, t_h)) = m^0((t_1, \ldots, t_h))$$

gives us an integral point in $A^S(q, r)$ satisfying the parity constraints in (21) of Lemma 42. □

**Lemma 48.** For an $\alpha$-typical $q \in V^n$, a $(q, \beta)$-typical $r \in R^S(q, h)$, $r_0 = r_0(q)$ and $m \in M^{S^*}(q, r_0)$ we have that

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

uniformly.

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

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

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

$$B(x, y) = -|V|^{1+h} \sum_{t \in V^{1+h}} x(t)y(t) + \frac{|V|^2}{2} \sum_{i=1}^h \sum_{a, b \in V} x(t_0 = a, t_i = b)y(t_0 = a, t_i = b) + |V|^2 \sum_{a, b \in V} x(t_0 = a, t_\Sigma = b)y(t_0 = a, t_\Sigma = b).$$

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

**Lemma 49.** The following holds

$$\lim_{n \to \infty} \sup_{q \in V^n} \sup_{r \in R^S(q, h) \text{ typical}} P((\Sigma(\vec{Q}) = r) \land (\vec{Q} \text{ is not } \gamma \text{ typical}) \land m_{\vec{Q}} = m) |V|^n = 0.$$
Proof. Take any $\alpha$-typical $q \in V^n$ and $(q, \beta)$-typical $r \in R^S(q,h)$. We define

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

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

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

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 23.

Let $S_{q,d}^m$ be the sum of $d$ i.i.d. random $m$-permutations of $q$. The analogue of Theorem 9 is the following.

**Theorem 50.** For $d \geq 3$ and $\frac{1}{2} < \alpha < \frac{2}{3}$ we have

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

This theorem follows immediately from Theorem 40 once we prove the following analogue of Lemma 24.

**Lemma 51.** Let $q \in V^n$ be $\alpha$-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 $C$ (independent of $q, r$), such that

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

This will be proved after Lemma 52 because the proofs of these two lemmas share some ideas.

Once we have Theorem 50 we only need to control the non-typical vectors to obtain Theorem 4. This can be done almost the same way as in Section 4. Here we list the necessary modifications.

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

**Lemma 52.** Let $q, r \in V^n$ and $m \in M^S(q,r) = \{ m_Q | \ Q \text{ is a } (q, 1, d)\text{-tuple and } \Sigma(Q) = r \}$. We define

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

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 $\bar{Q} = (\bar{q}^{(0)}, \bar{q}^{(1)}, \ldots, \bar{q}^{(d-1)})$ we have that $r - \Sigma(\bar{Q})$ is an $m$-permutation of $q$ and the $(q, 1, d)$-tuple $Q' = (\bar{q}^{(0)}, \bar{q}^{(1)}, \ldots, \bar{q}^{(d-1)}, r - \Sigma(\bar{Q}))$ satisfies $m_{Q'} = m$. Then there is a polynomial $f(n)$ (not depending on $q, r$ or $m$) such that

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

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

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

31
Proof. Let \( X = (X_0, X_1, X_2, \ldots, X_d) \in V^{1+d} \) be a random variable, such that \( P(X = t) = \frac{m(t)}{n} \) for every \( t \in V^{1+d} \). We define \( X_\Sigma = \sum_{i=1}^d X_i \). Let \( h(Y) \) denote the Shannon entropy of the random variable \( Y \). 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

\[
p(m) = c_2(m) \exp \left( n \left( h(X) - h(X, X_\Sigma) - \frac{1}{2} \sum_{i=1}^{d-1} h(X_0, X_i) \right) \right),
\]
where \( \frac{1}{c_1(m)} \geq c_1(m), c_2(m) \leq b(n) \) for some polynomial \( b(n) \). The random variables \( X \) and \((X_0, X_1, \ldots, X_{d-1}, X_\Sigma)\) mutually determine each other, thus \( h(X) = h(X_0, X_1, \ldots, X_{d-1}, X_\Sigma) \). Using the well-known properties of entropy we get

\[
h(X) = h(X_0, \ldots, X_{d-1}, X_\Sigma) \leq h(X_0) + \sum_{i=1}^{d-1} (h(X_0, X_i) - h(X_0)) + (h(X_0, X_\Sigma) - h(X_0)).
\]

Or more generally for every \( i = 1, 2, \ldots, d \)

\[
h(X) \leq h(X_0) + \sum_{1 \leq j \leq d \atop j \neq i} (h(X_0, X_j) - h(X_0)) + (h(X_0, X_\Sigma) - h(X_0)).
\]

Summing up these inequalities for \( i = 1, 2, \ldots, d-1 \) we get that

\[
(d-1)h(X) \leq (d-1)h(X_0) + h(X_0, X_d) - h(X_0) + (d-2) \sum_{i=1}^{d-1} (h(X_0, X_i) - h(X_0)) + (d-1)(h(X_0, X_\Sigma) - h(X_0)) =
\]

\[
(d-2) \sum_{i=1}^{d-1} h(X_0, X_i) + (d-1)h(X_0, X_d) + (d-1)h(X_0, X_\Sigma) - (d-1)^2 h(X_0).
\]

