Title
Distribution of sandpile groups of directed and undirected bipartite graphs

ISBN
9798244802511

Author
Singhal, Deepesh

Publication Date
2026-05-07

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA,
IRVINE

Distribution of sandpile groups of directed and undirected bipartite graphs

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Deepesh Singhal

Dissertation Committee:
Nathan Kaplan, Chair
Asaf Ferber
Alexandra Florea

2026

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor, Nathan Kaplan, for his guidance and continued support throughout my time at U.C. Irvine. His mentorship has been instrumental in shaping my mathematical interests and has continually inspired me to pursue work of the highest caliber.

I am also grateful to the other members of my dissertation committee, Asaf Ferber and Alexandra Florea, for their time, support, and helpful feedback.

I would like to thank my friends Yuxin, Trung, Jeck, Fabian, Tianhao, and So for their friendship, encouragement, and support during graduate school.

I acknowledge support from NSF Grant DMS 2154223.

VITA

Deepesh Singhal

EDUCATION

Doctor of Philosophy in Mathematics **2026**
University of California, Irvine *Irvine, California*
Advisor: Nathan Kaplan

Master of Science in Mathematics **2022**
University of California, Irvine *Irvine, California*

Bachelor of Science in Mathematics, First Class Honors **2020**
Hong Kong University of Science and Technology *Hong Kong*

Exchange Student **Spring 2019**
National University of Singapore *Singapore*

ACADEMIC POSITIONS

Graduate Student Researcher **2023-2024**
University of California, Irvine *Irvine, California*

Associate Instructor, MATH 2E (Multivariable Calculus) **Summer 2023**
University of California, Irvine *Irvine, California*

Teaching Assistant, Department of Mathematics **2020-2026**
University of California, Irvine *Irvine, California*

Assistant for Undergraduate Research Project **Summer 2024**
University of California, Irvine *Irvine, California*

HONORS AND AWARDS

Von Neumann Award, U.C.I. **2024**
Research Mentorship Certificate, U.C.I. **2024**
Euler Outstanding Promise as a Graduate Student Award, U.C.I. **2022**
Epsilon Fund Award, H.K.U.S.T **2020**
Bronze Medal, International Mathematics Olympiad **2016**
Honourable Mention, Asia Pacific Mathematics Olympiad **2015**

REFEREED JOURNAL PUBLICATIONS

The p-rank stratification of the moduli space of double covers of a fixed elliptic curve 2025
with Y. Lin, K. Chang, D. Dragutinovic, S. Groen, and N. Tallaj
Nagoya Mathematical Journal

On a Conjecture of Beelen, Datta and Ghorpade for the Number of Points of Varieties over Finite Fields 2025
with Y. Lin
European Journal of Mathematics

On the Smallest Partition Associated to a Numerical Semigroup 2026
with N. Kaplan, K. Kim, C. McGeorge, and F. Ramirez
Contemporary Mathematics

Abelian covers of $\mathbb{P}^1$ of p-ordinary Ekedahl-Oort type 2024
with Y. Lin and E. Mantovan
International Mathematics Research Notices

Density questions in rings of the form $\mathcal{O}_K[\gamma] \cap K$ 2023
with Y. Lin
International Journal of Number Theory

Enumerating numerical sets associated to a numerical semigroup 2023
with A. Chen, N. Kaplan, C. O'Neill, and L. Lawson
Discrete Applied Mathematics

Primes in denominators of algebraic numbers 2023
with Y. Lin
International Journal of Number Theory

The Expected Embedding Dimension, Type and Weight of a Numerical Semigroup 2023
with N. Kaplan
Enumerative Combinatorics and Applications

Frobenius allowable gaps of Generalized Numerical Semigroups 2022
with Y. Lin
Electronic Journal of Combinatorics

Distribution of genus among numerical semigroups with fixed Frobenius number 2022
Semigroup Forum

Complementary Numerical Sets 2022
with M. Guhl, J. Juarez, V. Ponomarenko, and R. Rechkin
Integers: Electronic Journal of Combinatorial Number Theory

Numerical Semigroups of small and large type 2021
International Journal of Algebra and Computation

Density of Numerical Sets Associated to a Numerical Semigroup 2021
with Y. Lin
Communications in Algebra

PREPRINTS

Largest zero-dimensional intersection of r degree d hypersurfaces in $\mathbb{P}^m$ 2025
with Y. Lin
arXiv:2507.05732

Non-μ-ordinary Newton polygons in the Torelli locus 2024
with Y. Lin and E. Mantovan
arXiv:2406.09632

The shape of a random numerical semigroup 2026
with M. Bras-Amorós and N. Kaplan
arXiv:2604.26127

Distribution of sandpile groups of random bipartite graphs 2026
Preprint

Distribution of sandpile groups of random directed bipartite graphs 2026
Preprint

Sandpile groups of random bipartite graphs and families of distributions with the same moments 2026
with J. Fulman, N. Kaplan, and O. Warnaar
Preprint

On the asymptotic growth of the number of associated numerical sets 2026
with A. Chen, N. Kaplan, L. Lawson, and C. O'Neill
Preprint

ABSTRACT OF THE DISSERTATION

Distribution of sandpile groups of directed and undirected bipartite graphs

By

Deepesh Singhal

Doctor of Philosophy in Mathematics

University of California, Irvine, 2026

Nathan Kaplan, Chair

This thesis studies the asymptotic distribution of sandpile groups of random bipartite graphs in both the directed and undirected settings. Fix a prime p and let the two parts of the bipartition have sizes n and $\lceil \alpha n \rceil$, where $\frac{1}{p} < \alpha \leq 1$. For directed Erdős-Rényi bipartite graphs, this thesis proves that the p-Sylow subgroup of the sandpile group converges to the conjectured Cohen-Lenstra distribution. For undirected Erdős-Rényi bipartite graphs, it proves the corresponding conjecture for odd primes p, where the conjectured limit is the symmetric Cohen-Lenstra distribution. In the undirected case with $p = 2$, the limiting distribution has been conjectured to be a variant of the symmetric Cohen-Lenstra distribution. Our results provide strong evidence for this conjecture.

For a fixed finite abelian p-group G, the surjective moment of a random finite abelian p-group X is the expected number of surjective homomorphisms from X to G. The surjective moment method seeks to identify a limiting distribution by computing these expectations for every G and then showing that they determine the distribution. A central difficulty in both settings is that the usual surjective moment method does not apply directly: the surjective moments can diverge even though the conjectured limiting distributions have finite surjective moments.

The main idea is to isolate a high-probability subset of graphs on which the relevant moments

are well behaved, and to show that the complementary exceptional set is rare enough that it does not affect the limiting distribution. In all cases, after restricting to these high-probability subsets, the resulting surjective moments agree with the moments predicted by the conjectured limiting distributions. In the directed case for all primes p, and in the undirected case for odd primes p, Wood's universality result then yields the conjectured limiting distribution. For $p = 2$ in the undirected case, the computed moments agree with those of the conjectured distribution, but these moments do not by themselves determine a unique limiting law. These results extend the known picture for random graphs to the bipartite directed and undirected settings.

Chapter 1

Introduction

1.1 Background

1.1.1 Cokernels of random matrices

Random finite abelian groups arising in number theory can often be modeled as cokernels of random matrices with entries in $\mathbb{Z}$. Their p-Sylow subgroups can be modeled as cokernels of the corresponding matrices with entries in $\mathbb{Z}_p$. If $X \in \mathbb{M}_n(\mathbb{Z}_p)$, then X is a map from $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$, and its cokernel is denoted by $\operatorname{Coker}(X) := \mathbb{Z}_p^n / \operatorname{Im}(X)$. If the matrix X is of full rank, then $\operatorname{Coker}(X)$ is an abelian p-group.

The Cohen-Lenstra distributions arise naturally in this setting. They are distributions on the set of isomorphism classes of finite abelian p-groups. They are defined as follows, for $0 < u < p$,

$$P_{\infty,u}(G) := \frac{|G|^{\log_p(u)}}{|\operatorname{Aut}(G)|} \left(\tfrac{u}{p}; \tfrac{1}{p}\right)_\infty .$$

Here the q-shifted factorials are defined as

$$(x;q)_i := (1-x)(1-xq)\cdots(1-xq^{i-1}), \quad (x;q)_\infty := \prod_{j=0}^{\infty}(1-xq^j).$$

Friedman and Washington [8] computed the limiting distribution of $\mathrm{Coker}(X)$, where X is a Haar uniform element of $\mathbb{M}_n(\mathbb{Z}_p)$.

Theorem 1.1.1. *[8] Let $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ be Haar-random. Then for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \cong G] = P_{\infty,1}(G).$$

This result gives one of the earliest random matrix realizations of the Cohen-Lenstra distribution. It shows that the weighting by $|\mathrm{Aut}(G)|^{-1}$ arises naturally from the cokernels of Haar-random p-adic matrices.

Wood [24] showed that the same distribution is obtained even if the entries are not Haar-uniform. A random variable $x \in \mathbb{Z}_p$ is called *ϵ-balanced* if for every $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\mathbb{P}[x \equiv a \pmod{p}] < 1-\epsilon.$$

Wood considered random matrices $X \in \mathbb{M}_n(\mathbb{Z}_p)$, whose entries are independent and ϵ-balanced and proved that they have the same limiting cokernel distribution as the Haar-uniform case.

Theorem 1.1.2. *[24] Let $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ be a random matrix whose entries are independent and ϵ-balanced. Then for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \cong G] = P_{\infty,1}(G).$$

Wood [24] also proves a stronger result for rectangular matrices. If $X \in \mathbb{M}_{n,n+u}(\mathbb{Z}_p)$, then X defines a homomorphism $\mathbb{Z}_p^{n+u} \to \mathbb{Z}_p^n$, and its cokernel is denoted by $\operatorname{Coker}(X) := \mathbb{Z}_p^n / \operatorname{Im}(X)$.

Theorem 1.1.3. *[24] Fix a prime p and integer $u \geq 0$. Let $X_n \in \mathbb{M}_{n,n+u}(\mathbb{Z}_p)$ be a random matrix whose entries are independent and ϵ-balanced. Then for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{Coker}(X_n) \cong G] = P_{\infty,p^{-u}}(G).$$

Nguyen and Wood [17] extended this result for matrices over $\mathbb{Z}$, instead of $\mathbb{Z}_p$. If $X \in \mathbb{M}_{n,n+u}(\mathbb{Z})$, then $\operatorname{Coker}(X) = \mathbb{Z}^n / \operatorname{Im}(X)$ is an abelian group. For a fixed prime p, under appropriate hypotheses, the limiting distribution of the p-Sylow subgroup of $\operatorname{Coker}(X)$ can be obtained from Theorem 1.1.3. However, Nguyen and Wood obtain the limiting distribution of $\operatorname{Coker}(X)$, not just its p-Sylow subgroup.

Theorem 1.1.4. *[17] Fix an integer $u \geq 0$ and constants $0 < \epsilon < 1$ and $T > 0$. For each positive integer n, let $\xi_n \in \mathbb{Z}$ be a random integer that is $n^{-1+\epsilon}$-balanced for every prime p and satisfies $|\xi_n| \leq n^T$. Let $X_n \in \mathbb{M}_{n,n+u}(\mathbb{Z})$ be a random matrix whose entries are independent, identically distributed copies of the random integer ξ_n defined above. Then for every finite abelian group B,*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{Coker}(X_n) \cong B] = \frac{1}{|B|^u\,|\operatorname{Aut}(B)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1}.$$

Further, Nguyen and Wood compute the probability for $\operatorname{Coker}(X)$ to be cyclic.

Theorem 1.1.5 (Nguyen and Wood [17])**.** *Fix an integer $u \geq 0$ and constants $0 < \epsilon < 1$ and $T > 0$. For each positive integer n, let $X_n \in \mathbb{M}_{n,n+u}(\mathbb{Z})$ be a random matrix as in*

Theorem 1.1.4. Then,

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \textit{ is cyclic}] = \prod_{p \textit{ prime}} \left(1 - \frac{1}{(p-1)p^{u+1}}\right) \prod_{k=u+1}^{\infty} \zeta(k)^{-1}.$$

There are several further developments of this circle of ideas. Cheong and Kaplan [4] studied cokernels of polynomial expressions $P(A)$, where A is a Haar-random matrix over $\mathbb{Z}_p$. Cheong and Yu [5] proved the ϵ-balanced analogue for cokernels of polynomial expressions $P(A)$. Cheong and Huang [3] studied the distribution of $P(A+pB)$, where P is a polynomial expression, A is a fixed matrix and B is Haar-random. Lee [13] studied the joint distribution of several cokernels of the form $\mathrm{Coker}(P_1(A)), \ldots, \mathrm{Coker}(P_r(A))$, showing that one can study finer questions than the distribution of a single cokernel. Finally, Nguyen and Wood [18] developed a local and global universality theory for more structured random matrix ensembles, including symmetric, skew-symmetric, and Laplacian-type models.

1.1.2 Cokernels of random symmetric matrices

For symmetric matrices, the limiting distributions differ from the Cohen-Lenstra distributions $P_{\infty,u}$. This is because the cokernel of a symmetric matrix naturally carries an additional algebraic structure, namely a canonical symmetric bilinear pairing.

Let $X \in \mathbb{M}_n(\mathbb{Z}_p)$ be symmetric. If X is nonsingular, then $\mathrm{Coker}(X)$ is a finite abelian p-group, and it carries a canonical perfect symmetric bilinear pairing, which we denote by δ_X. If G is a finite abelian p-group equipped with a perfect symmetric bilinear pairing δ, then we denote by $\mathrm{Aut}(G,\delta)$ the group of automorphisms of G preserving δ. We also define

$$P^{\mathrm{Sym}}_{\infty,p}(G) := \frac{|\{\text{symmetric, bilinear, perfect pairings } G \times G \to \mathbb{C}^\times\}|}{|G|\,|\mathrm{Aut}(G)|} \prod_{k\geq 0}(1 - p^{-1-2k}).$$

Clancy, Kaplan, Leake, Payne, and Wood [6] proved that Haar-random symmetric matrices over $\mathbb{Z}_p$ give rise to this distribution. Their result is stated naturally at the level of finite abelian p-groups equipped with perfect symmetric bilinear pairings, and the group-only statement follows by summing over all perfect pairings on a fixed group. Bhargava, Kane, Lenstra, Poonen, and Rains [2] showed an analogous result for cokernels of Haar-random alternating matrices over $\mathbb{Z}_p$.

Theorem 1.1.6. *[6] Let $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ be Haar-random in the additive group of symmetric matrices. Let G be a finite abelian p-group and let δ be a perfect symmetric bilinear pairing on G. Then*

$$\lim_{n\to\infty} \mathbb{P}[(\mathrm{Coker}(X_n), \delta_{X_n}) \cong (G, \delta)] = \frac{1}{|G|\,|\mathrm{Aut}(G,\delta)|} \prod_{k\geq 0}(1 - p^{-1-2k}).$$

In particular,

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

Wood [23] extended this result to random symmetric matrices, whose entries on and below the diagonal are independent and ϵ-balanced. Restricting her result to a single prime p, one obtains the following statement.

Theorem 1.1.7. *[23] Let $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ be a random symmetric matrix, whose entries on and below the diagonal are independent and ϵ-balanced. Then for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

Nguyen and Wood [18] proved global universality results for random symmetric integral matrices. In particular, they computed the limiting probability that the cokernel is cyclic.

Theorem 1.1.8. *[18] Let $X_n \in \mathbb{M}_n(\mathbb{Z})$ be a random symmetric matrix, whose entries on and below the diagonal are independent, identically distributed and ϵ-balanced at every prime p. Then*

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(X_n) \text{ is cyclic}] = \prod_{i=1}^{\infty} \zeta(2i+1)^{-1}.$$

Hodges [11] proved the corresponding result for the distribution of the cokernel along with its pairing.

Theorem 1.1.9. *[11] Fix a prime p. Let $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ be a random symmetric matrix, whose entries on and below the diagonal are independent and ϵ-balanced. Let G be a finite abelian p-group equipped with a perfect symmetric bilinear pairing δ. Then*

$$\lim_{n\to\infty} \mathbb{P}[(\mathrm{Coker}(X_n), \delta_{X_n}) \cong (G, \delta)] = \frac{1}{|G|\,|\mathrm{Aut}(G,\delta)|} \prod_{k\geq 0}(1 - p^{-1-2k}).$$

Shen [20] later reproved this symmetric universality theorem by a different method and obtained effective error bounds.

1.1.3 Sandpile groups of random graphs

Let Γ be a graph on vertices $1, \ldots, n$ without loops. Write $\deg(i,j)$ for the number of edges between i and j, and $\deg(j) = \sum_{i:i\neq j} \deg(i,j)$. Define the Laplacian $L(\Gamma)$ by

$$L_{ij} = \begin{cases} \deg(i,j), & i \neq j, \\ -\deg(j), & i = j, \end{cases}$$

so that $\sum_{i=1}^{n} L_{ij} = 0$ for all j. Let $\mathbb{Z}_0^n$ be the subgroup of $\mathbb{Z}^n$ consisting of vectors whose coordinates sum to 0. Then $\mathrm{Im}(L) \subseteq \mathbb{Z}_0^n$, and the sandpile group of Γ is $S_\Gamma := \mathbb{Z}_0^n / \mathrm{Im}(L)$.

If Γ is connected, then $\operatorname{corank}(L) = 1$ and S_Γ is a finite abelian group.

Similarly, let $\vec{\Gamma}$ be a directed graph on vertices $1, \ldots, n$ without loops. Write $\deg(i, j)$ for the number of directed edges $i \to j$, and set $\deg(j) = \sum_{i:i\neq j} \deg(i, j)$, the in-degree of the vertex j. Define the Laplacian $L(\vec{\Gamma})$ by

$$L_{ij} = \begin{cases} \deg(i, j), & i \neq j, \\ -\deg(j), & i = j, \end{cases}$$

so that again $\sum_{i=1}^n L_{ij} = 0$ for all j. The sandpile group of $\vec{\Gamma}$ is $S_{\vec{\Gamma}} := \mathbb{Z}_0^n / \operatorname{Im}(L)$. If $\vec{\Gamma}$ is strongly connected, then $\operatorname{corank}(L) = 1$ and $S_{\vec{\Gamma}}$ is a finite abelian group.

For undirected Erdős-Rényi graphs, let $G(n, v)$ denote the random graph on n vertices in which each edge is included independently with probability $v \in (0, 1)$. For fixed v, the graph $G(n, v)$ is connected with probability tending to 1 as $n \to \infty$, so $S_{G(n,v)}$ is a finite abelian group with probability tending to 1. Wood [23] proved that the distribution of its Sylow p-subgroups converges to $P^{\mathrm{Sym}}_{\infty,p}$. This is closely related to Theorem 1.1.7. It doesn't directly follow because the columns of the Laplacian matrix sum up to 0. For an abelian group G, we denote its Sylow p-subgroup by $(G)_p$.

Theorem 1.1.10. *[23] Let p be a prime and let G be a finite abelian p-group. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G(n,v)})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

Mészáros [15] proved an analogous result for random d-regular graphs. Suppose $d \geq 3$ and n is even. Let H_n be the random d-regular graph obtained by taking the union of d independent uniform random perfect matchings on the set of n vertices.

Theorem 1.1.11. *[15] Let p be a prime and let G be a finite abelian p-group.*

1. *If d is odd, or if d is even and p is odd, then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{H_n})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

2. *If d is even and $p = 2$, then $(S_{H_n})_2$ always has odd rank, and for every finite abelian 2-group G of odd rank,*

$$\lim_{n\to\infty} \mathbb{P}[(S_{H_n})_2 \cong G] = 2^{\mathrm{rank}(G)} P^{\mathrm{Sym}}_{\infty,2}(G).$$

For directed Erdős-Rényi graphs, let $\vec{G}(n,v)$ denote the random directed graph on n vertices in which each ordered pair $i \to j$ with $i \neq j$ is included independently with probability $v \in (0,1)$. For fixed v, the graph $\vec{G}(n,v)$ is strongly connected with probability tending to 1 as $n \to \infty$, and hence $S_{\vec{G}(n,v)}$ is finite with probability tending to 1. Koplewitz [12] showed that the Sylow p-subgroups converge to the distribution $P_{\infty,1/p}$. Nguyen and Wood [17] extended this result to the distribution of the entire sandpile group. This result is closely related to Theorem 1.1.4.