Therefore

\[
h(X_0) + h(X) - h(X_0, X_\Sigma) - \frac{1}{2} \sum_{i=1}^d h(X_0, X_i) =
\]

\[
h(X_0) + h(X) - h(X_0, X_\Sigma) = \frac{1}{2(d-1)} \sum_{i=1}^{d-1} h(X_0, X_i) - \frac{1}{2} \left( \frac{d-2}{d-1} \sum_{i=1}^{d-1} h(X_0, X_i) + h(X_0, X_d) \right)
\]

\[
\leq h(X_0) + h(X) - h(X_0, X_\Sigma) - \frac{1}{2(d-1)} \sum_{i=1}^{d-1} h(X_0, X_i) - \frac{1}{2} (h(X) + (d-1)h(X_0) - h(X_0, X_\Sigma)) =
\]

\[
\frac{1}{d-1} \left( h(X) - h(X_0, X_\Sigma) - \frac{1}{2} \sum_{i=1}^{d-1} h(X_0, X_i) \right) + \frac{d-3}{2(d-1)} (h(X) - h(X_0, X_\Sigma)) - \frac{(d-3)}{2} h(X_0)
\]

\[
\leq \frac{1}{d-1} \left( h(X) - h(X_0, X_\Sigma) - \frac{1}{2} \sum_{i=1}^{d-1} h(X_0, X_i) \right)
\]

32
using that \( h(X) \leq h(X_0, X_\Sigma) + (d - 1) h(X_0) \). This gives the first statement. To get the second one observe that

\[
|S(q)|P(S_{q,d}^m = r) = \sum_{m \in \mathcal{M}^f(q,r)} E(M) \leq \sum_{m \in \mathcal{M}^f(q,r)} f(n)p(m) \leq |\mathcal{M}^S(q,r)|f(n)P(r - S_{q,d} \sim q)^{\frac{1}{r}}.
\]

Now we prove Lemma 53.

**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 \( P(\Sigma(Q) = r \text{ and } m \Sigma = m) \). To show this, let \( X = (X_0, X_1, X_2) \in V^{1+2} \) be a random variable, such that \( P(X = t) = \frac{m(t)}{n} \) for every \( t \in V^{1+2} \), and let \( X_\Sigma = X_1 + X_2 \). Then \( P(\Sigma(Q) = r \text{ and } m \Sigma = m) \) can be upper bounded by some polynomial multiple of

\[
\exp \left( n \left( h(X) - h(X_0, X_\Sigma) - \frac{1}{2} (h(X_0, X_1) + h(X_0, X_1)) \right) \right) = \exp \left( n \left( h(X_0) - \frac{1}{2} (h(X_0, X_1) + h(X_0, X_\Sigma) - h(X) - h(X_0)) \right) \right) \leq \exp(-nh(X_0)) \leq |V|^{-n} \exp(Cn^{2\alpha - 1}),
\]

using the fact that \( h(X_0, X_1) + h(X_0, X_\Sigma) \geq h(X_0) + h(X_0, X_1, X_\Sigma) = h(X_0) + h(X) \).

For any non-negative integral vector \( m \) indexed by \( V^{1+d} \) we define

\[
E(m) = \frac{m(V^{1+d})!}{\prod_{a \in V} m(t_0 = a)!} \left( \frac{m(V^{1+d})!}{2^{m(V^{1+d})/2}(m(V^{1+d})/2)!} \right)^{-d} \prod_{a,b \in V} m(t_0 = a, t_\Sigma = b)! \prod_{t \in V^{1+d}} m(t)! \prod_{i=1}^{d} \left( \prod_{a \in V} \frac{m(t_i = a, t_0 = a)!}{2^{m(t_i = a, t_0 = a)/2}(m(t_i = a, t_0 = a)/2)!} \right) \left( \prod_{a \neq b \in V} \sqrt{m(t_0 = a, t_i = b)!} \right).
\]

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

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

\[
1 + \frac{m_0(t_0 = u, t_\Sigma = u)}{1 + m_0(u)} \leq \log^4 n,
\]

and for every \( c \in W \) we have

\[
|m(t_0 = c) - \frac{n}{|W|}| < 2n^\alpha,
\]

where \( n = \sum_{t \in V^{1+d}} m(t) \).

**Lemma 53.** Consider a non-negative integral 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 \( x_U \in \mathbb{R}^{V^{1+d}} \) such that \( x_U(u) = 1 \) and \( x_U(t) = 0 \) for every \( t \neq u \in V^{1+d} \). If \( u \in W^{1+d} \) then

\[
E(m_0 + x_U)/E(m_0) = O(\log^4 n),
\]

33
if \( u_0 \not\in W \) 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 \( u \not\in W^{1+d} \), then
\[
E(m_0 + \chi_u)/E(m_0) = O(\log^2 n).
\]

There is a \( D, \delta > 0 \), such that for any \( i \in \{h+1, h+2, \ldots, \ell\} \) we have
\[
E(m_0 + \chi_i)/E(m_0) = O\left((n^{-\delta} \log^D n)^{\|m\|_{W^C}}\right).
\]

Proof. Let \( g = \frac{1+m_0(t_0=u, t_\Sigma=w)}{1+m_0(u)} \), \( h = \frac{n+1}{m(t_0-u_0)+1} \) and \( f_i = \sqrt{1+m_0(t_0=u_0, t_i=u_i)} \).
Note that
\[
E(m_0 + \chi_u)/E(m_0) = O(g \cdot h \cdot \prod_{i=1}^d f_i).
\]

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 \( u_0 \not\in W \), 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 \( u \not\in W^{1+d} \) we consider two cases. First assume that \( u_\Sigma \in dW \), then \( g = O(n) \), \( h = O(1) \), moreover there are at least two indices \( i \) such that \( u_i \not\in W \). 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. Now assume that \( u_\Sigma \not\in dW \), then \( g = O(\log n) \), \( h = O(1) \) and \( f_i \leq 1 \) for every \( i \). The statement follows.