Theorem 1.1.12. *[17] Fix $0 < v < 1$. Then for every finite abelian group B,*

$$\lim_{n\to\infty} \mathbb{P}[S_{\vec{G}(n,v)} \cong B] = \frac{1}{|B|\,|\mathrm{Aut}(B)|} \prod_{k=2}^{\infty} \zeta(k)^{-1}.$$

In particular, if p is a prime and G is a finite abelian p-group, then

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}(n,v)})_p \cong G] = P_{\infty,1/p}(G).$$

Mészáros [15] also studied random d-regular directed graphs. Suppose $d \geq 3$. Let D_n be the random d-regular directed graph obtained by choosing d independent uniform random permutations $\pi_1, \ldots, \pi_d$ of $\{1, \ldots, n\}$ and, for each $v \in \{1, \ldots, n\}$ and $1 \leq j \leq d$, adding a directed edge from v to $\pi_j(v)$.

Theorem 1.1.13. *[15] Let p be a prime and let G be a finite abelian p-group. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{D_n})_p \cong G] = P_{\infty,1}(G).$$

We now turn to bipartite graphs, which are the main focus of this thesis. Let $n_1 \geq n_2$ be positive integers and let $v \in (0, 1)$. The Erdős-Rényi random bipartite graph $G(n_1, n_2, v)$ is the bipartite graph with vertex sets V_1 and V_2 of sizes n_1 and n_2 respectively, where each of the $n_1 n_2$ possible edges between V_1 and V_2 is included independently with probability v. We are most interested in the regime $n_2 = \lceil \alpha n_1 \rceil$ for a fixed constant $0 < \alpha \leq 1$, and we write $G_\alpha(n, v) := G(n, \lceil \alpha n \rceil, v)$.

Similarly, let $\vec{G}(n_1, n_2, v)$ denote the directed Erdős-Rényi random bipartite graph with vertex sets V_1 and V_2 of sizes n_1 and n_2, where each of the $2n_1n_2$ possible directed edges from V_1 to V_2 and from V_2 to V_1 is included independently with probability $v \in (0, 1)$. Again, in the regime $n_2 = \lceil \alpha n_1 \rceil$, we write $\vec{G}_\alpha(n, v) := \vec{G}(n, \lceil \alpha n \rceil, v)$.

On the directed side, Bhargava, DePascale, and Koenig [1] conjectured that the Sylow p-subgroups of the sandpile groups of $\vec{G}_\alpha(n, v)$ have the same limiting distribution as in the directed Erdős-Rényi case.

Conjecture 1.1.14. *[1] Let p be a prime, let $0 < v < 1$, let $1/p < \alpha \leq 1$, and let G be a finite abelian p-group. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}_\alpha(n,v)})_p \cong G] = P_{\infty,1/p}(G).$$

On the undirected side, the conjectural distribution depends on whether p is odd or $p = 2$.

For odd primes, the conjectured limit is the same distribution $P^{\mathrm{Sym}}_{\infty,p}$ that occurs for ordinary random graphs. For $p = 2$, the conjectured limit is a modified distribution involving the additional factor $|G/2G|/2$.

Conjecture 1.1.15 ([1, 10])**.** *Let p be a prime, let $0 < v < 1$, let $1/p < \alpha \leq 1$, and let G be a finite abelian p-group. Then we have*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G_\alpha(n,v)})_p \cong G] = \begin{cases} P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } p \text{ is odd,} \\ \frac{|G/2G|}{2} P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } p = 2. \end{cases}$$

The main results of this thesis are to prove the directed bipartite conjecture for all primes, and to prove the undirected bipartite conjecture for odd primes.

Theorem 1.1.16. *Let p be a prime, let $0 < v < 1$, let $1/p < \alpha \leq 1$, and let G be a finite abelian p-group. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}_\alpha(n,v)})_p \cong G] = P_{\infty,1/p}(G).$$

Theorem 1.1.17. *Let p be an odd prime, let $0 < v < 1$, let $1/p < \alpha \leq 1$, and let G be a finite abelian p-group. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G_\alpha(n,v)})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

It is also natural to study the ranks of these Sylow p-subgroups. If G is a finite abelian p-group, we define its rank by $\operatorname{rank}(G) := \log_p |G/pG|$.

On the directed side, Bhargava, DePascale, and Koenig [1] determined the limiting distribution of the p-ranks of the sandpile groups of random directed bipartite graphs. It is shown in [10] that this is consistent with Theorem 1.1.16.

Theorem 1.1.18. *[1] Let p be a prime, let $0 < v < 1$, let $1/p < \alpha \leq 1$, and let r be a nonnegative integer. Then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{\vec{G}_\alpha(n,v)})_p) = r] = \frac{1}{p^{r^2+r}} \left(p^{-r-2}; p^{-1}\right)_\infty \left(p^{-1}; p^{-1}\right)_r.$$

On the undirected side, the conjectural limiting distribution of the p-rank depends on whether p is odd or equal to 2.

Conjecture 1.1.19. *[10] Let p be a prime, let $1/p < \alpha \leq 1$, and let r be a nonnegative integer. Then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G_\alpha(n,v)})_p) = r] = \begin{cases} \dfrac{1}{(-p^{-1}; p^{-1})_\infty \, p^{\binom{r+1}{2}} \, (p^{-1}; p^{-1})_r} & \text{if } p \text{ is odd,} \\ \dfrac{1}{(-1; 1/2)_\infty \, 2^{\binom{r}{2}} \, (1/2; 1/2)_r} & \text{if } p = 2. \end{cases}$$

In Chapter 3, we prove this conjecture for all primes including $p = 2$.

Theorem 1.1.20. *Let p be a prime, let $1/p < \alpha \leq 1$, and let r be a nonnegative integer. Then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G_\alpha(n,v)})_p) = r] = \begin{cases} \dfrac{1}{(-p^{-1}; p^{-1})_\infty \, p^{\binom{r+1}{2}} \, (p^{-1}; p^{-1})_r} & \text{if } p \text{ is odd,} \\ \dfrac{1}{(-1; 1/2)_\infty \, 2^{\binom{r}{2}} \, (1/2; 1/2)_r} & \text{if } p = 2. \end{cases}$$

For odd primes, the undirected rank theorem also follows from Theorem 1.1.17 together with the known rank distribution of a random finite abelian p-group distributed according to $P^{\mathrm{Sym}}_{\infty,p}$. The case $p = 2$ gives additional evidence for the conjectural distribution of the full

2-Sylow subgroup.

Chapter 2 is a copy of [22] and is dedicated to proving Theorem 1.1.16. Chapter 3 is a copy of [21] and is dedicated to proving Theorem 1.1.17 and Theorem 1.1.20.

1.2 Method of moments

1.2.1 Surjective moments

Let X be a random finite abelian p-group. For a finite abelian p-group G, let $\mathrm{Sur}(X, G)$ denote the set of surjective homomorphisms from X to G. The *surjective G-moment* of X is $\mathbb{E}[|\mathrm{Sur}(X, G)|]$. The method of moments studies the distribution of a random finite abelian p-group by computing these surjective moments.

The surjective moments of $P_{\infty,u}$ were computed by Fulman and Kaplan [9].

Theorem 1.2.1. *[9, Theorem 5.3] Suppose $0 < u < p$, and let X be a random finite abelian p-group distributed according to $P_{\infty,u}$. Then for every finite abelian p-group G,*

$$\mathbb{E}[|\mathrm{Sur}(X, G)|] = |G|^{\log_p(u)}.$$

In particular, for the distribution $P_{\infty,1/p}$ that occurs in the directed bipartite problem, one has $\mathbb{E}[|\mathrm{Sur}(X, G)|] = \frac{1}{|G|}$.

The surjective moments of $P^{\mathrm{Sym}}_{\infty,p}$ were computed by Clancy, Kaplan, Leake, Payne, and Wood [6]. In the result

$$\Lambda^2 G := (G \otimes G)/\langle g \otimes g : g \in G\rangle.$$

Theorem 1.2.2. *[6, Theorem 11] Suppose p is a prime, and let X be a random finite abelian*

p-group distributed according to $P^{\mathrm{Sym}}_{\infty,p}$. Then for every finite abelian p-group G,

$$\mathbb{E}[|\mathrm{Sur}(X,G)|] = \left|\Lambda^2 G\right|.$$

In the undirected bipartite problem at $p = 2$, the conjectured measure belongs to a larger family of measures that was defined in [10]. For a prime p and a parameter $-1 \leq a \leq 1$, they define the measure $P^{M,1}_{p,a}$ on finite abelian p-groups as

$$P^{M,1}_{p,a}(G) := \begin{cases} \frac{1-a}{2} p^{\mathrm{rank}(G)} P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } \mathrm{rank}(G) \text{ is odd,} \\ \frac{1+a}{2} p^{\mathrm{rank}(G)} P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } \mathrm{rank}(G) \text{ is even.} \end{cases}$$

The superscript M is for Mészáros. In particular, $P^{M,1}_{p,-1}$ occurs in the distribution of sandpile groups of random d-regular graphs when d is even and $p = 2$, while $P^{M,1}_{p,0}$ is the conjectural distribution for Sylow 2-subgroups of sandpile groups of random bipartite graphs.

The surjective moments of $P^{M,1}_{p,a}$ were computed in [10].

Theorem 1.2.3. *[10, Theorem 9] Suppose p is a prime, $-1 \leq a \leq 1$, and let X be a random finite abelian p-group distributed according to $P^{M,1}_{p,a}$. Then for every finite abelian p-group G,*

$$\mathbb{E}[|\mathrm{Sur}(X,G)|] = p^{\mathrm{rank}(G)} \left|\Lambda^2 G\right|.$$

In particular, these moments do not depend on a.

Several of the distribution results cited in the previous section are proved by first computing the surjective moments of the relevant random groups. More precisely, if X_n is a sequence of random finite abelian p-groups and ν is the conjectured limiting distribution, one shows that for every finite abelian p-group G, $\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(X_n,G)|]$ agrees with the corresponding surjective moment of ν. The following theorems record these moment computations.

Wood [23] proved that if X_n is the sandpile group of an Erdős-Rényi random graph, then its limiting surjective moments are given by $|\Lambda^2 G|$.

Theorem 1.2.4. *[23, Theorem 1.2] Let $\Gamma \in G(n, v)$ be an Erdős-Rényi random graph, and let S_Γ be its sandpile group. Then for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}((S_\Gamma)_p, G)|] = \left|\Lambda^2 G\right|.$$

Wood [24] proved the analogous moment formula for cokernels of random matrices.

Theorem 1.2.5. *[24, Theorem 2.9] Let $u \geq 0$ be an integer. Let $M_n \in \mathbb{M}_{n,n+u}(\mathbb{Z}_p)$ be a random matrix whose entries are independent and ϵ-balanced. Then for every finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(M_n), G)|] = |G|^{-u}.$$

Mészáros [15] proved analogous moment formulas for sandpile groups of random regular graphs.

Theorem 1.2.6. *[15, Theorems 1.3 and 1.4] Let Γ_n be the sandpile group of the random d-regular directed graph D_n, and let S_n be the sandpile group of the random d-regular graph H_n.*

1. *For every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}((\Gamma_n)_p, G)|] = 1.$$

2. For every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}((S_n)_p, G)|] = \begin{cases} |\Lambda^2 G| & \text{if } d \text{ is odd or } p \text{ is odd,} \\ 2^{\mathrm{rank}(G)}\,|\Lambda^2 G| & \text{if } d \text{ is even and } p = 2. \end{cases}$$

A slight variation appears in Hodges [11], where the random objects are finite abelian p-groups equipped with symmetric pairings, and one counts surjections preserving the pairings. The set of pairing-preserving surjections is denoted by Sur^*.

Theorem 1.2.7. *[11, Theorem 8.2] Let $\Gamma \in G(n,v)$ be an Erdős-Rényi random graph, let S_Γ be its sandpile group, and let δ_{S_Γ} be its canonical symmetric pairing. Let G be a finite abelian p-group equipped with a symmetric pairing δ on its dual. Then*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}^*((S_\Gamma, \delta_{S_\Gamma}), (G,\delta))|] = |G|^{-1}.$$

Related moment computations for random finite abelian p-groups equipped with additional algebraic structure also appear in work of Lipnowski, Sawin, and Tsimerman [14].

1.2.2 Moments on high probability subsets

In the case of bipartite graphs, for both the directed and undirected cases, the method of moments does not apply directly. Indeed, the surjective moments often blow up to infinity, even though the conjectured limiting distributions have finite surjective moments. See Section 2.7 and Section 3.8.

The reason is that a small exceptional set of graphs contributes negligibly to the distribution, but contributes disproportionately to the surjective moments. Recall that we have two sets of vertices V_1 of size n and V_2 of size $\lceil \alpha n \rceil$. In both the directed and undirected bipartite settings, the exceptional set consists of graphs for which too many vertices in V_1 have degree divisible by p. The remedy is to restrict attention to the complement of this exceptional set of graphs and compute the conditional surjective moments there. Since the exceptional set has probability tending to 0, conditioning on its complement does not change the limiting distribution.

The graphs that we are trying to exclude are those for which the number of vertices in V_1 with degree divisible by p is larger than $|V_2| = \lceil \alpha n \rceil$. In particular, if $\alpha = 1$, then we do not need to exclude any of the graphs. In fact, the issue of the moments blowing up only arises when $\alpha < 1$.

We first consider the directed bipartite model. Let $\vec{G}_\alpha(n, v)$ be the directed Erdős-Rényi random bipartite graph with bipartition (V_1, V_2), where $|V_1| = n$ and $|V_2| = \lceil \alpha n \rceil$. For a directed bipartite graph $\vec{\Gamma}$ with this bipartition, define

$$\gamma(\vec{\Gamma}) := \left| \{ x \in V_1 : \deg_{\vec{\Gamma}}(x) \equiv 0 \pmod{p} \} \right|,$$

where $\deg_{\vec{\Gamma}}(x)$ denotes the in-degree of the vertex x. For $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$, define the good subset

$$\mathcal{E}^{\mathrm{dir}}_{n,\rho} := \left\{ \vec{\Gamma} : \left| \gamma(\vec{\Gamma}) - \frac{n}{p} \right| \le \rho n \right\}.$$

We will show the following in Chapter 2.

Theorem 1.2.8. *Let p be a prime, $0 < v < 1$, $1/p < \alpha \le 1$, and $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$. Then*

$$\lim_{n \to \infty} \mathbb{P}[\vec{G}_\alpha(n, v) \in \mathcal{E}^{\mathrm{dir}}_{n,\rho}] = 1.$$

Moreover, for every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{E}\Big[\Big|\mathrm{Sur}((S_{\vec{G}_\alpha(n,v)})_p, G)\Big| \;\Big|\; \vec{G}_\alpha(n,v) \in \mathcal{E}^{\mathrm{dir}}_{n,\rho}\Big] = \frac{1}{|G|}.$$

Thus, after conditioning on the event $\mathcal{E}^{\mathrm{dir}}_{n,\rho}$, the surjective moments agree with the moments of the distribution $P_{\infty,1/p}$.

We now turn to the undirected bipartite model. Let $G_\alpha(n,v)$ be the Erdős-Rényi random bipartite graph with bipartition (V_1, V_2), where $|V_1| = n$ and $|V_2| = \lceil \alpha n \rceil$. For such a graph Γ, define

$$\gamma(\Gamma) := \left|\{x \in V_1 : \deg_\Gamma(x) \equiv 0 \pmod{p}\}\right|.$$

For $0 < \rho < \alpha - \frac{1}{p}$, define the good subset

$$\mathcal{E}^{\mathrm{und}}_{n,\rho} := \left\{\Gamma : \gamma(\Gamma) < \left(\frac{1}{p} + \rho\right) n\right\}.$$

Theorem 1.2.9. *Let p be a prime, $0 < v < 1$, $1/p < \alpha \le 1$, and $0 < \rho < \alpha - \frac{1}{p}$. Then*

$$\lim_{n\to\infty} \mathbb{P}[G_\alpha(n,v) \in \mathcal{E}^{\mathrm{und}}_{n,\rho}] = 1.$$

Moreover, for every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{E}\big[\big|\mathrm{Sur}((S_{G_\alpha(n,v)})_p, G)\big| \;\big|\; G_\alpha(n,v) \in \mathcal{E}^{\mathrm{und}}_{n,\rho}\big] = \begin{cases} |\Lambda^2 G| & \text{if } p \text{ is odd,} \\ |G/pG|\;|\Lambda^2 G| & \text{if } p = 2. \end{cases}$$

Therefore, once one works on the high-probability subsets $\mathcal{E}^{\mathrm{dir}}_{n,\rho}$ and $\mathcal{E}^{\mathrm{und}}_{n,\rho}$, the surjective moments are exactly what one would expect based on the conjectured distributions. This is the key step that allows the method of moments to be applied in our setting.

1.2.3 Moments determine the distribution

A natural question is whether the surjective moments determine the distribution of a random finite abelian p-group. Ellenberg, Venkatesh, and Westerland [7] showed that the Cohen–Lenstra distribution $P_{\infty,1}$ is characterized by having all surjective moments equal to 1. Wood [23] showed that the surjective moments determine the distribution, provided the moments are not too large.

Theorem 1.2.10. *[23, Theorem 8.2] Let X_n be a sequence of random finite abelian p-groups and let Y be another random finite abelian p-group such that for every finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(X_n, G)|] = \mathbb{E}[|\mathrm{Sur}(Y, G)|] \leq \left|\Lambda^2 G\right|.$$

Then for every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{P}[X_n \cong G] = \mathbb{P}[Y \cong G].$$

This theorem explains why the moment computations in the previous subsection lead to the distribution results stated earlier. Indeed, by Theorem 1.2.1, the surjective moments of $P_{\infty,1}$ are equal to 1, and the surjective moments of $P_{\infty,1/p}$ are equal to $|G|^{-1}$; both of these are bounded above by $|\Lambda^2 G|$. Therefore, once one proves that a sequence of random finite abelian p-groups has limiting surjective moments equal to 1 or $|G|^{-1}$, Theorem 1.2.10 implies convergence in distribution to $P_{\infty,1}$ or $P_{\infty,1/p}$ respectively. This applies, for example, to the cokernels of random matrices considered by Wood [24], to the sandpile groups of random directed regular graphs considered by Mészáros [15] and the directed bipartite result proved in Chapter 2.

Similarly, by Theorem 1.2.2, the surjective moments of $P^{\mathrm{Sym}}_{\infty,p}$ are exactly $|\Lambda^2 G|$. Hence Theorem 1.2.10 also implies convergence in distribution to $P^{\mathrm{Sym}}_{\infty,p}$ once one has shown that $\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(X_n, G)|] = |\Lambda^2 G|$ for every finite abelian p-group G. This is the mechanism behind Wood's [23] result for Erdős-Rényi random graphs, the odd-p and odd-d cases of Mészáros's [15] theorem for random regular graphs and the odd-prime undirected bipartite result proved in Chapter 3.

A much more general framework for such questions was later developed by Sawin and Wood [19], who studied moment problems for random objects in a category.

However, this argument breaks down for the moment sequence $p^{\mathrm{rank}(G)}\,|\Lambda^2 G|$. Indeed, Theorem 1.2.3 shows that the one-parameter family of measures $P^{M,1}_{p,a}$, with $-1 \le a \le 1$, all have the same surjective moments. Thus these moments are too large for the analogue of Theorem 1.2.10 to hold. In particular, the moments alone are not enough to identify the conjectural distribution of Sylow 2-subgroups in the undirected bipartite setting.

Although these moments do not determine the full distribution, Wood proved that after adding one extra piece of information, namely the limiting probability that the rank is odd, they do determine the limiting distribution of the ranks.