The prove the last statement of the lemma, take any \( i \in \{h+1, h+2, \ldots, \ell\} \). Since \( m_i \) is not supported on \( W^{1+d} \) we have a \( u \not\in W^{1+d} \) such that \( m_i(u) \geq 1 \). If \( u_0 \not\in W \), then \( m_i(t_0 \not\in W) \geq m_i(t_0 = u_0) \geq 1 \). If \( u_0 \in W \), then there is a \( j \) such that \( u_j \not\in W \), thus
\[
m_i(t_0 \not\in W) \geq m_i(t_0 = u_j, t_j = u_0) = m(t_0 = u_0, t_j = u_j) \geq m_i(u) \geq 1.
\]
In both cases we obtained that \( m_i(t_0 \not\in W) \geq 1 \). Note that for \( d \geq 3 \) we have \( d/2 - 1 > 0 \). From the previous statements it follows that for a large enough \( D \) and a small enough \( \delta > 0 \) we have
\[
E(m_0 + m_i)/E(m_0) = O\left((\log^D n)^{\|m\|_{W^C}} n^{-(d/2-1)}\right) = O\left((n^{-\delta} \log^D n)^{\|m\|_{W^C}}\right).
\]

With these modifications above we proved Theorem 4.

As an easy consequence of Theorem 4 we obtain following analog of Corollary 36. 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 \( q_1, q_2, \ldots, q_{n-1} \) is denoted by \( G_q \). Let \( U_q^S \) be a uniform random element of the set \( \{w \in G_n': |< q \otimes w > | \leq I_2\} \).

**Corollary 54.** We have
\[
\lim_{n \to \infty} \sum_{q \in V^{n-1}} d_\infty(C_n', U_q^S) = 0.
\]

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 \( P(U_q^S = r) = |V|^{- (n-1) 2^{\text{Rank}_2(V)}} | \wedge^2 V | \). Therefore, Theorem 23 can be proved using the following observation.

**Lemma 55.** 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 \( 2^{\text{Rank}_2(V)} \) in \( V \).

If \( d \) is odd Theorem 1 follows from Theorem 2 and the results of Wood [20][Theorem 8.3].
Towards understanding the 2-Sylow subgroup in the case of even $d$

For a non-negative integer $k$, let $FA(2, k)$ be the set of (isomorphism classes of) finite abelian 2-groups $G$ such that the exponent of $G$ divides $2^k$. Moreover, let $FA_{odd}(2, k)$ be the set of groups in $FA(2, k)$ with odd rank.

Assume that $d$ is even. Let $\Delta_n$ be the reduced Laplacian of $H_n$, and $\Gamma_n$ be the corresponding sandpile group. Observe that the mod 2 reduction of $\Delta_n$ is a symplectic matrix of odd dimension, so we have the following lemma.

**Lemma 56.** The group $\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}$ has odd rank.

The next lemma shows that the limiting distribution of the 2-Sylow subgroup $\Gamma_n, 2$ is uniquely determined by its moments and the extra condition that it has odd rank.

**Lemma 57.** (i) Let $k$ be a positive integer. Then there is a unique probability measure $\nu_k$ on $FA_{odd}(2, k)$, such that $\text{Sur}(\nu_k, V) = |\wedge^2 V|2^{\text{Rank}_2(V)}$ for any $V \in FA(2, k)$. Moreover, if $X_n$ is a sequence of random finitely generated abelian groups of odd rank, such that for any $V \in FA(2, k)$ we have

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

then for every $V \in FA_{odd}(2, k)$

$$\lim_{n \to \infty} P(X_n \otimes \mathbb{Z}/2^k\mathbb{Z} \cong V) = \nu_k(V).$$

(ii) There is a unique probability measure $\nu$ on the set of finite abelian 2-groups of odd rank, such that $\text{Sur}(\nu, V) = |\wedge^2 V|2^{\text{Rank}_2(V)}$ for any finite abelian 2-group $V$. Moreover, if $X_n$ is a sequence of random finite abelian 2-groups of odd rank, such that for any finite abelian 2-group $V$ we have

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

then for every finite abelian 2-group $V$ of odd rank we have

$$\lim_{n \to \infty} P(X_n \cong V) = \nu(V).$$

(iii) We have the following formula for $\nu_1$. For any odd $r$ the following holds

$$\nu_1((\mathbb{Z}/2\mathbb{Z})^r) = \frac{2^r}{\prod_{i=1}^r (2^i - 1)} \prod_{i=1}^\infty (1 + 2^{-i})^{-1}.$$

**Proof.** The statements of (i) can be obtained by slightly modifying the argument of Wood [20] [Theorem 8.3] by making use of the fact that the ranks of the groups $X_n$ are odd. We only point out the details needed to be changed. Lemma 8.1. should be replaced by the following lemma.

---

5To be precise, $\Gamma_{n,2}$ might have even rank, because if $H_n$ is not connected, then the rank of $\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}$ and $\Gamma_{n,2}$ are different. But the probability of this tends to 0.