Theorem 1.2.11. *[25, Corollary 2.12] Let X_n be a sequence of random finite abelian p-groups such that for every $k \in \mathbb{Z}_{\ge 0}$,*

$$\lim_{n\to\infty} \mathbb{E}[\left|\mathrm{Sur}(X_n, (\mathbb{Z}/p\mathbb{Z})^k)\right|] = p^k \left|\Lambda^2(\mathbb{Z}/p\mathbb{Z})^k\right|.$$

Assume moreover that there is a constant $v \in [0,1]$ such that

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{rank}(X_n) \textit{ is odd}] = v.$$

Then for every $r \in \mathbb{Z}_{\geq 0}$,

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}(X_n) = r] = \begin{cases} 2v\frac{1}{(-1;p^{-1})_\infty}p^{-\binom{r}{2}}\frac{1}{(p^{-1};p^{-1})_r} & \text{if } r \text{ is odd,} \\ 2(1-v)\frac{1}{(-1;p^{-1})_\infty}p^{-\binom{r}{2}}\frac{1}{(p^{-1};p^{-1})_r} & \text{if } r \text{ is even.} \end{cases}$$

Based on this, we should expect that in the undirected bipartite setting with $p = 2$, the probability of odd rank goes to $\frac{1}{2}$. We show that this is indeed the case.

Theorem 1.2.12. *Suppose $p = 2$, $0 < v < 1$ and $1/2 < \alpha \leq 1$. Then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G_\alpha(n,v)})_2) \text{ is odd}] = \frac{1}{2}.$$

This leads to the distribution of the rank of Sylow 2-subgroups in the undirected bipartite setting, as shown in Chapter 3.

A related result was proved by Mészáros in the case of random regular graphs. His theorem shows that if one restricts attention to finite abelian 2-groups of odd rank, then the moments $2^{\operatorname{rank}(G)} |\Lambda^2 G|$ do determine the limiting distributions.

Theorem 1.2.13. *[15, Theorem 8.7] Suppose X_n is a sequence of random finite abelian 2-groups of odd rank, such that for every finite abelian 2-group G,*

$$\lim_{n\to\infty} \mathbb{E}[|\operatorname{Sur}(X_n, G)|] = 2^{\operatorname{rank}(G)} \left|\Lambda^2 G\right|.$$

Then for every finite abelian 2-group G, we have

$$\lim_{n\to\infty} \mathbb{P}[X_n \cong G] = P^{M,1}_{2,-1}(G) = \begin{cases} 2^{\operatorname{rank}(G)} P^{\mathrm{Sym}}_{\infty,2}(G) & \text{if } \operatorname{rank}(G) \text{ is odd,} \\ 0 & \text{if } \operatorname{rank}(G) \text{ is even.} \end{cases}$$

We suspect the following.

Conjecture 1.2.14. *Let X_n be a sequence of random finite abelian p-groups such that for every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(X_n, G)|] = p^{\mathrm{rank}(G)} \left|\Lambda^2(\mathbb{Z}/p\mathbb{Z})^k\right|.$$

Assume moreover that there is a constant $v \in [0,1]$ such that

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{rank}(X_n) \text{ is odd}] = v.$$

Then for every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{P}[X_n \cong G] = P^{M,1}_{2,1-2v}(G) = \begin{cases} v2^{\mathrm{rank}(G)} P^{\mathrm{Sym}}_{\infty,2}(G) & \text{if } \mathrm{rank}(G) \text{ is odd,} \\ (1-v)2^{\mathrm{rank}(G)} P^{\mathrm{Sym}}_{\infty,2}(G) & \text{if } \mathrm{rank}(G) \text{ is even.} \end{cases}$$

If this is true, then the $p = 2$ case of Conjecture 1.1.15 would follow from the work in Chapter 3.

1.3 Wood's moment computations

In this section, we sketch two moment computations due to Wood that are most relevant to this thesis. The first concerns cokernels of random rectangular matrices and leads to the Cohen-Lenstra type distributions that appear in the directed setting. The second concerns sandpile groups of random graphs and leads to the symmetric distribution that appears in the undirected setting. The purpose of this section is to explain, at a heuristic level, the main ideas in these two arguments before turning to the bipartite models in Chapter 2 and Chapter 3.

1.3.1 The directed case in Wood's argument

We will sketch Wood's proof of Theorem 1.2.5 in [24]. Suppose $X_n \in \mathbb{M}_{n,n+u}(\mathbb{Z}_p)$ is a random matrix whose entries are independent and ϵ-balanced. Fix a finite abelian p-group G. We want to estimate the expected number of surjections $\mathrm{Coker}(X_n) \twoheadrightarrow G$. Since X_n is a map $\mathbb{Z}_p^{n+u} \to \mathbb{Z}_p^n$, every surjection $\mathrm{Coker}(X_n) \twoheadrightarrow G$ lifts to a surjection from $\mathbb{Z}_p^n$ to G. Thus,

$$\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|] = \sum_{F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)} \mathbb{P}[F \circ X_n = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n+u}, G)].$$

Since the columns of X_n are independent, the probability $\mathbb{P}[F \circ X_n = 0]$ factors into a product of single-column probabilities. If we denote the i-th column vector of X_n as $X_n(i)$, then

$$\mathbb{P}[F \circ X_n = 0] = \prod_{i=1}^{n+u} \mathbb{P}[F \circ X_n(i) = 0].$$

If the entries of X_n were Haar-uniform, then each $F \circ X_n(i)$ would be uniformly distributed in G and $\mathbb{P}[F \circ X_n(i) = 0] = \frac{1}{|G|}$. This would mean $\mathbb{P}[F \circ X_n = 0] = \frac{1}{|G|^{n+u}}$. Since $\left|\mathrm{Sur}(\mathbb{Z}_p^n, G)\right| = |G|^n (1 - o(1))$, this would imply

$$\lim_{n \to \infty} \mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|] = \lim_{n \to \infty} |G|^n (1 - o(1)) \frac{1}{|G|^{n+u}} = \frac{1}{|G|^u}.$$

When the entries of X_n are only given to be ϵ-balanced, not Haar-uniform, then $F \circ X_n(i)$ need not be uniformly distributed in G. However, Wood shows that for most surjections $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$, the random variable $F \circ X_n(i)$ is close to uniformly distributed in G.

To simplify the notation, let X be a random column vector $X \in \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}_p^n)$, whose entries are independent and ϵ-balanced. Denote $[n] = \{1, \dots, n\}$. Let $e_1, \dots, e_n$ be the standard basis of $V = \mathbb{Z}_p^n$. Given a subset $\sigma \subseteq [n]$, let V_σ be the $\mathbb{Z}_p$-submodule of V generated by e_i for $i \in \sigma$ and $V_{\setminus \sigma}$ is generated by e_i for $i \in [n] \setminus \sigma$.

Wood introduces the notion of a code of distance d.

Definition 1.3.1. [24] A surjection $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ is called a code of distance d with image G, if for every subset $\sigma \subseteq [n]$ with $|\sigma| < d$, we have $F(V_{\setminus\sigma}) = G$.

This means that, not only is F surjective, but it remains surjective after deleting fewer than d coordinates. Using discrete Fourier analysis, she proves that if F is such a code of distance δn with image G, then $\mathbb{P}[F(X) = A] \approx \frac{1}{|G|}$ uniformly in $A \in G$, with exponentially small error. It follows that for these F the probability $\mathbb{P}[F \circ X_n = 0]$ is close to $|G|^{-(n+u)}$.

Wood shows that for fixed $\delta > 0$, most $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ are codes of distance δn with image G. Therefore, their combined contribution to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ is close to $\frac{1}{|G|^u}$. It remains to bound the contributions of the surjections F which are not codes of distance δn.

For this, Wood introduces the δ-depth of F.

Definition 1.3.2. Given $\delta > 0$ and $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$, the δ-depth of F is defined to be the largest positive integer D for which there is a subset $\sigma \subseteq [n]$ with $|\sigma| < \log_p(D)\delta n$ such that $[G : F(V_{\setminus\sigma})] = D$, or 1 if there is no such σ.

If such a σ exists, then we say that F is of δ-type $(G, F(V_{\setminus\sigma}))$. If there is no such σ, then we set the δ-type to be (G, G).

It is noted in [24, Remark 2.5] that if F has δ-depth 1, then it is a code of distance δn.

Suppose H is a subgroup of G with $[G : H] = D > 1$. Consider $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ of δ-type (G, H). Consider $\sigma = \{i : F(e_i) \notin H\}$. So $\sigma \neq \emptyset$ and $F(V_{\setminus\sigma}) = H$. Let F_σ and $F_{\setminus\sigma}$ be the restrictions of F to V_σ and $V_{\setminus\sigma}$ respectively. Then we can see from the definition of δ-depth that $F_{\setminus\sigma} \in \mathrm{Sur}(V_{\setminus\sigma}, H)$ is a code of distance δn with image H. We can similarly divide X

into X_σ and $X_{\backslash\sigma}$. Note that $X_{\backslash\sigma}$ is independent of X_σ. Therefore,

$$\begin{aligned}\mathbb{P}[F(X)=0] &= \mathbb{P}[F_{\backslash\sigma}(X_{\backslash\sigma}) = -F_\sigma(X_\sigma)] \\ &= \mathbb{P}[F_{\backslash\sigma}(X_{\backslash\sigma}) = -F_\sigma(X_\sigma) \mid F_\sigma(X_\sigma) \in H] \times \mathbb{P}[F_\sigma(X_\sigma) \in H].\end{aligned}$$

Since $F_{\backslash\sigma} \in \mathrm{Sur}(V_{\backslash\sigma}, H)$ is a code of distance δn with image H, we know that $F_{\backslash\sigma}(X_{\backslash\sigma})$ is close to being uniformly distributed in H, meaning

$$\mathbb{P}[F_{\backslash\sigma}(X_{\backslash\sigma}) = -F_\sigma(X_\sigma) \mid F_\sigma(X_\sigma) \in H] \approx \frac{1}{|H|}.$$

Moreover, since $\sigma \neq \emptyset$, the condition $F_\sigma(X_\sigma) \in H$ is non-trivial. Since the entries of X are ϵ-balanced, it follows that $\mathbb{P}[F_\sigma(X_\sigma) \in H] \le 1-\epsilon$, see [24]. Without being rigorous about the error terms, this implies that if F is of δ-type (G, H), then

$$\mathbb{P}[F \circ X_n = 0] \le \frac{1}{|H|^{n+u}}(1-\epsilon)^{n+u}(1+o(1)).$$

In order to bound the total contribution to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ of F of δ-type (G, H), we need to bound the number of $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ of δ-type (G, H). For each such F, there is a $\sigma \subseteq [n]$ with $|\sigma| < \log_p(D)\delta n \le \log_p(|G|)\delta n$ such that $F(V_{\backslash\sigma}) \subseteq H$.

By expanding σ, we can assume that $|\sigma| = \lfloor \log_p(|G|)\delta n \rfloor$. So the number of choices for σ is at most $\exp(O(\delta n))$. Once σ is chosen then the number of choices for F is at most

$$|H|^{n-|\sigma|}\,|G|^{|\sigma|} = |H|^n \exp(O(\delta n)).$$

Therefore, total contribution to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ of F of δ-type (G, H) is at most

$$\frac{(1-\epsilon)^u(1+o(1))}{|H|^u}(1-\epsilon)^n \exp(O(\delta n)).$$

We can choose a sufficiently small δ to ensure that this goes to 0 as $n \to \infty$.

Wood uses these estimates to show that the combined contribution of non-codes to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ goes to 0 as $n \to \infty$. Since the combined contribution of codes of distance δn goes to $\frac{1}{|G|^u}$, it follows that

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|] = \frac{1}{|G|^u}.$$

1.3.2 The undirected case in Wood's argument

We now sketch Wood's computation of moments in [23]. Suppose $X_n \in \mathbb{M}_n(\mathbb{Z}_p)$ is a random symmetric matrix whose entries on and below the diagonal are independent and ϵ-balanced. Fix a finite abelian p-group G. We want to estimate the expected number of surjections $\mathrm{Coker}(X_n) \twoheadrightarrow G$. Note that the Laplacian of a graph is a bit different from X_n, since the columns of the Laplacian sum up to 0. However, they have the same surjective moments as $n \to \infty$ and the moments of the sandpile group are computed using the X_n model.

Since X_n is a map $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$, every surjection $\mathrm{Coker}(X_n) \twoheadrightarrow G$ lifts to a surjection from $\mathbb{Z}_p^n$ to G. Thus,

$$\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|] = \sum_{F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)} \mathbb{P}[F \circ X_n = 0 \in \mathrm{Hom}(\mathbb{Z}_p^n, G)].$$

So, as in Wood's argument for rectangular random matrices, the moment computation is reduced to understanding the probability that a fixed surjection F kills the random matrix. Wood again divides the surjections $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ into codes and non-codes and further divides the non-codes based on δ-depth.

For $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ that are codes of distance δn with image G, Wood shows that

$$\mathbb{P}[F \circ X_n = 0 \in \mathrm{Hom}(\mathbb{Z}_p^n, G)] \approx \frac{|\Lambda^2 G|}{|G|^n}. \tag{1.1}$$

Moreover, for any $F' \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ (still assuming F is a code), she shows that

$$\mathbb{P}[F \circ X_n = F'] \leq K \frac{1}{|G|^n}, \tag{1.2}$$

for some constant K. We will sketch the proof of (1.1). The proof of (1.2) is similar.

The difference from the directed case is that here X_n is symmetric, so its columns are not independent of each other. Thus, we cannot write the probability $\mathbb{P}[F \circ X_n = 0]$ as a product of probabilities over individual columns. Instead Wood applies discrete Fourier analysis to the indicator of the event $F \circ X_n = 0$.

Let $G^* := \mathrm{Hom}(G, \mathbb{C}^\times)$ be the group of characters of G. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{Z}_p^n$. By discrete Fourier analysis, we know that

$$\mathbb{1}_{(F \circ X_n)(e_i)=0} = \frac{1}{|G|} \sum_{\phi \in G^*} \phi((F \circ X_n)(e_i)).$$

Therefore,

$$\mathbb{P}[F \circ X_n = 0] = \mathbb{E}\left[\prod_{i=1}^n \mathbb{1}_{(F \circ X_n)(e_i)=0}\right] = \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)} \mathbb{E}\left[\prod_{i=1}^n C(e_i)(F \circ X_n(e_i))\right].$$

Denote the entries of X_n on and below the diagonal as x_{ij}, with $1 \leq j \leq i \leq n$. Since X_n is symmetric, we have

$$\prod_{i=1}^n C(e_i)(F \circ X_n(e_i)) = \prod_{1 \leq j < i \leq n} \Big(C(e_i)(F(e_j)) C(e_j)(F(e_i))\Big)^{x_{ij}} \prod_{1 \leq i \leq n} \Big(C(e_i)(F(e_i))\Big)^{x_{ii}}.$$

This leads her to denote the coefficients

$$E[C,F](i,j) = \begin{cases} C(e_i)(F(e_j))C(e_j)(F(e_i)) & \text{if } i \neq j, \\ C(e_i)(F(e_i)) & \text{if } i = j. \end{cases}$$

Since the x_{ij} are independent, we see that

$$\mathbb{P}[F \circ X_n = 0] = \frac{1}{|G|^n} \sum_{C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)} \prod_{1 \leq j \leq i \leq n} \mathbb{E}\Big[E[C,F](i,j)^{x_{ij}}\Big].$$

If the x_{ij} were Haar-uniform in $\mathbb{Z}_p$, then we would have

$$\mathbb{E}\Big[E[C,F](i,j)^{x_{ij}}\Big] = \begin{cases} 1 & \text{if } E[C,F](i,j) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

This would imply

$$\mathbb{P}[F \circ X_n = 0] = \frac{\big|\{C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*) : \text{all } E[C,F](i,j) = 1\}\big|}{|G|^n}.$$

The $C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)$, such that all $E[C,F](i,j) = 1$ are called F-special. Wood shows that for each $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$, the number of F-special C is $|\Lambda^2 G|$. Therefore, if the x_{ij} were Haar-uniform, then (1.1) would be an exact equality.

If the x_{ij} are only assumed to be ϵ-balanced, not Haar-uniform, then the combined contribution of F-special C to $\mathbb{P}[F \circ X_n = 0]$ is still $\frac{|\Lambda^2 G|}{|G|^n}$. Therefore, we need to show that the combined contribution of the C that are not F-special is small.

Wood shows the following.

Lemma 1.3.3. *[23, Lemma 4.2] If $\xi \neq 1$ is a p^m-th root of unity and $x \in \mathbb{Z}_p$ is ϵ-balanced,*

then

$$|\mathbb{E}[\xi^x]| \leq \exp\left(-\frac{\epsilon}{p^{2m}}\right).$$

This lemma implies that

$$\left|\prod_{1\leq j\leq i\leq n} \mathbb{E}\Big[E[C,F](i,j)^{x_{ij}}\Big]\right| \leq \exp\left(-\frac{\epsilon}{|G|^2} \times |\{(i,j) : E[C,F](i,j) \neq 1\}|\right).$$

The C that are not F-special will have at least one coefficient $E[C,F](i,j)$ that is not 1. If a large number of the coefficients are not 1, then that C will have a small contribution.

If F is a code of distance δn with image G, then Wood partitions $\mathrm{Hom}(\mathbb{Z}_p^n, G^*)$ into those C that are (γ, F)-robust and those that are not (γ, F)-robust. Here $\gamma > 0$, is an independent parameter to δ. She shows the following.

1. Most $C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)$ are (γ, F)-robust. The number of C that are not (γ, F)-robust is at most $\exp(O(\gamma n))$.

2. If $C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)$ is (γ, F)-robust, then the number of coefficients $E[C,F](i,j)$ that are not 1 is at least $\Omega(\gamma\delta n^2)$. In particular, C is not F-special. Here, the Ω notation means bounded below by a positive constant times $\gamma\delta n^2$.

3. If $C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)$ is not F-special, then the number of coefficients $E[C,F](i,j)$ that are not 1 is at least $\Omega(\delta n)$.

By point 2, the combined contribution of C that are (γ, F)-robust is at most

$$\frac{1}{|G|^n} |G|^n \exp(-\Omega(\epsilon\gamma\delta n^2)) = \exp(-\Omega(\epsilon\gamma\delta n^2)).$$

By points 1 and 3, the combined contribution of C that are not (γ, F)-robust and not F-

special is at most

$$\frac{1}{|G|^n}\exp(O(\gamma n))\exp(-\Omega(\epsilon\delta n)).$$

Thus, the combined contribution of $C \in \mathrm{Hom}(\mathbb{Z}_p^n, G^*)$ that are not F-special is at most

$$\frac{1}{|G|^n}\Big(\,|G|^n \exp\big(-\Omega(\epsilon\gamma\delta n^2)\big)+\exp\big(O(\gamma n)-\Omega(\epsilon\delta n)\big)\Big).$$

We can choose a sufficiently small $\gamma > 0$, so that this is $\frac{1}{|G|^n}o(1)$. By including the contribution of C that are F-special, it will follow that

$$\mathbb{P}[F \circ X_n = 0 \in \mathrm{Hom}(\mathbb{Z}_p^n, G)] = \frac{1}{|G|^n}\Big(\left|\Lambda^2 G\right| + o(1)\Big),$$

which is stronger than (1.1).

This is true for all F that are codes of distance δn with image G. The number of F that are codes is $|G|^n\,(1-o(1))$. Therefore, the combined contribution of codes to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ is

$$|G|^n\,(1-o(1))\frac{1}{|G|^n}\Big(\left|\Lambda^2 G\right| + o(1)\Big) \to \left|\Lambda^2 G\right|.$$

The only thing that is left is to show that the combined contribution of F that are not codes goes to 0. Fix such an F, and suppose its δ-type is (G, H), where H is a proper subgroup of G and $[G : H] = D > 1$. Define

$$\sigma = \{i \in [n] : F(e_i) \notin H\}, \qquad \tau = \{i \in [n] : F(e_i) \in H\}.$$

Thus $\sigma \sqcup \tau = [n]$. By reordering the basis vectors if necessary, we may assume that the indices in σ come first and the indices in τ come last.