6Or slightly more generally $X_n$ has odd rank and it is a direct sum of a finite abelian 2-group and a finitely generated free abelian group.
Lemma 58. 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 \( z_1, \ldots, z_m \)

\[
\tilde{H}_{m,2,b}(z) = \sum_{d_1,\ldots,d_m \geq 0} a_{d_1,\ldots,d_m} z_1^{d_1} \cdots z_m^{d_m}
\]
and a constant \( E \) such that

\[
a_{d_1,\ldots,d_m} \leq E 2^{-b_1 d_1 - d_1 (d_1 + 1)}.
\]

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

Proof. The proof is the same as the proof of [20] Lemma 8.1. But instead of \( G(z_1) \) we use

\[
\tilde{G}_1 = \prod_{j > b_1 \text{ odd}} \left( 1 - \frac{z_1}{2j} \right) = \sum_{d_1 \geq 0} c_{d_1} z_1^{d_1}.
\]

Observe that \( \tilde{G}_1(4z) = (1 - \frac{1}{2^{b_1}})\tilde{G}_1(z) \). So \( 4^n c_n = c_n - 2^{-b_1} c_{n-1} \), or equivalently \( c_n = \frac{2^{-b_1} - 2n}{1 - 4^{-1}} c_{n-1} \). Since \( c_0 = 1 \), by induction we obtain that

\[
c_n = \frac{(-1)^n 2^{-nb_1 - n(n+1)}}{\prod_{i=1}^{n+1} (1 - 4^{-i})}.
\]

So \( |c_n| \leq 2^{-nb_1 - n(n+1)} \prod_{i=1}^{\infty} (1 - 4^{-i})^{-1} \).

Lemma 7.4. of Wood [20] states that there is a constant \( F \) such that for any abelian 2-group \( G \) of type \( \lambda \) we have

\[
\sum_{\text{\( G_1 \) subgroup of } G} |\wedge^2 G_1| \leq F^{\lambda_1 2 \sum_i \frac{\lambda_i (\lambda_i - 1)}{2}}.
\]

As a simple corollary of this we obtain that

\[
\sum_{\text{\( G_1 \) subgroup of } G} |\wedge^2 G_1|^{2 \text{\( \text{Rank}_2(G_1) \)}} \leq F^{\lambda_1 2 \text{\( \text{Rank}_2(G) \}) 2 \sum_i \frac{\lambda_i (\lambda_i - 1)}{2}} = F^{\lambda_1 2 \lambda_1 + \sum_i \frac{\lambda_i (\lambda_i - 1)}{2}}. \quad (27)
\]

Instead of Theorem 8.2. we use the following lemma.

**Lemma 59.** Let \( m \geq 1 \) be an integer. Let \( M_0 \) be the set of partitions \( \lambda \) with at most \( m \) parts. Let \( M \) be the set of partitions \( \lambda \in M_0 \) such that \( \lambda_1 \) is odd.

Suppose we have non-negative reals \( x_{\mu}, y_{\mu} \), for each partition \( \mu \in M \). Further suppose that we have non-negative reals \( C_{\lambda} \) for each \( \lambda \in M_0 \) such that

\[
C_{\lambda} \leq F^{m 2^{\lambda_1 + \sum_i \frac{\lambda_i (\lambda_i - 1)}{2}}},
\]

where \( F > 0 \) is an absolute constant. Suppose that for all \( \lambda \in M_0 \),

\[
\sum_{\mu \in M} x_{\mu} 2^{\sum_i \lambda_i \mu_i} = \sum_{\mu \in M} y_{\mu} 2^{\sum_i \lambda_i \mu_i} = C_{\lambda}. \quad (28)
\]

Then for all \( \mu \), we have that \( x_{\mu} = y_{\mu} \).
To proceed with the proof we need to prove that \( \sum_{\lambda \in M_0} A_\lambda C_\lambda \) is absolutely convergent. We have

\[
\sum_{\lambda \in M_0} |A_\lambda C_\lambda| \leq \sum_{d_1,\ldots,d_m \geq 0 \atop d_2 + \cdots + d_m \leq \mu_1} |a_{d_1,d_2,\ldots,d_m}| F^m 2^{\sum d_i + \sum \frac{m-1}{2}(\sum d_i - d_i - 1)} \leq \sum_{d_1,\ldots,d_m \geq 0 \atop d_2 + \cdots + d_m \leq \mu_1} E^2 b_2 d_1 - d_1 (d_1 + 1) F^m 2^{\sum d_i + \sum \frac{m-1}{2}(\sum d_i - d_i - 1)}.
\]

For each choice of \( d_2,\ldots,d_m \), the remaining sum over \( d_1 \) is a constant times \( \sum_{d_1 \geq 0} 2^{d_1 - (b_1 - \frac{1}{2}d_2 + \cdots + d_m - \frac{d_1}{2})} \), which converges, so it follows that \( \sum_{\lambda \in M} A_\lambda C_\lambda \) converges absolutely.

The rest of the proof follows by repeating the arguments of Wood [20]. To prove (1) first we need to following lemma.