Let V_σ and V_τ be the submodules of $\mathbb{Z}_p^n$ generated by $\{e_i : i \in \sigma\}$ and $\{e_i : i \in \tau\}$ respectively. Let

$$F_\sigma := F|_{V_\sigma} \in \mathrm{Hom}(V_\sigma, G), \qquad F_\tau := F|_{V_\tau} \in \mathrm{Hom}(V_\tau, H).$$

By the definition of δ-type, we know that $|\sigma| < \log_p(D)\delta n$ and it can be shown that F_τ is a code of distance δn with image H. Since $H \subsetneq G$, we know that $\sigma \neq \emptyset$.

We now write the symmetric matrix X_n in block form as

$$X_n = \begin{bmatrix} X_{\sigma,\sigma} & X_{\sigma,\tau} \\ X_{\tau,\sigma} & X_{\tau,\tau} \end{bmatrix}.$$

We know that $X_{\tau,\sigma} = X_{\sigma,\tau}^T$ and that $X_{\sigma,\sigma}$ and $X_{\tau,\tau}$ are symmetric.

The condition $F \circ X_n = 0$ means that $F_\sigma \circ X_{\sigma,\sigma} + F_\tau \circ X_{\tau,\sigma} = 0$ and $F_\sigma \circ X_{\sigma,\tau} + F_\tau \circ X_{\tau,\tau} = 0$. In particular,

$$\mathbb{P}[F \circ X_n = 0] \leq \mathbb{P}[F_\tau \circ X_{\tau,\tau} = -F_\sigma \circ X_{\sigma,\tau}].$$

Since $F_\tau \in \mathrm{Hom}(V_\tau, H)$, we know that $F_\tau \circ X_{\tau,\tau} \in \mathrm{Hom}(V_\tau, H)$. Therefore,

$$\begin{aligned}
&\mathbb{P}[F_\tau \circ X_{\tau,\tau} = -F_\sigma \circ X_{\sigma,\tau}] \\
&= \mathbb{P}\big[F_\tau \circ X_{\tau,\tau} = -F_\sigma \circ X_{\sigma,\tau} \mid F_\sigma \circ X_{\sigma,\tau} \in \mathrm{Hom}(V_\tau, H)\big] \times \mathbb{P}[F_\sigma \circ X_{\sigma,\tau} \in \mathrm{Hom}(V_\tau, H)].
\end{aligned}$$

Since $X_{\tau,\tau}$ is independent of $X_{\sigma,\tau}$ and F_τ is code of distance δn with image H, (1.2) tells us that

$$\mathbb{P}\big[F_\tau \circ X_{\tau,\tau} = -F_\sigma \circ X_{\sigma,\tau} \mid F_\sigma \circ X_{\sigma,\tau} \in \mathrm{Hom}(V_\tau, H)\big] \leq K \frac{1}{|H|^{|\tau|}}.$$

Since σ is nonempty, the condition $F_\sigma \circ X_{\sigma,\tau} \in \mathrm{Hom}(V_\tau, H)$ is non-trivial. Using the fact that each x_{ij} is ϵ-balanced, Wood shows that

$$\mathbb{P}[F_\sigma \circ X_{\sigma,\tau} \in \mathrm{Hom}(V_\tau, H)] \leq (1-\epsilon)^{|\tau|}.$$

Combining this with the previous estimate gives

$$\mathbb{P}[F \circ X_n = 0] \leq K \left(\frac{1-\epsilon}{|H|}\right)^{|\tau|} = K \left(\frac{1-\epsilon}{|H|}\right)^{n} \exp(O(\delta n)).$$

As we saw in the directed case, the number of $F \in \mathrm{Sur}(\mathbb{Z}_p^n, G)$ of δ-type (G, H) is at most $|H|^n \exp(O(\delta n))$. Therefore, their combined contribution to $\mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|]$ is at most

$$K(1-\epsilon)^n \exp(O(\delta n)).$$

If we choose a sufficiently small $\delta > 0$, then this will go to 0. It follows that the combined contribution of all F that are not codes of distance δn goes to 0 as $n \to \infty$. Hence

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(\mathrm{Coker}(X_n), G)|] = |\Lambda^2 G|.$$

Chapter 2

Distribution of Sandpile Groups of Random Directed Bipartite Graphs

Abstract

Fix a prime p and a constant $\frac{1}{p} < \alpha \leq 1$. Consider the random directed Erdős–Rényi bipartite graph $\vec{G}(n, \lceil \alpha n \rceil, v)$ with bipartition (V_1, V_2) of sizes $|V_1| = n$ and $|V_2| = \lceil \alpha n \rceil$, and edge probability $0 < v < 1$. Bhargava, DePascale and Koenig in [1] conjectured a limiting distribution for the p-Sylow subgroup of the sandpile group of $\vec{G}(n, \lceil \alpha n \rceil, v)$ as $n \to \infty$. We prove this conjecture.

Similar results have previously been proved by computing the expected number of surjections from the random abelian p-group onto H, for each finite abelian p-group H. However, in the case of p-Sylow subgroups of sandpile groups of random directed bipartite graphs, these surjective moments often diverge to infinity, despite the conjectured limiting distribution having finite moments. We resolve this by restricting to a high-probability subset of graphs on which the surjective moments are well-behaved, and discarding a rare exceptional set of

graphs whose contribution to the distribution vanishes but whose contribution to the surjective moments often diverges. Computing the conditional surjective moments on the good set and applying Wood's universality theorem yields the desired convergence in distribution.

2.1 Introduction

Fix a prime p throughout the paper. Define the q-shifted factorials

$$(x;q)_i := (1-x)(1-xq)\cdots(1-xq^{i-1}).$$

Let $\vec{\Gamma}$ be a directed graph on vertices $1,\ldots,n$ without any loops. Write $\deg(i,j)$ for the number of directed edges $i \to j$, and set $\deg(j) = \sum_{i:i\neq j}\deg(i,j)$, the in-degree of the vertex. Define the Laplacian $L(\vec{\Gamma})$ by

$$L_{ij} = \begin{cases} \deg(i,j), & i \neq j, \\ -\deg(j), & i = j, \end{cases} \qquad \text{so that} \qquad \sum_{i=1}^{n} L_{ij} = 0 \ \text{ for all } j.$$

Let $\mathbb{Z}_0^n$ be the subset of $\mathbb{Z}^n$ consisting of vectors that sum up to 0. Hence $L : \mathbb{Z}^n \to \mathbb{Z}^n$ satisfies $\operatorname{Im}(L) \subseteq \mathbb{Z}_0^n$. We define the *sandpile group* of $\vec{\Gamma}$ as $S_{\vec{\Gamma}} := \mathbb{Z}_0^n/\operatorname{Im}(L)$. If $\vec{\Gamma}$ is strongly connected, then $\operatorname{corank}(L) = 1$ and $S_{\vec{\Gamma}}$ is a finite abelian group.

Let $\vec{G}(n,v)$ denote the directed Erdős-Rényi random graph on n vertices in which each ordered pair $i \to j$ with $i \neq j$ is included independently with probability $v \in (0,1)$. For fixed v, $\vec{G}(n,v)$ is strongly connected with probability tending to 1 as $n \to \infty$. Consequently, the sandpile group $S_{\vec{G}(n,v)}$ is a finite abelian group with probability tending to 1.

For $0 < u < p$, the measure $P_{\infty,u}$ is defined as

$$P_{\infty,u}(G) := \frac{|G|^{\log_p(u)}}{|\operatorname{Aut}(G)|}\left(\frac{u}{p};\frac{1}{p}\right)_\infty.$$

Koplewitz [12, Theorem 1] shows that as $n \to \infty$, the distribution of the Sylow p-subgroups of the sandpile group of a directed Erdős-Rényi random graph with n vertices converges to $P_{\infty,\frac{1}{p}}$.

Theorem 2.1.1. *[12, Theorem 1] Consider a finite abelian p-group G. Then for a random directed graph $\vec{G}(n, v)$,*

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}(n,v)})_p \cong G] = P_{\infty,\frac{1}{p}}(G).$$

Nguyen and Wood [17, Theorem 1.6] determined the distribution of the entire sandpile group of a directed Erdős-Rényi random graph as $n \to \infty$.

Theorem 2.1.2. *[17, Theorem 1.6] Consider a finite abelian group G. Then for a random directed graph $\vec{G}(n, v)$,*

$$\lim_{n\to\infty} \mathbb{P}[S_{\vec{G}(n,v)} \cong G] = \frac{1}{|G|\,|\mathrm{Aut}(G)|} \prod_{k=2}^{\infty} \zeta(k)^{-1}.$$

Mészáros also determined the distribution of the Sylow p-subgroups of sandpile groups of random d-regular directed graphs [15]. Suppose $d \geq 3$. The random d-regular directed graph D_n is obtained by choosing d independent uniform random permutations $\pi_1, \ldots, \pi_d$ of $\{1, \ldots, n\}$ and, for each $v \in \{1, \ldots, n\}$ and $1 \leq j \leq d$, adding a directed edge from v to $\pi_j(v)$. Let S_{D_n} denote the sandpile group of D_n.

Theorem 2.1.3. *[15, Theorem 1.1] Consider a finite abelian p-group G. Then we have*

$$\lim_{n\to\infty} \mathbb{P}\left((S_{D_n})_p \cong G\right) = P_{\infty,1}(G).$$

We consider random directed bipartite graphs. Let $n_1 \geq n_2$ be positive integers and fix $v \in$

$(0,1)$. The *directed Erdős-Rényi random bipartite graph* $\vec{G}(n_1, n_2, v)$ is a directed bipartite graph with vertex sets V_1 of size n_1 and V_2 of size n_2 where each of the $2n_1n_2$ potential directed edges from V_1 to V_2 and V_2 to V_1 is included independently with probability v. We are most interested in the case where n_1 and n_2 go to infinity together and $n_2 = \lceil \alpha n_1 \rceil$ for a fixed constant $0 < \alpha \leq 1$. We write $\vec{G}_\alpha(n, v)$ in place of $\vec{G}(n, \lceil \alpha n \rceil, v)$. Let $S_{\vec{G}_\alpha(n,v)}$ denote the sandpile group of the directed graph $\vec{G}_\alpha(n, v)$. Bhargava, DePascale and Koenig in [1] conjectured the distribution of the Sylow p-subgroup of the sandpile group $S_{\vec{G}_\alpha(n,v)}$.

Conjecture 2.1.4. *[1] Consider constants* $0 < v < 1$ *and* $\frac{1}{p} < \alpha \leq 1$ *and a finite abelian* p*-group* G*. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}_\alpha(n,v)})_p \cong G] = P_{\infty,\frac{1}{p}}(G).$$

Note that the limit does not depend on the edge probability v. Our main result is to prove this conjecture.

Theorem 2.1.5. *Consider constants* $0 < v < 1$ *and* $\frac{1}{p} < \alpha \leq 1$ *and a finite abelian* p*-group* G*. Then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{\vec{G}_\alpha(n,v)})_p \cong G] = P_{\infty,\frac{1}{p}}(G).$$

The distribution of the p-ranks of $S_{\vec{G}_\alpha(n,v)}$ was determined by Bhargava, DePascale and Koenig in [1]. It is shown in [10] that this is consistent with Conjecture 2.1.4.

Theorem 2.1.6. *Let* p *be prime,* $0 < v < 1$ *and* $\frac{1}{p} < \alpha \leq 1$*. Then*

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{rank}((S_{\vec{G}_\alpha(n,v)})_p) = r] = \frac{1}{p^{r^2+r}} \frac{\left(\frac{1}{p^{r+2}}; \frac{1}{p}\right)_\infty}{\left(\frac{1}{p}; \frac{1}{p}\right)_r}.$$

In upcoming work [21], we study random undirected bipartite graphs. For odd p, we determine the distribution of the p-Sylow subgroups of their sandpile groups. For $p = 2$, where an interesting special distribution arises, we do not completely determine the distribution, but we prove several intermediate results.

2.1.1 Random Matrix model

Let $\mathbb{Z}_p$ be the ring of p-adic integers. Fix $0 < \epsilon < 1$ for the rest of the paper. A random variable x taking values in $\mathbb{Z}_p$ is called *ϵ-balanced* if for each $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\mathbb{P}[x \equiv a \pmod p] < 1 - \epsilon.$$

We consider a random matrix model for the Laplacian of $\vec{G}_\alpha(n, v)$ as a random matrix $L_{n_1,n_2} \in \mathbb{M}_{n_1+n_2}(\mathbb{Z}_p)$ as follows:

$$L_{n_1,n_2} = \begin{bmatrix} -\sum b_{1j} & 0 & \dots & 0 & a_{11} & a_{12} & \dots & a_{1n_2} \\ 0 & -\sum b_{2j} & \dots & 0 & a_{21} & a_{22} & \dots & a_{2n_2} \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \dots & -\sum b_{n_1 j} & a_{n_1 1} & a_{n_1 2} & \dots & a_{n_1 n_2} \\ b_{11} & b_{21} & \dots & b_{n_1 1} & -\sum a_{i1} & 0 & \dots & 0 \\ b_{12} & b_{22} & \dots & b_{n_1 2} & 0 & -\sum a_{i2} & \dots & 0 \\ \vdots & & & \vdots & \vdots & & \ddots & \vdots \\ b_{1n_2} & b_{2n_2} & \dots & b_{n_1 n_2} & 0 & 0 & \dots & -\sum a_{in_2} \end{bmatrix},$$

where all a_{ij} and b_{ij} are ϵ-balanced and independent. Now, $L_{n_1,n_2} \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, \mathbb{Z}_p^{n_1+n_2})$. Let Z_n consist of the vectors in $\mathbb{Z}_p^n$ whose entries sum to 0, so $\mathrm{Im}(L_{n_1,n_2}) \subseteq Z_{n_1+n_2}$. We denote $G(L_{n_1,n_2}) = Z_{n_1+n_2}/\,\mathrm{Im}(L_{n_1,n_2})$. In particular, if a_{ij} and b_{ij} took values 1 and 0 with probability v and $1 - v$ respectively, then $L_n^{(\alpha)}$ would be the random matrix arising from the Laplacian of the random graph $\vec{G}_\alpha(n,v)$. Moreover, in the (high probability) event that $\vec{G}_\alpha(n,v)$ is connected, the random finite abelian p-group $G(L_n^{(\alpha)})$ would become isomorphic to the p-Sylow subgroup of $S_{\vec{G}_\alpha(n,v)}$.

One of the difficulties of working with L_{n_1,n_2} is that the diagonal entries depend on other entries of the matrix. We therefore consider a related random matrix whose diagonal entries are independent. Consider the random matrix $M_{n_1,n_2} \in \mathbb{M}_{n_1+n_2}(\mathbb{Z}_p)$ defined as follows:

$$M_{n_1,n_2} = \begin{bmatrix} c_1 & 0 & \dots & 0 & a_{11} & a_{12} & \dots & a_{1n_2} \\ 0 & c_2 & \dots & 0 & a_{21} & a_{22} & \dots & a_{2n_2} \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \dots & c_{n_1} & a_{n_11} & a_{n_12} & \dots & a_{n_1n_2} \\ b_{11} & b_{21} & \dots & b_{n_11} & d_1 & 0 & \dots & 0 \\ b_{12} & b_{22} & \dots & b_{n_12} & 0 & d_2 & \dots & 0 \\ \vdots & & & \vdots & \vdots & & \ddots & \vdots \\ b_{1n_2} & b_{2n_2} & \dots & b_{n_1n_2} & 0 & 0 & \dots & d_{n_2} \end{bmatrix},$$

where all a_{ij} and b_{ij} are ϵ-balanced and c_j and d_j are Haar uniform and mutually independent. Note that $M_{n_1,n_2} \in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2}, \mathbb{Z}_p^{n_1+n_2})$, so we can consider the cokernel $\operatorname{Coker}(M_{n_1,n_2}) = \mathbb{Z}_p^{n_1+n_2}/\operatorname{Im}(M_{n_1,n_2})$.

For $0 < \alpha \leq 1$, we will denote $M_n^{(\alpha)} = M_{n,\lceil \alpha n\rceil}$ and $L_n^{(\alpha)} = L_{n,\lceil \alpha n\rceil}$. We will see that $\operatorname{Coker}(M_n^{(\alpha)})$ is easier to analyze than $G(L_n^{(\alpha)})$, and that its analysis helps us study $G(L_n^{(\alpha)})$.

We will prove the following:

Theorem 2.1.7. *Given $\frac{1}{p} < \alpha \leq 1$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{Coker}(M_n^{(\alpha)}) \cong G] = P_{\infty,1}(G).$$

Theorem 2.1.8. *Given $\frac{1}{p} < \alpha \leq 1$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{P}[G(L_n^{(\alpha)}) \cong G] = P_{\infty,\frac{1}{p}}(G).$$

Note that Theorem 2.1.8 directly implies Theorem 2.1.5.

We now briefly outline the paper. In Section 2.2, we explain the strategy of the proof. In Section 2.3 and Section 2.4, we study the independent diagonal model. In Section 2.5 and Section 2.6, we return to the Laplacian model. In Section 2.7, we show that the expected number of surjections to a fixed G can diverge to infinity. Finally, in Section 2.8, we prove several technical lemmas used throughout the paper.

2.2 Strategy

Previous results about the distribution of sandpile groups of random graphs and cokernels of random matrices have been proven using the following strategy. Suppose G_n is a sequence of random finite abelian p-groups and ν is the conjectured distribution as $n \to \infty$. The first step is to show that the surjective moments match. That is, for every finite abelian p-group H, we have

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(G_n, H)|] = \mathbb{E}[|\mathrm{Sur}(G, H)|], \tag{2.1}$$

where G is a finite abelian p-group chosen according to ν. The next step is to use a result, that if (2.1) is satisfied, then it implies that for every finite abelian p-group H

$$\lim_{n\to\infty} \mathbb{P}[G_n \cong H] = \nu(H).$$

The surjective moments of $P_{\infty,u}$ were computed by Wood in [24].

Theorem 2.2.1. *[24, Lemma 3.2] Suppose we are given a constant $0 < u < p$ and X is a random finite abelian p-group distributed according to $P_{\infty,u}$, Then for every finite abelian p-group G, we have*

$$\mathbb{E}[|\mathrm{Sur}(X, G)|] = |G|^{\log_p(u)} .$$

Based on this we should expect that for each finite abelian p-group H, we have

$$\lim_{n\to\infty} \mathbb{E}[\left|\mathrm{Sur}(\mathrm{Coker}(M_n^{(\alpha)}), H)\right|] = 1,$$

$$\lim_{n\to\infty} \mathbb{E}[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), H)\right|] = \frac{1}{|H|}.$$

However, this is not always the case, as we will show in Section 2.7. These limits sometimes blow up to infinity. The issue here is that a small subset of matrices contribute greatly to the surjective moments while contributing minimally to the distribution. We can get around this problem by restricting ourselves to a subset of the matrices whose probability goes to 1 as $n \to \infty$, and computing the moments on this subset.

2.2.1 Independent diagonal model

We denote

$$\Gamma(M_{n_1,n_2}) = \left\{1 \le i \le n_1 \mid c_i \equiv 0 \pmod p\right\} \quad \text{and} \quad \gamma(M_{n_1,n_2}) = \left|\Gamma(M_{n_1,n_2})\right|. \tag{2.2}$$

Since the c_i are Haar-uniform, we should expect $\gamma(M_{n_1,n_2})$ to be concentrated around $\frac{1}{p}n_1$. Given a constant $\rho > 0$, we consider the subset of matrices for which $\left|\gamma(M_{n_1,n_2}) - \frac{1}{p}n_1\right| \le \rho n_1$. We show in Corollary 2.8.2 that the probability of this goes to 1 as $n \to \infty$.

Given a function f that takes M_{n_1,n_2} as input, we denote the conditional expectation as

$$\mathbb{E}_\rho[f(M_{n_1,n_2})] = \mathbb{E}[f(M_{n_1,n_2}) \mid |\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1| \leq \rho n_1].$$

We also denote the expectation restricted to the event $|\gamma(M_{n_1,n_2}) - \frac{1}{p}n_1| \leq \rho n_1$ as

$$\mathbb{E}'_\rho[f(M_{n_1,n_2})] = \mathbb{P}[|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1| \leq \rho n_1] \times \mathbb{E}_\rho[f(M_{n_1,n_2})].$$

We will show that once we restrict ourselves to this subset, then we get the right surjective moments and the issue of moments blowing up to infinity is resolved.

Proposition 2.2.2. *Given $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}_\rho[\left|\mathrm{Sur}(\mathrm{Coker}(M_n^{(\alpha)}), G)\right|] = 1.$$

Note that the restriction $\rho < \alpha - \frac{1}{p}$ is to avoid the matrices for which $\gamma(M_n^{(\alpha)}) > n_2 = \lceil \alpha n \rceil$. These are the matrices responsible for the large surjective moments. If $\alpha = 1$, then no matrix can have $\gamma(M_n^{(\alpha)}) > n_2 = n$. In fact, if $\alpha = 1$, then the issue of moments blowing up does not arise and one could work directly with the raw moments $\lim_{n\to\infty} \mathbb{E}[\left| \mathrm{Sur}(\mathrm{Coker}(M_n^{(1)}), G)\right|]$.

Once we have the moments, we can show that the desired distribution occurs using the following result of Wood.

Theorem 2.2.3. *[23, Theorem 8.2] If X_n is a sequence of random abelian p-groups and Y is a random abelian p-group such that for every finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(X_n, G)|] = \mathbb{E}[|\mathrm{Sur}(Y, G)|] \leq \left|\Lambda^2 G\right|.$$

Then for every finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}[X_n \cong G] = \mathbb{P}[Y \cong G].$$

We can now show that Proposition 2.2.2 implies Theorem 2.1.7.

Theorem 2.1.7. Given $\frac{1}{p} < \alpha \leq 1$ and a finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{Coker}(M_n^{(\alpha)}) \cong G] = P_{\infty,1}(G).$$

Proof of Theorem 2.1.7 assuming Proposition 2.2.2. Fix $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$. Let G_n be a random finite abelian p-group distributed according to

$$\mathbb{P}[G_n \cong G] = \mathbb{P}\left[\mathrm{Coker}(M_n^{(\alpha)}) \cong G \mid \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right].$$

Therefore, Proposition 2.2.2 says that

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(G_n, G)|] = 1.$$

Therefore from Theorem 2.2.1 and Theorem 2.2.3 we see that for each finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{Coker}(M_n^{(\alpha)}) \cong G \mid \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = \lim_{n\to\infty} \mathbb{P}[G_n \cong G] = P_{\infty,1}(G).$$

Note that

$$
\begin{aligned}
&\mathbb{P}[\mathrm{Coker}(M_n^{(\alpha)}) \cong G] \\
&= \mathbb{P}\left[\mathrm{Coker}(M_n^{(\alpha)}) \cong G \mid \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] \times \mathbb{P}\left[\left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] \\
&+ \mathbb{P}\left[\mathrm{Coker}(M_n^{(\alpha)}) \cong G \mid \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| > \rho n\right] \times \mathbb{P}\left[\left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| > \rho n\right].
\end{aligned}
$$

The result follows since Corollary 2.8.2 says that $\lim_{n\to\infty} \mathbb{P}\left[\left|\gamma(M_n^{(\alpha)}) - \frac{1}{p}n\right| \leq \rho n\right] = 1$. $\square$

Moreover, to prove Proposition 2.2.2, it is enough to compute the Hom-moments.

Proposition 2.2.4. *Given $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}_\rho[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), G)\right|] = \left|\{\textit{Subgroups of } G\}\right|.$$

We show that the computation of Hom-moments indeed leads to the surjective moments.

Proof of Proposition 2.2.2. The result follows from Proposition 2.2.4 by induction on the size of G. $\square$

2.2.2 Laplacian model

Similarly to the independent diagonal model denote

$$\Gamma(L_{n_1,n_2}) = \left\{1 \leq i \leq n_1 \mid \sum_{j=1}^{n_2} b_{ij} \equiv 0 \pmod{p}\right\} \quad \text{and} \quad \gamma(L_{n_1,n_2}) = \left|\Gamma(L_{n_1,n_2})\right|.$$

Even though b_{ij} are not necessarily Haar uniform, as n_2 gets bigger $\sum_{j=1}^{n_2} b_{ij}$ would get close to being uniformly distributed $\bmod p$. Therefore, we should still expect $\gamma(L_{n_1,n_2})$ to be concentrated around $\frac{1}{p}n_1$. Given a constant $\rho > 0$, we consider the subset of matrices for which $\left|\gamma(L_{n_1,n_2}) - \frac{1}{p}n_1\right| \leq \rho n_1$. We show in Lemma 2.8.3 that the probability of this goes to 1 as $n \to \infty$.

Also as before, for a function f that takes L_{n_1,n_2} as input, we denote

$$\mathbb{E}_\rho[f(L_{n_1,n_2})] = \mathbb{E}[f(L_{n_1,n_2}) \mid |\gamma(L_{n_1,n_2}) - \tfrac{1}{p}n_1| \leq \rho n_1],$$

and

$$\mathbb{E}'_\rho[f(L_{n_1,n_2})] = \mathbb{P}[|\gamma(L_{n_1,n_2}) - \tfrac{1}{p}n_1| \leq \rho n_1] \times \mathbb{E}_\rho[f(L_{n_1,n_2})].$$

Once we restrict ourselves to this subset, then the issue of moments blowing up to infinity gets resolved and we get the right moments.

Proposition 2.2.5. *Given $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}_\rho[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), G)\right|] = \frac{1}{|G|}.$$

As in the independent diagonal model, the restriction $\rho < \alpha - \frac{1}{p}$ is to avoid the matrices for which $\gamma(L_n^{(\alpha)}) > n_2 = \lceil \alpha n \rceil$. These are the matrices responsible for the large surjective moments. These matrices correspond to those bipartite directed graphs for which the number of vertices in V_1 whose in-degree is divisible by p is larger than $|V_2| = \lceil \alpha n \rceil$. If $\alpha = 1$, then no matrix can have $\gamma(L_n^{(\alpha)}) > n_2 = n$. In fact, if $\alpha = 1$, then the issue of moments blowing up does not arise and one could work directly with the raw moments $\lim_{n\to\infty} \mathbb{E}[\left|\mathrm{Sur}(\mathrm{Coker}(L_n^{(1)}), G)\right|]$.

We show that Proposition 2.2.5 implies Theorem 2.1.8.

Theorem 2.1.8. Given $\frac{1}{p} < \alpha \leq 1$ and a finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}[G(L_n^{(\alpha)}) \cong G] = P_{\infty,\frac{1}{p}}(G).$$

Proof of Theorem 2.1.8 assuming Proposition 2.2.5. Fix $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$. Proposition 2.2.5, Theorem 2.2.1 and Theorem 2.2.3 imply that for each finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}\left[G(L_n^{(\alpha)}) \cong G \mid \left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = P_{\infty,\frac{1}{p}}(G).$$

Note that

$$\begin{aligned}
&\mathbb{P}[G(L_n^{(\alpha)}) \cong G] \\
&= \mathbb{P}\left[G(L_n^{(\alpha)}) \cong G \mid \left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] \times \mathbb{P}\left[\left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] \\
&+ \mathbb{P}\left[G(L_n^{(\alpha)}) \cong G \mid \left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| > \rho n\right] \times \mathbb{P}\left[\left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| > \rho n\right].
\end{aligned}$$

The result follows since Lemma 2.8.3 says that $\lim_{n\to\infty} \mathbb{P}\left[\left|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = 1.$ $\square$

Therefore, our goal now is to prove Proposition 2.2.4 and Proposition 2.2.5.

2.3 Setup for Independent diagonal model

Fix a finite abelian group G for this and the next section. Note that $M_{n_1,n_2} \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, \mathbb{Z}_p^{n_1+n_2})$, therefore,

$$\begin{aligned}
&\mathbb{E}'_\rho[|\mathrm{Hom}(\mathrm{Coker}(M_{n_1,n_2}), G)|] \\
&= \sum_{F\in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)} \mathbb{P}\left[F \circ M_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G) \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right].
\end{aligned}$$

First note that for each $F \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)$,

$$
\begin{aligned}
&\mathbb{P}\left[F \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right] \\
&= \sum_{\substack{S \subseteq [n_1]: \\ \left||S| - \frac{1}{p}n_1\right| \leq \rho n_1}} \mathbb{P}[F \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S].
\end{aligned}
\tag{2.3}
$$

Denote $A_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{n_1 j} \end{bmatrix} \in \mathbb{Z}_p^{n_1}$, $B_i = \begin{bmatrix} b_{i1} \\ \vdots \\ b_{in_2} \end{bmatrix} \in \mathbb{Z}_p^{n_2}$. Denote the standard basis of $\mathbb{Z}_p^{n_1}$ as $u_1, \ldots, u_{n_1}$ and that of $\mathbb{Z}_p^{n_2}$ as $v_1, \ldots, v_{n_2}$. Also note that F can be decomposed into $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$ and $F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G)$. Since the columns of M_{n_1,n_2} are independent of each other, we see that

$$
\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S] \\
&= \prod_{i \in S} \mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \text{ and } c_i \equiv 0 \pmod{p}] \\
&\qquad \times \prod_{i \in [n_1] \setminus S} \mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \text{ and } c_i \not\equiv 0 \pmod{p}] \\
&\qquad \times \prod_{j \in [n_2]} \mathbb{P}[F_1(A_j) = -d_j F_2(v_j)].
\end{aligned}
\tag{2.4}
$$

We therefore want to estimate the probabilities appearing in (2.4). The vectors $A_j \in \mathbb{Z}_p^{n_1}$ and $B_i \in \mathbb{Z}_p^{n_2}$ have independent, ϵ-balanced entries. We will first compute such probabilities, in the case when the entries are Haar-uniform.

Lemma 2.3.1. *Suppose we are given $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ with $\mathrm{Im}(F) = H$. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and Haar-uniform. Then for each $h \in H$, we* *have*

$$\mathbb{P}\big[F(X) = h\big] = \frac{1}{|H|}.$$

Proof. Note that for each $g \in H$, $F^{-1}(g)$ is a translation of $\ker(F)$. Since the Haar measure is translation invariant, each $F^{-1}(g)$ must have the same Haar measure. Finally, since the measure of $\mathbb{Z}_p^n$ is 1, the measure of each $F^{-1}(g)$ is $\frac{1}{|H|}$. □

In the case where the entries of X are ϵ-balanced but not Haar-uniform, then we cannot compute the probability with such a simple method. In the next subsection, we will describe how to partition $\mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)$, how to estimate the probabilities for F in certain parts and how to bound them for F in other parts.

2.3.1 Codes and depth

In this subsection, we recall some material due to Wood [23, 24]. Let $V = \mathbb{Z}_p^n$ with the standard basis $\{v_1, \ldots, v_n\}$. Denote $[n] = \{1, \ldots, n\}$. Given a subset $\sigma \subseteq [n]$, we have a distinguished submodule $V_{\backslash\sigma} \subseteq V$, which is generated by v_i satisfying $i \notin \sigma$ and another distinguished submodule $V_\sigma \subseteq V$, which is generated by v_i satisfying $i \in \sigma$. The notions of code and δ-depth were defined by Wood in [24]. Our definitions are slightly different from hers.

Definition 2.3.2. Consider $F \in \mathrm{Hom}(V, G)$. It is called a code of distance d with image H if for every subset $\sigma \subseteq [n]$ with $|\sigma| < d$, we have $F(V_{\backslash\sigma}) = F(V) = H$.

This means not only is F surjective to H, but it remains surjective to H as long as you do not throw away too many basis vectors. If $\mathrm{Im}(F) = H$ and F is not a code, it means we can throw away a few basis vectors and shrink the image. The depth of F measures the extent to which we can shrink the image without throwing away too many basis vectors.

Definition 2.3.3. Given $\delta > 0$ and $F \in \mathrm{Hom}(V, G)$, the δ-depth of F is defined to be the largest positive integer D for which there is a subset $\sigma \subseteq [n]$ with $|\sigma| < \log_p(D)\delta n$ such that $[F(V) : F(V_{\backslash\sigma})] = D$, or 1 if there is no such σ.

If such a σ exists, then we say that F is of δ-type $(F(V), F(V_{\backslash\sigma}))$. If there is no such σ, then we set the δ-type to be $(F(V), F(V))$.

It is noted in [24, Remark 2.5] that if F has δ-depth 1, then it is a code of distance δn.

Given subgroups $T \subseteq H \subseteq G$, we denote

$$\mathcal{S}_{n,\delta}(H, T) := \{F \in \mathrm{Hom}(\mathbb{Z}_p^n, G) : \delta - \text{type } (H, T)\}.$$

This gives a cover

$$\mathrm{Hom}(\mathbb{Z}_p^n, G) = \bigcup_{H \subseteq G} \bigcup_{T \subseteq H} \mathcal{S}_{n,\delta}(H, T).$$

In general, this union need not be disjoint, since a given F may have δ-type (H, T) for more than one choice of T. However, the pieces $\mathcal{S}_{n,\delta}(H, H)$ consist of codes with image H, and these pieces are pairwise disjoint.

First consider the case $T = H$, so all $F \in \mathcal{S}_{n,\delta}(H, H)$ are codes of distance δn with image H. For such F, Wood shows that the probability is close to $\frac{1}{|H|}$ even when X is ϵ-balanced.

Lemma 2.3.4. *[24, Lemma 2.1] Suppose $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ is a code of distance d with image H. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then for every $f \in H$, we have*

$$\left| \mathbb{P}[F(X) = f] - \frac{1}{|H|} \right| \leq \exp\Big(- \frac{\epsilon d}{|G|^2} \Big).$$

Next consider the case $T \subsetneq H$. For $F \in \mathcal{S}_{n,\delta}(H,T)$, the probability can be bigger than $\frac{1}{|H|}$, but Wood shows that it can still be bounded as follows.

Lemma 2.3.5. *[24, Lemma 2.7] Suppose we are given subgroups $T \subsetneq H \subseteq G$, Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then for every $f \in G$, we have*

$$\mathbb{P}[F(X) = f] \leq (1-\epsilon)\left(\frac{1}{|T|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^2}\Big)\right).$$

Proof. Actually the result in [24, Lemma 2.7] is for $f = 0$, but the same proof goes through for any $f \in G$. □

Corollary 2.3.6. *Suppose we are given $\delta > 0$ and subgroups $T \subseteq H \subseteq G$. Denote*

$$e = \begin{cases} 1 & \text{if } T = H \\ 1-\epsilon & \text{if } T \subsetneq H. \end{cases}$$

Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then for every $F \in \mathcal{S}_{n,\delta}(H,T)$ and for every $f \in G$, we have

$$\mathbb{P}[F(X) = f] \leq e\left(\frac{1}{|T|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^2}\Big)\right).$$

Proof. First, consider the case $T = H$, so F is a code of distance δn with image T. Now, if $f \notin T$, then the probability is zero and the inequality holds trivially, whereas if $f \in T$, then the result follows from Lemma 2.3.4.

Next, consider the case $T \subsetneq H$. Then the result follows from Lemma 2.3.5. □

We will also need a bound for the probability that $F(X)$ belongs to another subgroup.

Lemma 2.3.7. *Suppose we are given $\delta > 0$, subgroups $T \subseteq H \subseteq G$ and another subgroup $T' \subseteq G$. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then for every $F \in \mathcal{S}_{n,\delta}(H, T)$, we have*

$$\mathbb{P}[F(X) \in T'] \leq \left(\frac{|T \cap T'|}{|T|} + \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right).$$

Proof. Denote $D = [H : T]$. Consider the map $\pi : H \twoheadrightarrow H/(H \cap T')$. So $\pi \circ F \in \operatorname{Hom}(\mathbb{Z}_p^n, H/(H \cap T'))$. Moreover, $F(X) \in T'$ if and only if $(\pi \circ F)(X) = 0$. There is some $\sigma \subseteq [n]$ with $|\sigma| \leq \delta n \log_p(D)$ such that $F(V_{\backslash \sigma}) = T$.

Also,

$$F \in \operatorname{Hom}(V_{\backslash \sigma} \oplus V_\sigma, G) = \operatorname{Hom}(V_{\backslash \sigma}, G) \oplus \operatorname{Hom}(V_\sigma, G),$$

so we can decompose $F = (F_{\backslash \sigma}, F_\sigma)$ and $X = (X_{\backslash \sigma}, X_\sigma)$. Note that

$$(\pi \circ F)(X) = (\pi \circ F_{\backslash \sigma})(X_{\backslash \sigma}) + (\pi \circ F_\sigma)(X_\sigma).$$

We will show that $\pi \circ F_{\backslash \sigma}$ is a code of distance δn with image $\pi(T)$. Assume for the sake of contradiction that this is not true. This means there is some proper subgroup $L \subsetneq \pi(T)$ and $\tau \subseteq [n] \setminus \sigma$ with $|\tau| < \delta n$ such that $(\pi \circ F)(V_{\backslash(\sigma \cup \tau)}) \subseteq L$. Hence $F(V_{\backslash(\sigma \cup \tau)}) \subseteq \pi^{-1}(L)$. We also know that $F(V_{\backslash(\sigma \cup \tau)}) \subseteq F(V_{\backslash \sigma}) = T$, and hence $F(V_{\backslash(\sigma \cup \tau)}) \subseteq \pi^{-1}(L) \cap T$. Since L is a proper subgroup of $\pi(T)$, it follows that $\pi^{-1}(L) \cap T$ is a proper subgroup of T. This means that $D' = [H : \pi^{-1}(L) \cap T] \geq pD$. Moreover, $|\sigma \cup \tau| < \delta n \log_p(D) + \delta n \leq \delta n \log_p(D')$. However, this implies that the δ-depth of F is at least D', which is a contradiction. We conclude that $\pi \circ F_{\backslash \sigma}$ is a code of distance δn with image $\pi(T)$.

Therefore, by Lemma 2.3.4, we see that

$$\begin{aligned}\mathbb{P}[F(X) \in T'] &= \mathbb{P}[(\pi \circ F)(X) = 0] = \mathbb{P}[(\pi \circ F_{\setminus\sigma})(X_{\setminus\sigma}) = -(\pi \circ F_\sigma)(X_\sigma)] \\ &= \mathbb{P}[(\pi \circ F_{\setminus\sigma})(X_{\setminus\sigma}) = -(\pi \circ F_\sigma)(X_\sigma) \mid (\pi \circ F_\sigma)(X_\sigma) \in \pi(T)]\mathbb{P}[(\pi \circ F_\sigma)(X_\sigma) \in \pi(T)] \\ &\leq \left(\frac{1}{|\pi(T)|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^2}\Big)\right) \times 1.\end{aligned}$$

The result follows since $|\pi(T)| = \frac{|T|}{|T \cap T'|}$. □

We will also need bounds on the sizes of $\mathcal{S}_{n,\delta}(H,T)$. We start with the case $T \subsetneq H$.

Lemma 2.3.8. *[23, Lemma 5.2] Given subgroups $T \subsetneq H \subseteq G$, denote $D = [H : T] > 1$. Then we have*

$$|\mathcal{S}_{n,\delta}(H,T)| \leq \binom{n}{\lceil \delta \log_p(D) n \rceil - 1} |T|^n D^{\delta \log_p(D) n}.$$

Denote the binary entropy function as $H(\alpha) = -\alpha \log_2(\alpha) - (1-\alpha)\log_2(1-\alpha)$. It is known that $\binom{a}{b} \leq 2^{H(\frac{b}{a})a}$ and that $H(\alpha) \leq 2\sqrt{\alpha}$. It follows that $\binom{a}{b} \leq 2^{2\sqrt{ab}}$. The following corollary follows at once.