Lemma 60. For a random finite 2-group \( X \) we have

\[
P(X \notin FA(2,k)) \leq \frac{E|\text{Sur}(X,\mathbb{Z}/2^{k+1}\mathbb{Z})|}{2^k}.
\]

Proof. Observe that if a finite abelian 2-group has exponent \( 2^{k+1} \), then it has at least \( 2^k \) surjective homomorphism to \( \mathbb{Z}/2^{k+1}\mathbb{Z} \). Thus the statement follows from

\[
E|\text{Sur}(X,\mathbb{Z}/2^{k+1}\mathbb{Z})| \geq P(x \notin AF(2,k))2^k.
\]

Now we prove the uniqueness of the measure \( \nu \). Let \( \nu \) be a measure satisfying the properties of (1). Let \( X \) be a random group with distribution \( \nu \). Let \( V \in FA_{\text{odd}}(2,k) \). Take any \( m > k \). Then for any \( W \in FA(2,m) \) we have

\[
E|\text{Sur}(X \otimes \mathbb{Z}/2^m\mathbb{Z}, W)| = E|\text{Sur}(X, W)| = |W|2^{\text{Rank}_2(W)}.
\]

Using the statement of (1) we get that \( X \otimes \mathbb{Z}/2^m\mathbb{Z} \) has distribution \( \nu_m \). Thus

\[
\nu(V) = P(X \cong V) = P(X \otimes \mathbb{Z}/2^m\mathbb{Z} \cong V) = \nu_m(V).
\]

This shows that the only possible measure is the one defined as follows. For \( V \in FA_{\text{odd}}(2,k) \) we set \( \nu(V) = \nu_m(V) \), where \( m > k \). A similar argument as above shows that this does not depend on the choice of \( m \) as long as \( m > k \). An alternative way to express \( \nu(V) \) is

\[
\nu(V) = \lim_{m \to \infty} \nu_m(V).
\]

We need to prove that for any \( W \in FA(2,k) \) we have \( \text{Sur}(\nu, W) = |W|2^{\text{Rank}_2(W)} \). Let \( \tilde{\nu} \) be the push forward of the measure \( \nu \) by the map \( X \mapsto X \otimes \mathbb{Z}/2^k\mathbb{Z} \). It is enough to prove that \( \tilde{\nu} = \nu_k \). If \( V \) has exponent smaller than \( 2^k \), then \( \tilde{\nu}(V) = \nu(V) = \nu_k(V) \). If \( V \in FA_{\text{odd}}(2,k) \setminus FA_{\text{odd}}(2,k-1) \) then

\[
\tilde{\nu}(V) = \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \ni V} \nu(U) = \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \ni V} \lim_{m \to \infty} \nu_m(U) \leq \lim_{m \to \infty} \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \ni V} \nu_m(U) = \nu_k(V),
\]

37
using Fatou’s lemma and the fact that if $X_m$ has distribution $\nu_m$ for $m > k$, then $X_m \otimes \mathbb{Z}/2^k\mathbb{Z}$ has distribution $\nu_k$. Using the latter fact and Lemma 60 we obtain that

$$\nu_k(V) = P(X_m \otimes \mathbb{Z}/2^k\mathbb{Z} \cong V) = \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \cong V} \nu_m(U) + \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \cong V} \nu_m(U) \leq \sum_{U \otimes \mathbb{Z}/2^k\mathbb{Z} \cong V} \nu(U) + P(X_m \not\in FA(2, m - 1)) \leq \tilde{\nu}(V) + \frac{\mathbb{E}|\text{Sur}(X, \mathbb{Z}/2^m\mathbb{Z})|}{2^{m-1}} = \tilde{\nu}(V) + 2^{-(m-2)}.$$

Tending to infinity with $m$, we obtain that $\nu_k(V) \leq \tilde{\nu}(V)$. So indeed $\nu_k = \tilde{\nu}$.

The last statement of (iii) follows from (i) and (29). The statement of (iii) follows from (i) and the results of Heath-Brown [11].

In Lemma 57 above we concentrated only on the prime 2 for simplicity, but the using the same argument we can handle finitely many primes simultaneously by following the argument of Wood [20]. So indeed the convergence of the moments together with Lemma 56 imply Theorem 1 for the random graphs $H_n$ and even $d$, where $\nu$ is the unique distribution given by (ii) of Lemma 57.

We were not able to give an explicit formula for $\nu$, but using (iii) of Lemma 57 we can give an explicit formula for the limit distribution of the rank of $\Gamma_{n,2}$. That is, we have the following theorem.

**Theorem 61.** Let $2 = p_1, p_2, \ldots, p_s$ be the distinct primes. Assume that $d \geq 3$. Let $S_{n,i}$ be the $p_i$-Sylow subgroup of $S_n$. For $i = 1, 2, \ldots, s$ let $r_i$ be a non-negative integer. Then in the case of odd $d$ we have

$$\lim_{n \to \infty} P(S_{n,i} = r_i \text{ for all } i = 1, 2, \ldots, s) = \prod_{i=1}^{s} \left( p_i^{\frac{r_i(r_i+1)}{2}} \prod_{j=r_i+1}^{\infty} (1 - p_i^{-j}) \prod_{j=1}^{\infty} (1 - p_i^{-2j})^{-1} \right).$$

In case of even $d$, assuming that $r_1$ is odd we have

$$\lim_{n \to \infty} P(S_{n,i} = r_i \text{ for all } i = 1, 2, \ldots, s) = \left( \frac{2^{r_1}}{\prod_{i=1}^{2^{r_1}} (2^i - 1)} \prod_{i=1}^{\infty} (1 + 2^{-i})^{-1} \right)^{s} \prod_{i=2}^{s} \left( p_i^{\frac{r_i(r_i+1)}{2}} \prod_{j=r_i+1}^{\infty} (1 - p_i^{-j}) \prod_{j=1}^{\infty} (1 - p_i^{-2j})^{-1} \right).$$

In the rest of the section we give another characterization of the distribution $\nu$.