Corollary 2.3.9. *Given $D > 1$ and subgroups $T \subsetneq H \subseteq G$ with $[H : T] = D$, we have*

$$|\mathcal{S}_{n,\delta}(H,T)| \leq 2^{n\sqrt{\delta \log_p(|G|)}} |T|^n D^{\delta \log_p(D) n}.$$

Given a group G, let K_G be the number of subgroups of G. We estimate the size of $\mathcal{S}_{n,\delta}(H,H)$.

Lemma 2.3.10. *Consider $0 < \delta < \frac{1}{3\log_p(|G|)}$. There is a constant $c_{G,\delta} > 0$ (depending on G and δ), such that for each subgroup $H \subseteq G$*

$$|H|^n \left(1 - K_G \exp(-c_{G,\delta} n) - K_G 2^{-n}\right) \leq |\mathcal{S}_{n,\delta}(H,H)| \leq |H|^n.$$

Proof. The upper bound follows from the fact that

$$\mathcal{S}_{n,\delta}(H,H) \subseteq \mathrm{Hom}(\mathbb{Z}_p^n, H).$$

Moreover,

$$\mathrm{Hom}(\mathbb{Z}_p^n, H) \setminus \mathcal{S}_{n,\delta}(H,H) = \bigcup_{T \subsetneq H} \mathcal{S}_{n,\delta}(H,T) \cup \mathrm{Hom}(\mathbb{Z}_p^n, T).$$

The number of T is at most K_G, and

$$\left|\mathrm{Hom}(\mathbb{Z}_p^n, T)\right| = |T|^n \leq \frac{|H|^n}{2^n}.$$

Denote $[H:T] = D > 1$. Then we know that

$$|\mathcal{S}_{n,\delta}(H,T)| \leq 2^{n\sqrt{\delta \log_p(|G|)}} |H|^n D^{-n+\delta \log_p(D) n} \leq |H|^n \left(2^{\sqrt{\delta \log_p(|G|)} - 1 + \delta \log_p(|G|)}\right)^n.$$

The bound on δ also ensures that $\sqrt{\delta \log_p(|G|)} - 1 + \delta \log_p(|G|) < 0$. The result follows. □

2.4 Independent diagonal model

We have fixed a finite abelian p-group G. Recall that given $\delta > 0$, we can partition

$$\mathrm{Hom}(\mathbb{Z}_p^{n_1}, G) = \bigcup_{H_1 \subseteq G} \bigcup_{T_1 \subseteq H_1} \mathcal{S}_{n_1,\delta}(H_1, T_1),$$

$$\mathrm{Hom}(\mathbb{Z}_p^{n_2}, G) = \bigcup_{H_2 \subseteq G} \bigcup_{T_2 \subseteq H_2} \mathcal{S}_{n_2,\delta}(H_2, T_2).$$

We will show the following.

Proposition 2.4.1. *Given $\frac{1}{p} < \alpha \leq 1$ and $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group*

G, there is $\delta > 0$ such that for any subgroups $T_1 \subseteq H_1 \subseteq G$, $T_2 \subseteq H_2 \subseteq G$, we have

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(H_2,T_2)} \mathbb{P}\left[(F_1,F_2)\circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \le \rho n\right]$$
$$= \begin{cases} 1 & \text{if } T_1 = H_1 = T_2 = H_2 \\ 0 & \text{otherwise.} \end{cases}$$

This will imply Proposition 2.2.4.

Proposition 2.2.4. Given $\frac{1}{p} < \alpha \le 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), G)\right|\right] = \left|\text{Subgroups of } G\right|.$$

Proof of Proposition 2.2.4 assuming Proposition 2.4.1. Proposition 2.4.1 implies that

$$\lim_{n\to\infty} \mathbb{E}'_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), G)\right|\right] = \left|\text{Subgroups of } G\right|.$$

The result follows from Corollary 2.8.2. □

On each piece, our goal is to estimate

$$\mathbb{P}\left[(F_1,F_2)\circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \le \rho n_1\right].$$

This probability can be decomposed as shown in (2.3) and (2.4).

2.4.1 Main term

In this subsection, the only requirement we put on δ is that $0 < \delta < \frac{1}{3\log_p(|G|)}$ and we focus on the case when $T_1 = H_1 = T_2 = H_2$. Denote this subgroup as H. This means that F_1 is a code of distance δn_1 with image H and F_2 is a code of distance δn_2 with image H.

We start by estimating the probability that $(F_1, F_2) \circ M_{n_1,n_2} = 0$ and $\Gamma(M_{n_1,n_2}) = S$ for a fixed subset $S \subseteq [n_1]$.

Lemma 2.4.2. *Suppose $\frac{1}{p} < \alpha \leq 1$, $\alpha n_1 \leq n_2 \leq n_1$ and $S \subseteq [n_1]$. If H is a subgroup of G, $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$ is a code of distance δn_1 with image H and $F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G)$ is a code of distance δn_2 with image H. Then, for sufficiently large values of n_1 (depending on $G, \epsilon, \delta, \alpha$), we have*

$$\left|\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S] - \frac{1}{p^{|S|}}\Big(1 - \frac{1}{p}\Big)^{n_1-|S|} \frac{1}{|H|^{n_1+n_2}}\right|$$
$$\leq \frac{1}{p^{|S|}}\Big(1 - \frac{1}{p}\Big)^{n_1-|S|} 4n_1 \frac{1}{|H|^{n_1+n_2-1}} \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

Proof. We estimate each term in the product given by (2.4). First, for $i \in S$, we know that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \text{ and } c_i \equiv 0 \pmod p]$$
$$= \mathbb{P}[c_i \equiv 0 \pmod p]\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \equiv 0 \pmod p]$$
$$= \frac{1}{p}\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \equiv 0 \pmod p].$$

Moreover, Lemma 2.3.4 tells us that

$$\left|\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \equiv 0 \pmod p] - \frac{1}{|H|}\right| \leq \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big) \leq \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

For $i \in [n_1] \setminus S$, we similarly see that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \text{ and } c_i \not\equiv 0 \pmod p]$$
$$= \mathbb{P}[c_i \not\equiv 0 \pmod p]\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \not\equiv 0 \pmod p]$$
$$= (1 - \tfrac{1}{p})\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \not\equiv 0 \pmod p].$$

Moreover, Lemma 2.3.4 tells us that

$$\left|\mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \not\equiv 0 \pmod p] - \frac{1}{|H|}\right| \leq \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big) \leq \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

Finally for $j \in [n_2]$, Lemma 2.3.4 tells us that

$$\left|\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] - \frac{1}{|H|}\right| \leq \exp\Big(-\frac{\epsilon\delta n_1}{|G|^2}\Big) \leq \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

Now, in order to apply Corollary 2.8.5, we need

$$\frac{\exp\big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\big)}{2^{\frac{1}{2n_1}} - 1} \leq \frac{1}{|H|}.$$

This inequality holds for sufficiently large n_1, since the limit of the left hand side is 0. Therefore, Corollary 2.8.5 tells us that

$$\left|\frac{1}{\frac{1}{p^{|S|}}(1-\frac{1}{p})^{n_1-|S|}}\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S] - \frac{1}{|H|^{n_1+n_2}}\right|$$
$$\leq 2(n_1+n_2)\frac{1}{|H|^{n_1+n_2-1}}\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

The result follows. $\square$

Next, we sum over the different subsets $S \subseteq [n_1]$ that satisfy $\left||S| - \frac{1}{p}n_1\right| \leq \rho n_1$.

Corollary 2.4.3. *Suppose $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$, $\alpha n_1 \leq n_2 \leq n_1$ and H is a subgroup of G. Suppose that $F_1 \in \operatorname{Hom}(\mathbb{Z}_p^{n_1}, G)$ is a code of distance δn_1 with image H and $F_2 \in \operatorname{Hom}(\mathbb{Z}_p^{n_2}, G)$ is a code of distance δn_2 with image H. Then, for sufficiently large* *values of n_1 (depending on $G, \epsilon, \delta, \alpha$), we have*

$$\left|\mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \textit{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right] - \frac{1}{|H|^{n_1+n_2}}\right|$$
$$\leq 4n_1 \frac{1}{|H|^{n_1+n_2-1}} \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big) + \frac{2}{|H|^{n_1+n_2}} \exp\big(-2\rho^2 n_1\big).$$

Proof. We sum the estimate of Lemma 2.4.2 over the different $S \subseteq [n_1]$ with $\left||S| - \frac{1}{p}n_1\right| \leq \rho n_1$,

$$\left|\mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right] - \frac{1}{|H|^{n_1+n_2}} \sum_{k:\left|k-\frac{1}{p}n_1\right|\leq \rho n_1} \tbinom{n_1}{k} \tfrac{1}{p^k}\big(1-\tfrac{1}{p}\big)^{n_1-k}\right|$$
$$\leq 4n_1 \frac{1}{|H|^{n_1+n_2-1}} \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big).$$

Lemma 2.8.1 implies that

$$\left|\frac{1}{|H|^{n_1+n_2}} \sum_{k:\left|k-\frac{1}{p}n_1\right|\leq \rho n_1} \binom{n_1}{k} \frac{1}{p^k}\Big(1-\frac{1}{p}\Big)^{n_1-k} - \frac{1}{|H|^{n_1+n_2}}\right| \leq \frac{2}{|H|^{n_1+n_2}} \exp\big(-2\rho^2 n_1\big). \qquad \square$$

We now sum over the different $F_1 \in \mathcal{S}_{n,\delta}(H,H)$, $F_2 \in \mathcal{S}_{n,\delta}(H,H)$. Here we will use our estimate for the size of $\mathcal{S}_{n,\delta}(H,H)$.

Proposition 2.4.4. *Suppose $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$, H is a subgroup of G and δ is a constant satisfying $0 < \delta < \frac{1}{3\log_p(|G|)}$. Then, we have*

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(H,H)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n\rceil,\delta}(H,H)} \mathbb{P}\left[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \textit{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = 1.$$

Proof. Let $n_1 = n$ and $n_2 = \lceil \alpha n \rceil$. Corollary 2.4.3 implies that

$$\Bigg| \Bigg(\sum_{F_1 \in \mathcal{S}_{n_1,\delta}(H,H)} \sum_{F_2 \in \mathcal{S}_{n_2,\delta}(H,H)} \mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left| \gamma(M_{n_1,n_2}) - \tfrac{1}{p} n_1 \right| \le \rho n_1 \right] \Bigg) \\ - \frac{|\mathcal{S}_{n_1,\delta}(H,H)|\, |\mathcal{S}_{n_2,\delta}(H,H)|}{|H|^{n_1+n_2}} \Bigg| \\ \le 4 n_1 \, |H| \exp\Big(- \frac{\epsilon \delta \alpha n_1}{|G|^2} \Big) + 2 \exp\big(- 2\rho^2 n_1 \big).$$

Lemma 2.3.10 tells us that

$$|H|^{n_1} - K_G \, |H|^{n_1} \Big(\exp(-c_{G,\delta} n_1) + 2^{-n_1} \Big) \le |\mathcal{S}_{n_1,\delta}(H,H)| \le |H|^{n_1},$$

and

$$|H|^{n_2} - K_G \, |H|^{n_2} \Big(\exp(-c_{G,\delta} n_2) + 2^{-n_2} \Big) \le |\mathcal{S}_{n_2,\delta}(H,H)| \le |H|^{n_2}.$$

Therefore,

$$\Big| |\mathcal{S}_{n_1,\delta}(H,H)| \times |\mathcal{S}_{n_2,\delta}(H,H)| - |H|^{n_1+n_2} \Big| \\ \le K_G \, |H|^{n_1+n_2} \Big(\exp(-c_{G,\delta} n_1) + 2^{-n_1} + \exp(-c_{G,\delta} n_2) + 2^{-n_2} \Big).$$

This implies

$$\left| \frac{|\mathcal{S}_{n_1,\delta}(H,H)| \times |\mathcal{S}_{n_2,\delta}(H,H)|}{|H|^{n_1+n_2}} - 1 \right| \le 2K_G \Big(\exp(-c_{G,\delta} \alpha n_1) + 2^{-\alpha n_1} \Big).$$

The result follows. $\square$

2.4.2 Error term

We are now left with the case when T_1, H_1, T_2, H_2 are not all the same. So at least of the following hold:

- $T_1 \subsetneq H_1$;
- $T_2 \subsetneq H_2$;
- $T_1 \neq T_2$.

We will actually split this further into the following cases:

- $T_1 \subsetneq H_1$;
- $T_2 \subsetneq H_2$;
- $T_1 \not\subseteq T_2$;
- $T_2 \not\subseteq T_1$ and $\alpha \neq 1$;
- $T_1 = H_1$, $T_2 = H_2$, $T_1 \subsetneq T_2$ and $\alpha = 1$.

For $t \in \{1, 2\}$, denote

$$e_t = \begin{cases} 1 - \epsilon & \text{if } T_t \subsetneq H_t \\ 1 & \text{if } T_t = H_t. \end{cases}$$

We will consider $F_1 \in \mathcal{S}_{n_1,\delta}(H_1, T_1)$ and $F_2 \in \mathcal{S}_{n_2,\delta}(H_2, T_2)$ and bound

$$\mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p} n_1\right| \leq \rho n_1\right].$$

We start by bounding the probability that $(F_1, F_2) \circ M_{n_1,n_2} = 0$ and $\Gamma(M_{n_1,n_2}) = S$ for a fixed subset $S \subseteq [n_1]$.

Lemma 2.4.5. *Suppose* $\frac{1}{p} < \alpha \leq 1$ *and* $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$. *Fix* $S \subseteq [n_1]$. *Consider* $F_1 \in \mathcal{S}_{n_1,\delta}(H_1, T_1)$ *and* $F_2 \in \mathcal{S}_{n_2,\delta}(H_2, T_2)$. *Assuming* $\alpha n_1 \leq n_2 \leq n_1$ *and that* n_1 *is sufficiently large in terms of* $G, \alpha, \delta, \epsilon$, *then*

$$\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \textit{ and } \Gamma(M_{n_1,n_2}) = S] \\
&\leq (\tfrac{1}{p})^{|S|} (\tfrac{1}{|G|})^{n_1 - |S|} \frac{e_1^{n_2} e_2^{|S|}}{|T_1|^{n_2} |T_2|^{|S|}} \left(1 + 4\,|G|\, n_1 \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right) \\
&\qquad \times \prod_{i \in [n_1] \setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[l F_2(B_i) = F_1(u_i)].
\end{aligned}$$

Proof. Recall from (2.4) that

$$\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S] \\
&= \prod_{i \in S} \mathbb{P}[c_i F_1(u_i) + F_2(B_i) = 0 \text{ and } c_i \equiv 0 \pmod p] \\
&\qquad \times \prod_{i \in [n_1] \setminus S} \mathbb{P}[c_i F_1(u_i) + F_2(B_i) = 0 \text{ and } c_i \not\equiv 0 \pmod p] \\
&\qquad \times \prod_{j \in [n_2]} \mathbb{P}[d_j F_2(v_j) + F_1(A_j) = 0].
\end{aligned}$$

For each $j \in [n_2]$, we know from Corollary 2.3.6 that

$$\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] \leq e_1 \left(\frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon\delta n_1}{|G|^2}\Big)\right).$$

Similarly, for each $i \in S$, we know by Corollary 2.3.6 that

$$\begin{aligned}
&\mathbb{P}[c_i F_1(u_i) + F_2(B_i) = 0 \text{ and } c_i \equiv 0 \pmod p] \\
&= \mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i \equiv 0 \pmod p]\,\mathbb{P}[c_i \equiv 0 \pmod p] \\
&\leq e_2 \left(\frac{1}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big)\right) \times \frac{1}{p}.
\end{aligned}$$

Finally, consider $i \in [n_1] \setminus S$. Note that even though $c_i \in \mathbb{Z}_p$, the value of $c_i F_1(u_i)$ only depends on $c_i \pmod{|G|}$. Therefore, we see that

$$\begin{aligned}
&\mathbb{P}[c_i F_1(u_i) + F_2(B_i) = 0 \text{ and } c_i \not\equiv 0 \pmod{p}] \\
&= \sum_{k \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[F_2(B_i) = -kF_1(u_i)]\mathbb{P}[c_i \equiv k \pmod{|G|}] \\
&= \frac{1}{|G|} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].
\end{aligned}$$

It follows that

$$\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \Gamma(M_{n_1,n_2}) = S] \\
&\leq (\tfrac{1}{p})^{|S|}(\tfrac{1}{|G|})^{n_1-|S|} e_1^{n_2} \left(\frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon\delta n_1}{|G|^2}\Big)\right)^{n_2} e_2^{|S|} \left(\frac{1}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big)\right)^{|S|} \\
&\qquad \times \prod_{i \in [n_1]\setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].
\end{aligned}$$

If n_1 is sufficiently large to ensure

$$\frac{\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)}{2^{\frac{1}{2n_1}} - 1} < \frac{1}{|G|} \leq \min\Big(\frac{1}{|T_1|}, \frac{1}{|T_2|}\Big),$$

then we are done by Corollary 2.8.5. $\square$

Next, we sum over the different subsets $S \subseteq [n_1]$ that satisfy $\Big||S| - \frac{1}{p}n_1\Big| \leq \rho n_1$ and also over different $F_1 \in \mathcal{S}_{n_1,\delta}(H_1, T_1)$ and $F_2 \in \mathcal{S}_{n_2,\delta}(H_2, T_2)$.

For each $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$, there is some $\sigma \subseteq [n_1]$ with $|\sigma| \leq \delta \log_p(D_1) n_1$ such that $F_1(V_{\setminus\sigma}) \subseteq T_1$. We will consider fixed subsets $\sigma \subseteq [n_1]$ and sum over those $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$ for which $F_1(V_{\setminus\sigma}) \subseteq T_1$. We will denote the sum over such F_1 as $\sum_{F_1:\sigma}$.

Proposition 2.4.6. *Suppose* $\frac{1}{p} < \alpha \leq 1$ *and* $0 < \rho < \min(\alpha - \frac{1}{p}, \frac{1}{p})$. *Assume that the* *subgroups $T_1 \subseteq H_1 \subseteq G$ and $T_2 \subseteq H_2 \subseteq G$ satisfy at least one of the following*

- $T_1 \subsetneq H_1$;
- $T_2 \subsetneq H_2$;
- $T_1 \not\subseteq T_2$;
- $T_2 \not\subseteq T_1$ *and* $\alpha \neq 1$.

Assuming $\delta > 0$ is sufficiently small in terms of these, we have

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(H_2,T_2)} \mathbb{P}\left[(F_1,F_2)\circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = 0.$$

Proof. Denote $D_1 = [H_1 : T_1]$, $D_2 = [H_2 : T_2]$, $n_1 = n$ and $n_2 = \lceil \alpha n \rceil$. First, consider a fixed $S \subseteq [n_1]$. Then we have

$$\begin{aligned}
&\sum_{F_1 \in \mathcal{S}_{n_1,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}_{n_2,\delta}(H_2,T_2)} \mathbb{P}[(F_1,F_2)\circ M_n^{(\alpha)} = 0 \text{ and } \Gamma(M_n^{(\alpha)}) = S] \\
&\leq (\tfrac{1}{p})^{|S|}(\tfrac{1}{|G|})^{n_1-|S|}\frac{e_1^{n_2}e_2^{|S|}}{|T_1|^{n_2}|T_2|^{|S|}}\left(1 + 4|G|\,n_1 \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right) \\
&\quad\times \sum_{F_2 \in \mathcal{S}_{n_2,\delta}(H_2,T_2)} \sum_{F_1 \in \mathcal{S}_{n_1,\delta}(H_1,T_1)} \prod_{i\in[n_1]\setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].
\end{aligned}$$

We will fix a choice of F_2, and bound the sum

$$\sum_{F_1 \in \mathcal{S}_{n_1,\delta}(H_1,T_1)} \prod_{i\in[n_1]\setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].$$

We write $V = \mathbb{Z}_p^{n_1}$. For a subset $\sigma \subseteq [n_1]$, denote by V_σ the subgroup of V generated by u_i for $i \in \sigma$ and $V_{\backslash\sigma}$ to be the subgroup of V generated by u_i for $i \notin \sigma$. Each $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$ with δ-depth D_1 and type (H_1, T_1), has some $\sigma \subseteq [n_1]$ with $|\sigma| = \delta \log_p(D_1) n_1$ such that

$F_1(V_{\setminus\sigma}) \subseteq T_1$ and $F_1(V_\sigma) \subseteq H_1$.