We start by showing that Lemma 63 is true under slightly weaker conditions.

**Lemma 62.** 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 $r = A_q$ and all the diagonal entries of $A$ are even.

**Proof.** We start by the following lemma. As in Lemma 45 let $V = \bigoplus_{i=1}^{\ell} <v_i>$.

**Lemma 63.** 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 $1 \leq i \leq \ell$. 

38
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 \( q_{\ell+1}, q_{\ell+2}, \ldots, q_n \) generates \( V \). Let us define \( q' = (v_1, v_2, \ldots, v_\ell, q_{\ell+1}, q_{\ell+2}, \ldots, q_n) \). 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 \( q_{\ell+1}, q_{\ell+2}, \ldots, q_n \) 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 \( r' = (B^{-1})^T r \). Observe that \(< q' \otimes r' >= Bq \otimes (B^{-1})^T r >= B^{-1} Bq \otimes r >= q \otimes r > \in I_2 \). Applying Lemma [53] 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 symmetric integral matrix with even diagonal entries. Moreover, \( Aq = B^T A'Bq = B^T A'q' = B^T r' = B^T (B^{-1})^T r = r \).

Lemma 64. Let \( V \) be a finite Abelian 2-group. Assume that \( 2^k \) is divisible by the exponent of \( V \). Let \( B_n \) be uniformly chosen from the set of symmetric matrices in \( M_n(\mathbb{Z}/2^k\mathbb{Z}) \). The random symmetric matrix \( A_n \) is obtained from \( B_n \) by multiplying each diagonal entry by 2. Then we have

\[
\lim_{n \to \infty} \mathbb{E}\{|q \in V^n| \ G_q = V, \ A_n q = 0\} = |\land^2 V|2^{\text{Rank}_2(V)}.
\]

Proof. Take any \( q \in V^n \) such that \( G_q = V \). Let \( C \) be a uniform element of \( M_n(\mathbb{Z}/2^k\mathbb{Z}) \). Observe that \( A_n \) has the same distribution as \( C + CT \). Therefore, the distribution of \( A_n q \) is the uniform distribution on the image of the \( M_n(\mathbb{Z}/2^k\mathbb{Z}) \to V^n \) homomorphism \( C \mapsto (C + CT)q \). From Lemma [62] 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 \( |V^n| (|\land^2 V|2^{\text{Rank}_2(V)})^{-1} \). It is clear that 0 is always contained in the image, thus

\[
\lim_{n \to \infty} \mathbb{E}\{|q \in V^n| \ G_q = V, \ A_n q = 0\} = \lim_{n \to \infty} \mathbb{E}\{|q \in V^n| \ G_q = V\} \frac{|\land^2 V|2^{\text{Rank}_2(V)}}{|V^n|} = |\land^2 V|2^{\text{Rank}_2(V)}.
\]

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 [57] we get the following.

Lemma 65. Let \( R_n \) be a random \( n \times n \) symmetric matrix over the 2-adic integers, distributed according to Haar measure. We obtain \( Q_n \) from \( R_n \) by multiplying each diagonal entry by 2. Let \( \Gamma_n \) be the cokernel of \( Q_n \). For any finite Abelian 2-group \( V \) we have

\[
\lim_{n \to \infty} \mathbb{E}|\text{Sur}(\Gamma_n, V)| = |\land^2 V|2^{\text{Rank}_2(V)}.
\]

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 symplectic matrix. Consequently, \( \text{Rank}_2(V) \equiv n \) modulo 2.

The lemma above and Lemma [57] gives the following characterization of \( \nu \).
Lemma 66. Let $\Gamma_n$ and $Q_n$ be as in Lemma 65. If $n$ is odd, then $\Gamma_n$ has odd rank. For any finite abelian 2-group $V$ of odd rank we have
\[ \lim_{n \to \infty} P(\Gamma_n \cong V) = \nu(V). \]

9 The sublinear growth of rank

In this section we prove Theorem 7. Let $\Gamma_n$ be the sandpile group of $H_n$. We start by a simple lemma. Recall that $\text{Rank}_p(\text{tors}(\Gamma_n))$ is the rank of the $p$-Sylow subgroup of $\text{tors}(\Gamma_n)$.

Lemma 67. There is a constant $c_d$ such that $|\text{tors}(\Gamma_n)| < c_d^n$. Consequently, for any prime $p$ we have
\[ \text{Rank}_p(\text{tors}(\Gamma_n)) \leq \frac{n \log c_d}{\log p}. \]

Proof. Let $v_1, v_2, \ldots, v_k = n$ 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 $\Delta_0$ 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 $\text{tors}(\Gamma_n) = \det 0$. Each row of $\Delta_0$ has Euclidean norm at most $c_d = \sqrt{2d^2}$. Thus, $\text{tors}(\Gamma_n) = \det 0 \leq c_d^{n-k} < c_d^n$. The proof of the second statement is straightforward from this.

The lemma above will be used for large primes, for small primes we will use the next lemma.

Lemma 68. For every prime $p$, there is a constant $C_p$ such that for any $n$ and $\varepsilon > 0$ we have
\[ P(\text{Rank}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}) \geq \varepsilon n) \leq C_p p^{-\varepsilon n}. \]

Proof. It is an easy consequence of Corollary 54 and Proposition 37 that
\[ \lim_{n \to \infty} E|\text{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \]
exists. This implies that there is a constant $C_p$ such that $E|\text{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \leq C_p$ for any $n$. Note that $|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| = |\text{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})|$. Thus, from Markov’s inequality
\[ P(\text{Rank}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}) \geq \varepsilon n) = P(|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| \geq p^{\varepsilon n}) \leq p^{-\varepsilon n}E|\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}| = p^{-\varepsilon n}E|\text{Hom}(\Gamma_n \otimes \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})| \leq C_p p^{-\varepsilon n}. \]

Now we are ready to prove Theorem 7. Take any $\varepsilon > 0$. Set $K = \exp(\varepsilon^{-1} \log c_d)$. Let $\{p_1, p_2, \ldots, p_s\}$ be the set of primes that are at most $K$. Using Lemma 68 we get that
\[ P(\text{Rank}(\Gamma_n \otimes \mathbb{Z}/p_i\mathbb{Z}) \geq \varepsilon n \text{ for some } i \in \{1, 2, \ldots, s\}) \leq \sum_{i=1}^{s} C_p p_i^{-\varepsilon n}. \]

Since $\sum_{i=1}^{\infty} \sum_{i=1}^{s} C_p p_i^{-\varepsilon n}$ is convergent, the Borel-Cantelli lemma gives us the following. With probability 1 there is an $N$ such that for every $n > N$ and $i = 1, 2, \ldots, s$ we have $\text{Rank}(\Gamma_n \otimes \mathbb{Z}/p_i\mathbb{Z}) < \varepsilon n$. By the choice of $K$ and Lemma 67, for a prime $p > K$ we have $\text{Rank}_p(\text{tors}(\Gamma_n)) \leq \varepsilon n$. Write $\Gamma_n$ as $\Gamma_n = \mathbb{Z}^f \times \text{tors}(\Gamma_n)$. Then for $n > N$ we have
\[ \text{Rank}(\Gamma_n) = f + \max_{p \text{ is a prime}} \text{Rank}_p(\text{tors}(\Gamma_n)) \leq \text{Rank}(\Gamma_n \otimes \mathbb{Z}/2\mathbb{Z}) + \max_{p \text{ is a prime}} \text{Rank}_p(\text{tors}(\Gamma_n)) \leq \varepsilon n + \varepsilon n. \]

Tending to 0 with $\varepsilon$ we get the statement.
10 Bounding the probabilities of non-typical events

At several points of the paper we need to bound the probability of that something is not-typical. These estimates are all based on the following lemma.

**Lemma 69.** Given $0 \leq a, b \leq n$, let $A$ and $B$ be a uniform independent random subset of $\{1, 2, \ldots, n\}$ such that $|A| = a$ and $|B| = b$. Then for any $k > 0$ we have

$$P \left( \left| A \cap B \right| - \frac{ab}{n} \geq k \right) \leq 2 \exp \left( \frac{k^2}{8 \min(a, n-a)} \right) \leq 2 \exp \left( -\frac{k^2}{8n} \right).$$

**Proof.** We may assume that $|A| \geq \frac{n}{2}$, because the case of $|A| < \frac{n}{2}$ can be reduced to this case by considering the complement of $A$ instead of $A$. Assume that we have an urn with $n$ balls, $b$ of them are black, the others are white. We start drawing balls from the urn without replacement. Let $X_i$ be the ratio of the black balls in the urn to the total number of balls left in the urn after we have drawn the $i$th ball. $X_0$ is defined to be $\frac{b}{n}$. This sequence will be a martingale and $|X_i - X_{i-1}| \leq \frac{1}{n-1}$. Clearly if we consider the number of black balls in the urn after drawing $n-a$ balls, this will be $X_{n-a}$. Observe that the distribution of $X_{n-a}$ is the same as the distribution of $|A \cap B|$. For any $i = 1, 2, \ldots, n-a$ we have $|X_i - X_{i-1}| \leq \frac{2}{n}$. Therefore from Azuma's inequality we have

$$P \left( \left| A \cap B \right| - \frac{ab}{n} \geq k \right) = P \left( a \left| X_{n-a} - \frac{b}{n} \right. \geq k \right) \leq$$

$$P \left( \left| X_{n-a} - \frac{b}{n} \right| \geq \frac{k}{n} \right) \leq 2 \exp \left( -\frac{k^2}{8(n-a)} \right) \leq 2 \exp \left( -\frac{k^2}{8n} \right) \quad (30)$$

Applying this iteratively we get the following lemma.