We fix a choice of $\sigma \subseteq [n_1]$ (in addition to fixing F_2 and S).

- For $i \in S \cap \sigma$, we have $|H_1|$ choices for $F_1(u_i)$.
- For $i \in S \setminus \sigma$, we have $|T_1|$ choices for $F_1(u_i)$.
- For $i \in \sigma \setminus S$, $F_1(u_i) \in H_1$, so

$$\sum_{h \in H_1} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = h] = \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) \in H_1] \leq \left|(\mathbb{Z}/|G|\,\mathbb{Z})^\times\right| = (1-\tfrac{1}{p})\,|G|\,.$$

- For $i \in (S \cup \sigma)^c$, $F_1(u_i) \in T_1$, so

$$\sum_{h \in T_1} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = h] = \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) \in T_1] = (1-\tfrac{1}{p})\,|G| \times \mathbb{P}[F_2(B_i) \in T_1].$$

  By Lemma 2.3.7, this is at most

$$(1-\tfrac{1}{p})\,|G| \times \left(\frac{|T_2 \cap T_1|}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big) \right).$$

We conclude that the sum over those F_1 corresponding to σ is bounded by

$$\begin{aligned}
&\sum_{F_1:\sigma} \prod_{i \in [n_1]\setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)] \\
&\leq |H_1|^{|S\cap\sigma|}\,|T_1|^{|S\setminus\sigma|}\,(1-\tfrac{1}{p})^{n_1-|S|}\,|G|^{n_1-|S|} \left(\frac{|T_2 \cap T_1|}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big) \right)^{n_1-|S\cup\sigma|} \\
&\leq D_1^{|\sigma|}\,|T_1|^{|S|}\,(1-\tfrac{1}{p})^{n_1-|S|}\,|G|^{n_1-|S|} \left(\frac{|T_2 \cap T_1|}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n_2}{|G|^2}\Big) \right)^{n_1-|S|-|\sigma|} \\
&\leq |T_1|^{|S|}\,(1-\tfrac{1}{p})^{n_1-|S|}\,|G|^{n_1-|S|} \left(\frac{|T_2 \cap T_1|}{|T_2|} + \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big) \right)^{n_1-|S|} \left(\frac{D_1\,|T_2|}{|T_2 \cap T_1|} \right)^{|\sigma|}.
\end{aligned}$$

Once n_1 is large enough to ensure,

$$\frac{\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)}{2^{\frac{1}{n_1}}-1} < \frac{1}{|G|},$$

then by Corollary 2.8.5 we have

$$\left(\frac{|T_2\cap T_1|}{|T_2|}+\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)^{n_1-|S|} \le \frac{|T_2\cap T_1|^{n_1-|S|}}{|T_2|^{n_1-|S|}}\left(1+2n_1\,|G|\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right).$$

By summing over $\sigma \subseteq [n_1]$ with $|\sigma| = \delta\log_p(D_1)n_1$, we see that

$$\begin{aligned}
&\sum_{F_1\in\mathcal{S}_{n_1,\delta}(H_1,T_1)}\prod_{i\in[n_1]\setminus S}\sum_{l\in(\mathbb{Z}/|G|\mathbb{Z})^\times}\mathbb{P}[lF_2(B_i)=F_1(u_i)]\\
&\le \binom{n_1}{\delta\log_p(D_1)n_1}|T_1|^{|S|}(1-\tfrac{1}{p})^{n_1-|S|}\,|G|^{n_1-|S|}\\
&\quad\times\frac{|T_2\cap T_1|^{n_1-|S|}}{|T_2|^{n_1-|S|}}\left(1+2n_1\,|G|\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)\left(\frac{D_1\,|T_2|}{|T_2\cap T_1|}\right)^{\delta\log_p(D_1)n_1}.
\end{aligned}$$

This implies that

$$\begin{aligned}
&\sum_{F_1\in\mathcal{S}_{n,\delta}(H_1,T_1)}\sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(H_2,T_2)}\mathbb{P}[(F_1,F_2)\circ M_n^{(\alpha)}=0\text{ and }\Gamma(M_n^{(\alpha)})=S]\\
&\le (\tfrac{1}{p})^{|S|}(\tfrac{1}{|G|})^{n_1-|S|}\frac{e_1^{n_2}e_2^{|S|}}{|T_1|^{n_2}\,|T_2|^{|S|}}\left(1+4\,|G|\,n_1\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)\\
&\times\binom{n_2}{\delta n_2\log_p(D_2)}|T_2|^{n_2}\,D_2^{\delta n_2\log_p(D_2)}\times\binom{n_1}{\delta\log_p(D_1)n_1}|T_1|^{|S|}(1-\tfrac{1}{p})^{n_1-|S|}\,|G|^{n_1-|S|}\\
&\times\frac{|T_2\cap T_1|^{n_1-|S|}}{|T_2|^{n_1-|S|}}\left(1+2n_1\,|G|\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)\left(\frac{D_1\,|T_2|}{|T_2\cap T_1|}\right)^{\delta\log_p(D_1)n_1}.
\end{aligned}$$

Rearranging the terms and using the fact that $\binom{a}{b}\le 2^{2\sqrt{ab}}$, we see that the above expression is at most

$$
\begin{aligned}
&(\tfrac{1}{p})^{|S|}(1-\tfrac{1}{p})^{n_1-|S|}e_1^{n_2}e_2^{|S|}\left(\frac{|T_2\cap T_1|}{|T_1|}\right)^{n_2-|S|}\left(\frac{|T_2\cap T_1|}{|T_2|}\right)^{n_1-n_2}\\
&\times 2^{2n_2(\delta\log_p(D_2))^{1/2}}2^{2n_1(\delta\log_p(D_1))^{1/2}}D_2^{\delta n_2\log_p(D_2)}\left(\frac{D_1\,|T_2|}{|T_2\cap T_1|}\right)^{\delta\log_p(D_1)n_1}\\
&\times\left(1+4\,|G|\,n_1\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)\left(1+2n_1\,|G|\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right).
\end{aligned}
$$

Since $e_1, e_2 \leq 1$, $n_2 = \lceil \alpha n\rceil$ and $(\frac{1}{p}-\rho)n \leq |S| \leq (\frac{1}{p}+\rho)n$ we see that

$$
\begin{aligned}
&e_1^{n_2}e_2^{|S|}\left(\frac{|T_2\cap T_1|}{|T_1|}\right)^{n_2-|S|}\left(\frac{|T_2\cap T_1|}{|T_2|}\right)^{n_1-n_2}\\
&\leq\left(e_1^{\alpha}e_2^{\frac{1}{p}-\rho}\left(\frac{|T_2\cap T_1|}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho}\left(\frac{|T_2\cap T_1|}{|T_2|}\right)^{1-\alpha}\right)^{n}\frac{|T_2|}{|T_2\cap T_1|}.
\end{aligned}
$$

Next, note that

$$
\begin{aligned}
&2^{2n_2(\delta\log_p(D_2))^{1/2}}2^{2n_1(\delta\log_p(D_1))^{1/2}}D_2^{\delta n_2\log_p(D_2)}\left(\frac{D_1\,|T_2|}{|T_2\cap T_1|}\right)^{\delta\log_p(D_1)n_1}\\
&\leq 2^{2(\log_p(D_2))^{1/2}}D_2^{\log_p(D_2)}\left(2^{2\alpha(\log_p(D_2))^{1/2}}2^{2(\log_p(D_1))^{1/2}}D_2^{\alpha\log_p(D_2)}\left(\frac{D_1\,|T_2|}{|T_2\cap T_1|}\right)^{\log_p(D_1)}\right)^{n\sqrt{\delta}}\\
&\leq 2^{2(\log_p(|G|))^{1/2}}\,|G|^{\log_p(|G|)}\left(2^{4(\log_p(|G|))^{1/2}}\,|G|^{3\log_p(|G|)}\right)^{n\sqrt{\delta}}.
\end{aligned}
$$

Further note that for sufficiently large n, we have

$$
\left(1+4\,|G|\,n_1\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)\left(1+2n_1\,|G|\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^2}\Big)\right)<2.
$$

We write

$$
B=2^{4(\log_p(|G|))^{1/2}}\,|G|^{3\log_p(|G|)},\qquad b=\frac{|T_2|}{|T_2\cap T_1|}2^{2(\log_p(|G|))^{1/2}}\,|G|^{\log_p(|G|)}\,2.
$$

Then we see that

$$\sum_{F_1 \in \mathcal{S}_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(H_2,T_2)} \mathbb{P}[(F_1,F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \Gamma(M_n^{(\alpha)}) = S]$$
$$\leq (\tfrac{1}{p})^{|S|}(1-\tfrac{1}{p})^{n_1-|S|} b \left(e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_1|} \right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_2|} \right)^{1-\alpha} B^{\sqrt{\delta}} \right)^n .$$

By summing over different S, we see that

$$\sum_{F_1 \in \mathcal{S}_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(H_2,T_2)} \mathbb{P}[(F_1,F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \left| \gamma(M_n^{(\alpha)}) - \tfrac{1}{p} n \right| \leq \rho n]$$
$$\leq b \left(e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_1|} \right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_2|} \right)^{1-\alpha} B^{\sqrt{\delta}} \right)^n .$$

Note that e_1, e_2, $\frac{|T_2 \cap T_1|}{|T_1|}$ and $\frac{|T_2 \cap T_1|}{|T_2|}$ are all at most one. Now, at least one of the following holds

- $T_1 \subsetneq H_1$. In this case $e_1 < 1$ and $\alpha > 0$, so $e_1^{\alpha} < 1$.
- $T_2 \subsetneq H_2$. In this case $e_2 < 1$ and $\frac{1}{p} - \rho > 0$, so $e_2^{\frac{1}{p}-\rho} < 1$.
- $T_1 \not\subseteq T_2$. In this case $\frac{|T_1 \cap T_2|}{|T_1|} < 1$ and $\alpha - \frac{1}{p} - \rho > 0$, so $\left(\frac{|T_1 \cap T_2|}{|T_1|} \right)^{\alpha-\frac{1}{p}-\rho} < 1$.
- $T_2 \not\subseteq T_1$ and $\alpha \neq 1$. In this case $\frac{|T_1 \cap T_2|}{|T_2|} < 1$ and $1 - \alpha > 0$, so $\left(\frac{|T_1 \cap T_2|}{|T_2|} \right)^{1-\alpha} < 1$.

This means that in all cases

$$e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_1|} \right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_2|} \right)^{1-\alpha} < 1.$$

We can therefore choose a sufficiently small δ to ensure that

$$e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_1|} \right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{|T_2 \cap T_1|}{|T_2|} \right)^{1-\alpha} B^{\sqrt{\delta}} < 1.$$

The result follows. ∎

We are only left with the case $T_1 = H_1$, $T_2 = H_2$, $T_1 \subsetneq T_2$ and $\alpha = 1$.

Proposition 2.4.7. *Suppose $\alpha = 1$ and $0 < \rho < \min(\alpha - \frac{1}{p}, \frac{1}{p})$. Assume that the subgroups $T_1 \subseteq H_1 \subseteq G$ and $T_2 \subseteq H_2 \subseteq G$ satisfy $T_1 = H_1$, $T_2 = H_2$ and $T_1 \subsetneq T_2$. For $\delta > 0$, we have*

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,T_1)} \sum_{F_2 \in \mathcal{S}_{n,\delta}(T_2,T_2)} \mathbb{P}\left[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \le \rho n\right] = 0.$$

Proof. Since $\alpha = 1$, $n_1 = n_2 = n$. We have $e_1 = e_2 = 1$, $F_1 \in \mathcal{S}_{n,\delta}(T_1, T_1)$ are codes of distance δn with image T_1 and $F_2 \in \mathcal{S}_{n,\delta}(T_2, T_2)$ are codes of distance δn with image T_2.

By the independence of columns of M_{n_1,n_2}, we have

$$\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0] = \prod_{i\in[n_1]} \mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \prod_{j\in[n_2]} \mathbb{P}[F_1(A_j) = -d_j F_2(v_j)].$$

For each $i \in [n]$, we know by Corollary 2.3.6 that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \le \frac{1}{|T_2|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^2}\Big).$$

For each $j \in [n]$, we know from Corollary 2.3.6 that

$$\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] \le \frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^2}\Big).$$

However, if $F_2(v_j) \in T_2 \setminus T_1$, then we can get a tighter upper bound. Since $F_1(A_j)$ can only take values in T_1, if $F_1(A_j) = -d_j F_2(v_j)$ then $d_j F_2(v_j) \in T_1$. If $F_2(v_j) \notin T_1$, this forces $d_j \equiv 0$

(mod p). We conclude that if $F_2(v_j) \in T_2 \setminus T_1$, then

$$\begin{aligned}
\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] &= \mathbb{P}[F_1(A_j) = -d_j F_2(v_j) \mid d_j F_2(v_j) \in T_1]\mathbb{P}[d_j F_2(v_j) \in T_1] \\
&\leq \left(\frac{1}{|T_1|} + \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right) \mathbb{P}[d_j \equiv 0 \pmod p] \\
&= \frac{1}{p} \left(\frac{1}{|T_1|} + \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right).
\end{aligned}$$

Since F_2 is a code of distance δn with image T_2, we know that

$$|\{j \in [n] : F_2(v_j) \notin T_1\}| \geq \delta n.$$

It follows that

$$\mathbb{P}[(F_1, F_2) \circ M_{n_1, n_2} = 0] \leq \left(\frac{1}{|T_2|} + \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right)^n \left(\frac{1}{p} \right)^{\delta n} \left(\frac{1}{|T_1|} + \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right)^n.$$

Once n is large enough to ensure,

$$\frac{\exp\left(-\frac{\epsilon \delta n}{|G|^2} \right)}{2^{\frac{1}{2n}} - 1} < \frac{1}{|G|},$$

then by Corollary 2.8.5 we know that

$$\mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0] \leq \left(\frac{1}{p} \right)^{\delta n} \frac{1}{|T_2|^n |T_1|^n} \left(1 + 4n |G| \exp\left(-\frac{\epsilon \delta n}{|G|^2} \right) \right).$$

Since $|\mathcal{S}_{n,\delta}(T_1,T_1)| \le |T_1|^n$ and $|\mathcal{S}_{n,\delta}(T_2,T_2)| \le |T_2|^n$, we conclude that

$$\begin{aligned}
&\sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,T_1)} \sum_{F_2 \in \mathcal{S}_{n,\delta}(T_2,T_2)} \mathbb{P}\left[(F_1,F_2)\circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \le \rho n\right] \\
&\le \sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,T_1)} \sum_{F_2 \in \mathcal{S}_{n,\delta}(T_2,T_2)} \mathbb{P}[(F_1,F_2)\circ M_n^{(\alpha)} = 0] \\
&\le \left(\frac{1}{p}\right)^{\delta n}\left(1 + 4n\,|G| \exp\left(-\frac{\epsilon\delta n}{|G|^2}\right)\right).
\end{aligned}$$

The result follows. $\square$

Notice that Proposition 2.4.4, Proposition 2.4.6 and Proposition 2.4.7 together prove Proposition 2.4.1. We have seen that Proposition 2.4.1 implies Proposition 2.2.4, which implies Proposition 2.2.2, which in turn implies Theorem 2.1.7.

2.5 Setup for Laplacian model

We continue to have a fixed finite abelian p-group G, and we wish to estimate the expected number of surjections from $G(L_{n_1,n_2})$ to G.

We denote $\mathrm{Sur}^*(\mathbb{Z}_p^{n_1+n_2}, G)$ to be the set of those maps in $\mathrm{Sur}(\mathbb{Z}_p^{n_1+n_2}, G)$, that are still surjective when restricted to $Z_{n_1+n_2}$. Note that every map in $\mathrm{Sur}(Z_{n_1+n_2}, G)$, can be extended to $|G|$ maps in $\mathrm{Sur}^*(\mathbb{Z}_p^{n_1+n_2}, G)$. Since $L_{n_1,n_2} \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, Z_{n_1+n_2})$, we see that

$$\begin{aligned}
&\mathbb{E}'_\rho[|\mathrm{Sur}(G(L_{n_1,n_2}), G)|] \\
&= \sum_{F \in \mathrm{Sur}(Z_{n_1+n_2}, G)} \mathbb{P}\left[F \circ L_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G) \text{ and } \left|\gamma(L_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \le \rho n_1\right] \\
&= \frac{1}{|G|} \sum_{F \in \mathrm{Sur}^*(\mathbb{Z}_p^{n_1+n_2}, G)} \mathbb{P}\left[F \circ L_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G) \text{ and } \left|\gamma(L_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \le \rho n_1\right].
\end{aligned}$$

We will relate this to our computations with M_{n_1,n_2}. Recall that M_{n_1,n_2} includes c_j and d_i as its entries, but these do not appear in L_{n_1,n_2}. Therefore, the c_j and d_i are independent of the entries of L_{n_1,n_2}. Moreover, they are Haar-uniform, so we see that

$$\begin{aligned}
&\mathbb{P}\left[F\circ L_{n_1,n_2}=0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},G) \text{ and } \left|\gamma(L_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\right]\\
&=\mathbb{P}\left[F\circ L_{n_1,n_2}=0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},G) \text{ and } \left|\gamma(L_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\right]\\
&\times |G|^{n_1+n_2}\prod_{i=1}^{n_1}\mathbb{P}[c_i\equiv -\sum_j b_{ij} \pmod{|G|}]\prod_{j=1}^{n_2}\mathbb{P}[d_j\equiv -\sum_i a_{ij} \pmod{|G|}]\\
&=|G|^{n_1+n_2}\mathbb{P}\Big[F\circ L_{n_1,n_2}=0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},G) \text{ and } \left|\gamma(L_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\\
&\qquad\qquad \text{and } d_j\equiv -\sum_i a_{ij} \pmod{|G|} \text{ and } c_i\equiv -\sum_j b_{ij} \pmod{|G|}\Big]\\
&=|G|^{n_1+n_2}\mathbb{P}\Big[F\circ M_{n_1,n_2}=0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},G) \text{ and } \left|\gamma(M_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\\
&\qquad\qquad \text{and } d_j+\sum_i a_{ij}\equiv 0 \pmod{|G|} \text{ and } c_i+\sum_j b_{ij}\equiv 0 \pmod{|G|}\Big].
\end{aligned}$$

Denote $F_0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},\mathbb{Z}/\left|G\right|\mathbb{Z})$, where F_0 maps a vector to the sum of its entries mod $|G|$. This means that

$$\begin{aligned}
&\mathbb{E}'_\rho[|\operatorname{Sur}(G(L_{n_1,n_2}),G)|]\\
&=|G|^{n_1+n_2-1}\sum_{F\in \operatorname{Sur}^*(\mathbb{Z}_p^{n_1+n_2},G)}\mathbb{P}\Big[(F,F_0)\circ M_{n_1,n_2}=0\in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2},G\oplus \mathbb{Z}/|G|),\left|\gamma(M_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\Big].
\end{aligned}$$

Note that $F\in \operatorname{Sur}^*(\mathbb{Z}_p^{n_1+n_2},G)$ if and only if $(F,F_0)\in \operatorname{Sur}(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/\left|G\right|\mathbb{Z}))$. Denote the projections from $G\oplus(\mathbb{Z}/\left|G\right|\mathbb{Z})$ to G as π_1, and to $\mathbb{Z}/\left|G\right|\mathbb{Z}$ as π_2. Denote

$$\operatorname{Sur}^1(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/\left|G\right|\mathbb{Z})):=\{F\in \operatorname{Sur}(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/\left|G\right|\mathbb{Z})):\pi_2\circ F=F_0\}.$$

We conclude that

$$\begin{aligned}
&\mathbb{E}'_\rho[|\operatorname{Sur}(G(L_{n_1,n_2}),G)|]\\
&=|G|^{n_1+n_2-1}\sum_{F\in \operatorname{Sur}^1(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/|G|\mathbb{Z}))}\mathbb{P}\Big[F\circ M_{n_1,n_2}=0 \text{ and } \left|\gamma(M_{n_1,n_2})-\tfrac{1}{p}n_1\right|\le \rho n_1\Big].
\end{aligned}\tag{2.5}$$

Note that the sum in (2.5) is closely related to the surjective $(G \oplus \mathbb{Z}/|G|\mathbb{Z})$-moment of $\mathrm{Coker}(M_{n_1,n_2})$. The difference is that we are only summing over some of the surjections from $\mathbb{Z}_p^{n_1+n_2}$ to $G \oplus \mathbb{Z}/|G|\mathbb{Z}$. We will use results from the previous section to estimate the probability that $F \circ M_{n_1,n_2} = 0$ and $\left|\gamma(M_{n_1,n_2}) - \frac{1}{p}n_1\right| \leq \rho n_1$.