**Lemma 70.** Given $0 \leq a_1, a_2, \ldots, a_d \leq n$, let $A_1, A_2, \ldots, A_d$ be uniform independent random subsets of $\{1, 2, \ldots, n\}$ such that $|A_i| = a_i$ for $i = 1, 2, \ldots, d$. Then we have

$$P \left( \left| A_1 \cap \cdots \cap A_d \right| - a_1 \frac{\prod_{i=2}^{d} a_i}{n} \geq (d-1)k \right) \leq 2(d-1) \exp \left( -\frac{k^2}{8a_1} \right) \leq 2(d-1) \exp \left( -\frac{k^2}{8n} \right).$$

**Proof.** The proof is by induction. For $d = 2$ it is true as Lemma 69 shows. Now we prove for $d$. By induction

$$P \left( \left| A_1 \cap \ldots A_{d-1} \right| - a_1 \frac{\prod_{i=2}^{d-1} a_i}{n} \geq (d-2)k \right) \leq 2(d-2) \exp \left( -\frac{k^2}{8a_1} \right).$$

Using Lemma 69 for $A_1 \cap \ldots A_{d-1}$ and $A_d$ and the fact that $|A_1 \cap \ldots A_{d-1}| \leq a_1$ we have

$$P \left( \left| A_1 \cap \ldots A_d \right| - \frac{|A_1 \cap \ldots A_{d-1}| a_d}{n} \geq k \right) \leq 2 \exp \left( -\frac{k^2}{8a_1} \right).$$

Thus with probability at least $1 - 2(d-1) \exp \left( -\frac{k^2}{8a_1} \right)$ we have that

$$\left| A_1 \cap \ldots A_d \right| - \frac{|A_1 \cap \ldots A_{d-1}| a_d}{n} \leq k$$
and for
\[ \Delta = |A_1 \cap \ldots \cap A_{d-1}| - n \prod_{i=1}^{d-1} \frac{a_i}{n} \]
the inequality \(|\Delta| \leq (d - 2)k\) holds. Therefore
\[
\left| |A_1 \cap \ldots \cap A_d| - n \prod_{i=1}^{d} \frac{a_i}{n} \right| = \left| A_1 \cap \ldots \cap A_d \right| - \frac{a_d(|A_1 \cap \ldots \cap A_{d-1}| - \Delta)}{n} \leq \frac{a_d \Delta}{n} \leq k + (d - 2)k \leq (d - 1)k.
\]

Lemma 20, 22, 26 and 30 follows easily.

Acknowledgements The author is grateful to Miklós Abért for the useful discussions. The author was partially supported by the ERC Consolidator Grant 648017.

References

[1] Miklós Abért, 'Graph convergence, Luck approximation mod p and the entropy of cellular automata', Growth, symbolic dynamics and combinatorics of words in groups, June 2, 2015, ENS, Paris, video available at https://www.youtube.com/watch?v=wRRFOGPnaJY

[2] Ágnes Backhausz, Balázs Szegedy, On large girth regular graphs and random processes on trees, arXiv:1406.4420

[3] M. Bhargava, D. Kane, H. Lenstra, B. Poonen, and E. Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves, preprint arXiv:1304.3971 2013.

[4] Julien Clancy, Timothy Leake, and Sam Payne. A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs. arXiv:1309.3340 [math], September 2013.

[5] Julien Clancy, Timothy Leake, Nathan Kaplan, Sam Payne, and Melanie Matchett Wood. On a Cohen-Lenstra heuristic for Jacobians of random graphs. 2014. preprint.

[6] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), volume 1068 of Lecture Notes in Math., pages 33-62. Springer, Berlin, 1984.

[7] Jordan Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, arXiv:0912.0325 2009.

[8] Matthew Farrell and Lionel Levine. CoEulerian graphs. Proceedings of the American Mathematical Society, 2015.

[9] E. Friedman and L. Washington, On the distribution of divisor class groups of curves over a finite field, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227-239.

[10] A. Frieze. Random structures and algorithms. In Proceedings of the International Congress of Mathematicians-Seoul 2014. Vol. 1, pages 311-340. Kyung Moon Sa, Seoul, 2014.
[11] D. R. Heath-Brown. The size of selmer groups for the congruent number problem, ii. 118, 1994. preprint version, http://eprints.maths.ox.ac.uk/154/.

[12] Alexander E. Holroyd, Lionel Levine, Karola Mészáros, Yuval Peres, James Propp, and David B. Wilson. Chip-firing and rotor-routing on directed graphs. In Vladas Sidoravicius and Maria Eulália Vares, editors, In and Out of Equilibrium 2, volume 60, pages 331-364. Birkhauser Basel, Basel.

[13] Jiaoyang Huang. Invertibility of adjacency matrices for random d-regular directed graphs, arXiv:1806.01382

[14] Shaked Koplewitz. Sandpile groups and the coeulerian property for random directed graphs, Advances in Applied Mathematics, 2017

[15] Lionel Levine and James Propp. What is ... a sandpile? Notices Amer. Math. Soc., 57(8):976-979, 2010.

[16] Serguei Norine and Peter Whalen. Jacobians of nearly complete and threshold graphs. European Journal of Combinatorics, 32(8):1368-1376, November 2011.

[17] Russel Lyons. Asymptotic Enumeration of Spanning Trees, Combin. Probab. Comput. 14 (2005), 491-522.

[18] Alexander Schrijver, Theory of Linear and Integer Programming, John Wiley & Sons,

[19] V. H. Vu. Combinatorial problems in random matrix theory. In Proceedings of the International Congress of Mathematicians-Seoul 2014. Vol. IV, pages 489-508. Kyung Moon Sa, Seoul, 2014.

[20] Melanie Matchett Wood, The distribution of sandpile groups of random graphs Journal of the American Mathematical Society 30 (2017), pp. 915-958.

[21] Melanie Matchett Wood, Random integral matrices and the Cohen Lenstra Heuristics, to appear American Journal of Mathematics,