Also denote

$$\mathrm{Hom}^1(\mathbb{Z}_p^n, G \oplus (\mathbb{Z}/|G|\mathbb{Z})) := \{F \in \mathrm{Hom}(\mathbb{Z}_p^n, G \oplus (\mathbb{Z}/|G|\mathbb{Z})) : \pi_2 \circ F = F_0\}.$$

For $F \in \mathrm{Sur}^1(\mathbb{Z}_p^{n_1+n_2}, G \oplus (\mathbb{Z}/|G|\mathbb{Z}))$, let F_1 be the restriction of F to $\mathbb{Z}_p^{n_1}$ and F_2 be its restriction to $\mathbb{Z}_p^{n_2}$. Then $F_1 \in \mathrm{Hom}^1(\mathbb{Z}_p^{n_1}, G \oplus \mathbb{Z}/|G|\mathbb{Z})$, $F_2 \in \mathrm{Hom}^1(\mathbb{Z}_p^{n_2}, G \oplus \mathbb{Z}/|G|\mathbb{Z})$ and $F_1(\mathbb{Z}_p^{n_1}) + F_2(\mathbb{Z}_p^{n_2}) = G \oplus \mathbb{Z}/|G|\mathbb{Z}$. This means that if F_1 is of type (H_1, T_1) and F_2 is of type (H_2, T_2), then $H_1 + H_2 = G \oplus \mathbb{Z}/|G|\mathbb{Z}$. Moreover, since F maps each basis vector of $\mathbb{Z}_p^n$ to something of the form $(g, 1)$, it follows that π_2 is surjective when restricted to H_1, T_1, H_2 or T_2. That is

$$\pi_2(H_1) = \pi_2(T_1) = \pi_2(H_2) = \pi_2(T_2) = \mathbb{Z}/|G|\mathbb{Z}.$$

Definition 2.5.1. We call a subgroup H of $G \oplus \mathbb{Z}/|G|\mathbb{Z}$, π_2-full if $\pi_2(H) = \mathbb{Z}/|G|\mathbb{Z}$.

Given π_2-full subgroups $T \subseteq H \subseteq G \oplus \mathbb{Z}/|G|\mathbb{Z}$, we denote

$$\mathcal{S}^1_{n,\delta}(H, T) := \{F \in \mathrm{Hom}^1(\mathbb{Z}_p^n, G \oplus \mathbb{Z}/|G|\mathbb{Z}) : \delta - \text{type } (H, T)\}.$$

We will estimate the size of $\mathcal{S}^1_{n,\delta}(H, T)$. We start with the case $T \subsetneq H$. Note that the size of $\mathcal{S}_{n,\delta}(H, T)$ was of the order of $|T|^n$, but the size of $\mathcal{S}^1_{n,\delta}(H, T)$ should be smaller because each basis element has to be mapped to something of the form $(g, 1)$.

Lemma 2.5.2. *Consider $D > 1$ and subgroups $T \subsetneq H \subseteq G \oplus \mathbb{Z}/|G|\mathbb{Z}$ such that H, T are both π_2-full and $[H : T] = D$. Then we have*

$$\left|\mathcal{S}^1_{n,\delta}(H,T)\right| \leq 2^{n\sqrt{2\delta\log_p(|G|)}} \frac{|T|^n}{|G|^n} D^{\delta\log_p(D)n}.$$

Proof. Any $F \in \mathcal{S}^1_{n,\delta}(H,T)$ would have a $\sigma \subseteq [n]$, such that $|\sigma| < \delta\log_p(D)n$ and $F(V_{\setminus\sigma}) \subseteq T$, $F(V_\sigma) \subseteq H$. By enlarging σ, we can assume that $|\sigma| = \lceil\delta\log_p(D)n\rceil - 1$.

Now there are $\binom{n}{\lceil\delta\log_p(D)n\rceil-1}$ choices for σ and once we choose σ then:

- For $i \in \sigma$, $F(v_i) \in H \cap \pi_2^{-1}(1)$. Since H is π_2-full $\left|H \cap \pi_2^{-1}(1)\right| = \frac{|H|}{|G|} = D\frac{|T|}{|G|}$, so $F(v_i)$ has $D\frac{|T|}{|G|}$ choices.

- For $i \notin \sigma$, $F(v_i) \in T \cap \pi_2^{-1}(1)$. Since T is also π_2-full $\left|T \cap \pi_2^{-1}(1)\right| = \frac{|T|}{|G|}$, so $F(v_i)$ has $\frac{|T|}{|G|}$ choices.

The result follows since $\binom{n}{\lceil\delta\log_p(D)n\rceil-1} \leq 2^{n\sqrt{\delta\log_p(|G|^2)}}$. $\square$

For ease of notation we denote $L_G = K_{G\oplus\mathbb{Z}/|G|\mathbb{Z}}$, the number of subgroups of $G \oplus \mathbb{Z}/|G|\mathbb{Z}$. We will now estimate the size of $\mathcal{S}^1_{n,\delta}(H,H)$ for $H = G \oplus \mathbb{Z}/|G|\mathbb{Z}$. We do not need this estimate for other H.

Lemma 2.5.3. *Consider $0 < \delta < \frac{1}{6\log_p(|G|)}$. There is a constant $c_{G,\delta} > 0$ (depending on G and δ), such that*

$$|G|^n \left(1 - L_G\exp(-c_{G,\delta}n) - L_G 2^{-n}\right) \leq \left|\mathcal{S}^1_{n,\delta}(G\oplus\mathbb{Z}/|G|\mathbb{Z}, G\oplus\mathbb{Z}/|G|\mathbb{Z})\right| \leq |G|^n.$$

Proof. The upper bound follows from the fact that

$$\mathcal{S}^1_{n,\delta}(G\oplus\mathbb{Z}/|G|\mathbb{Z}, G\oplus\mathbb{Z}/|G|\mathbb{Z}) \subseteq \mathrm{Hom}^1(\mathbb{Z}_p^n, G\oplus\mathbb{Z}/|G|\mathbb{Z}).$$

Moreover,

$$\begin{aligned}&\operatorname{Hom}^1(\mathbb{Z}_p^n, G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z})\setminus\mathcal{S}^1_{n,\delta}(G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z}, G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z})\\&=\bigcup_{T\subsetneq G\oplus\mathbb{Z}/|G|\mathbb{Z}}\mathcal{S}^1_{n,\delta}(G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z}, T)\cup\operatorname{Hom}^1(\mathbb{Z}_p^n, T).\end{aligned}$$

The number of T is at most L_G, and

$$\left|\operatorname{Hom}^1(\mathbb{Z}_p^n, T)\right| = \frac{\left|T\right|^n}{\left|G\right|^n}\leq\frac{\left|G\right|^{2n}}{2^n\left|G\right|^n}.$$

Denote $[G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z} : T] = D > 1$. Then we know that

$$\left|\mathcal{S}^1_{n,\delta}(G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z}, T)\right|\leq 2^{n\sqrt{2\delta\log_p(|G|)}}\frac{\left|G\right|^{2n}}{\left|G\right|^n}D^{-n+\delta\log_p(D)n}\leq\left|G\right|^n\left(2^{\sqrt{2\delta\log_p(|G|)}-1+\delta\log_p(|G|^2)}\right)^n.$$

The bound on δ also ensures that $\sqrt{2\delta\log_p(|G|)}-1+2\delta\log_p(|G|) < 0$. The result follows. $\square$

Now consider $F\in\mathcal{S}^1_{n,\delta}(H, T)$, for π_2-full subgroups $T\subseteq H\subseteq G\oplus\mathbb{Z}/\left|G\right|\mathbb{Z}$. Let $X\in\mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced.

- If $T = H$, then Lemma 2.3.4 implies that for every $f\in H$, we have

$$\left|\mathbb{P}[F(X) = f] - \frac{1}{|H|}\right|\leq\exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big).$$

- Denote

$$e = \begin{cases}1 & \text{if } T = H\\ 1-\epsilon & \text{if } T\subsetneq H.\end{cases}$$

Then by Corollary 2.3.6 for every $f \in G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}$, we have

$$\mathbb{P}[F(X) = f] \leq e\left(\frac{1}{|T|} + \exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big)\right).$$

- In Lemma 2.3.7 we bounded the probability that $F(X)$ belongs to another subgroup. However, for the Laplacian model, we will need to bound the probability that $F(X)$ belongs to another subgroup and $\pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times$.

We first bound the probability that $F(X)$ belongs to another subgroup and $\pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times$, for $F \in \mathcal{S}^1_{n,\delta}(H, T)$ with $T = H$.

Lemma 2.5.4. *Suppose $\delta > 0$ and $T, T' \subseteq G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}$ are π_2-full subgroups. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then, for every $F \in \mathcal{S}^1_{n,\delta}(T, T)$ we have*

$$\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \leq \left((1-\tfrac{1}{p})\frac{|T \cap T'|}{|T|} + \left|G\right|^2 \exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big)\right).$$

Proof. We know that T and T' are all π_2-full. We divide the proof into two cases based on whether $T \cap T'$ is π_2-full or not.

1. Case 1: $T \cap T'$ is not π_2-full. In this case, if $F(X) \in T'$, then $F(X) \in T \cap T'$, so $\pi_2(F(X)) \notin (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times$. Therefore,

   $$\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] = 0.$$

   The result follows.

2. Case 2: $T \cap T'$ is π_2-full. Then we know that

   $$\left|(T \cap T') \cap \pi_2^{-1}((\mathbb{Z}/\left|G\right|\mathbb{Z})^\times)\right| = (1-\tfrac{1}{p})\left|(T \cap T')\right|.$$

Therefore, Lemma 2.3.4 says that

$$\begin{aligned}
&\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \\
&= \mathbb{P}[F(X) \in (T \cap T') \cap \pi_2^{-1}((\mathbb{Z}/\left|G\right|\mathbb{Z})^\times)] \\
&\leq (1 - \tfrac{1}{p}) \left|T \cap T'\right| \left(\frac{1}{|T|} + \exp\Big(- \frac{\epsilon \delta n}{|G|^4} \Big) \right).
\end{aligned}$$

The result follows. $\square$

Next, we bound the probability that $F(X)$ belongs to another subgroup and $\pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times$, for $F \in \mathcal{S}^1_{n,\delta}(H,T)$ without the requirement that $T = H$. This leads to a slightly weaker bound.

Lemma 2.5.5. *Suppose $\delta > 0$, $T \subseteq H \subseteq G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}$ are π_2-full subgroups, and $T' \subseteq G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}$, is another π_2-full subgroup. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then, for every $F \in \mathcal{S}^1_{n,\delta}(H,T)$*

$$\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \leq \left((1 - \tfrac{1}{p}) \frac{\min(|T|, |T'|)}{|T|} + |G|^2 \exp\Big(- \frac{\epsilon \delta n}{|G|^4} \Big) \right).$$

Proof. Denote $D = [H : T]$. We know that H, T and T' are all π_2-full. We divide the proof into two cases based on whether $T \cap T'$ is π_2-full or not.

1. Case 1: $T \cap T'$ is not π_2-full. Since T and T' are both π_2-full, this implies that $T \cap T'$ is a proper subset of both T and of T'. This means that

   $$\left|T \cap T'\right| \leq \tfrac{1}{p} \min(|T|, |T'|) \leq (1 - \tfrac{1}{p}) \min(|T|, |T'|).$$

   Moreover, Lemma 2.3.7 implies that

$$\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \leq \mathbb{P}[F(X) \in T'] \leq \left(\frac{\left|T \cap T'\right|}{|T|} + \exp\Big(- \frac{\epsilon \delta n}{|G|^4} \Big) \right).$$

The result follows.

2. Case 2: $T \cap T'$ is π_2-full. There is some $\sigma \subseteq [n]$ with $|\sigma| \leq \delta n \log_p(D)$ such that $F(V_{\setminus\sigma}) = T$. Recall that $V_{\setminus\sigma}$ is the submodule of $\mathbb{Z}_p^n$ generated by those basis vectors u_i for which $i \notin \sigma$. Let V_σ be the submodule generated by u_i with $i \in \sigma$. Now,

$$F \in \operatorname{Hom}(V_{\setminus\sigma} \oplus V_\sigma, G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}) = \operatorname{Hom}(V_{\setminus\sigma}, G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}) \oplus \operatorname{Hom}(V_\sigma, G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}),$$

so we can decompose $F = (F_{\setminus\sigma}, F_\sigma)$ and $X = (X_{\setminus\sigma}, X_\sigma)$. We know that

$$F(X) = F_{\setminus\sigma}(X_{\setminus\sigma}) + F_\sigma(X_\sigma).$$

Thus $F(X) \in T'$ if and only if $F_{\setminus\sigma}(X_{\setminus\sigma}) \equiv -F_\sigma(X_\sigma) \pmod{T'}$. Similarly, $\pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times$ if and only if $\pi_2(F_{\setminus\sigma}(X_{\setminus\sigma})) \not\equiv -\pi_2(F_\sigma(X_\sigma)) \pmod{p}$. By conditioning based on the value of $F_\sigma(X_\sigma)$, we see that

$$\begin{aligned}
&\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \\
&= \sum_{h_0 \in H} \mathbb{P}[F_\sigma(X_\sigma) = h_0]\mathbb{P}[F_{\setminus\sigma}(X_{\setminus\sigma}) \equiv -h_0 (\text{mod } T'), \pi_2(F_{\setminus\sigma}(X_{\setminus\sigma})) \not\equiv -\pi_2(h_0) (\text{mod } p)].
\end{aligned}$$

For $h_0 \in H$, define

$$\begin{aligned}
S_1(h_0) &= \{h \in T : h \equiv -h_0 \pmod{T'}\}, \\
S_2(h_0) &= \{h \in T : h \equiv -h_0 \pmod{T'} \text{ and } \pi_2(h) \not\equiv -\pi_2(h_0) \pmod{p}\}.
\end{aligned}$$

This means that,

$$\begin{aligned}
&\mathbb{P}[F(X) \in T' \text{ and } \pi_2(F(X)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times] \\
&= \sum_{h_0 \in H} \mathbb{P}[F_\sigma(X_\sigma) = h_0]\mathbb{P}[F_{\setminus\sigma}(X_{\setminus\sigma}) \in S_2(h_0)].
\end{aligned}$$

We will show that for each h_0, $|S_2(h_0)| \leq (1 - \frac{1}{p})\, |T \cap T'|$.

- If $S_1(h_0) = \emptyset$, then this is trivially true.
- If $S_1(h_0) \neq \emptyset$, then pick $h_1 \in S_1(h_0)$. It follows that $S_1(h_0) = h_1 + T \cap T'$. Since $\pi_2(T \cap T') = \mathbb{Z}/\, |G|\, \mathbb{Z}$ (this is because we are in Case 2), it follows that $|S_2(h_0)| \leq (1 - \frac{1}{p})\, |T \cap T'|$.

By an identical argument to the one in Lemma 2.3.7, we see that $F_{\setminus\sigma}$ is a code of distance δn with image T. Therefore, Lemma 2.3.4 says that

$$\mathbb{P}[F_{\setminus\sigma}(X_{\setminus\sigma}) \in S_2(h_0)] \leq |S_2(h_0)| \left(\frac{1}{|T|} + \exp\Big(- \frac{\epsilon \delta n}{|G|^4} \Big) \right).$$

The result follows since $|S_2(h_0)| \leq (1 - \frac{1}{p})\, |T \cap T'|$.

$\square$

If we take $T' = G \oplus \mathbb{Z}/\, |G|\, \mathbb{Z}$, then $F(X) = T'$ is automatic. We are therefore left with the probability that $\pi_2(F(X)) \in (\mathbb{Z}/\, |G|\, \mathbb{Z})^{\times}$. We note this in a corollary.

Corollary 2.5.6. *Suppose $\delta > 0$, $T \subseteq H \subseteq G \oplus \mathbb{Z}/\, |G|\, \mathbb{Z}$ are π_2-full subgroups. Let $X \in \mathbb{Z}_p^n$ be a random vector whose entries are independent and ϵ-balanced. Then, for every $F \in \mathcal{S}^1_{n,\delta}(H, T)$*

$$\mathbb{P}[\pi_2(F(X)) \in (\mathbb{Z}/\, |G|\, \mathbb{Z})^{\times}] \leq \left((1 - \tfrac{1}{p}) + |G|^2 \exp\Big(- \frac{\epsilon \delta n}{|G|^4} \Big) \right).$$

Proof. Take $T' = G \oplus \mathbb{Z}/\, |G|\, \mathbb{Z}$. $\square$

2.6 Laplacian model

Recall the following:

1. We had shown in (2.5) that

$$\begin{aligned}&\mathbb{E}'_{\rho}[|\mathrm{Sur}(G(L_{n_1,n_2}),G)|]\\&=|G|^{n_1+n_2-1}\sum_{F\in\mathrm{Sur}^1(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/|G|\mathbb{Z}))}\mathbb{P}\Big[F\circ M_{n_1,n_2}=0\text{ and }\Big|\gamma(M_{n_1,n_2})-\tfrac{1}{p}n_1\Big|\leq\rho n_1\Big].\end{aligned}$$

2. Each $F\in\mathrm{Sur}^1(\mathbb{Z}_p^{n_1+n_2},G\oplus(\mathbb{Z}/|G|\mathbb{Z}))$, can be decomposed as (F_1,F_2), with $F_1\in\mathrm{Hom}^1(\mathbb{Z}_p^{n_1},G\oplus\mathbb{Z}/|G|\mathbb{Z})$, $F_2\in\mathrm{Hom}^1(\mathbb{Z}_p^{n_2},G\oplus\mathbb{Z}/|G|\mathbb{Z})$ satisfying $\mathrm{Im}(F_1)+\mathrm{Im}(F_2)=G\oplus\mathbb{Z}/|G|\mathbb{Z}$.

3. Given $\delta>0$, the set of (F_1,F_2) appearing this way can be partitioned as follows: Consider H_1 and H_2 to be π_2-full subgroups of $G\oplus\mathbb{Z}/|G|\mathbb{Z}$ such that $H_1+H_2=G\oplus\mathbb{Z}/|G|\mathbb{Z}$. Let T_1 be a π_2-full subgroup of H_1 and T_2 be a π_2-full subgroup of H_2. Then we consider $F_1\in\mathcal{S}^1_{n_1,\delta}(H_1,T_1)$ and $F_2\in\mathcal{S}^1_{n_2,\delta}(H_2,T_2)$. On each such piece, our goal is to estimate

$$\mathbb{P}\Big[(F_1,F_2)\circ M_{n_1,n_2}=0\text{ and }\Big|\gamma(M_{n_1,n_2})-\tfrac{1}{p}n_1\Big|\leq\rho n_1\Big].$$

We will show the following.

Proposition 2.6.1. *Given $\frac{1}{p}<\alpha\leq 1$ and $0<\rho<\min(\frac{1}{p},\alpha-\frac{1}{p})$ and a finite abelian p-group G, there is $\delta>0$, such that for any π_2-full subgroups $T_1\subseteq H_1\subseteq G\oplus\mathbb{Z}/|G|\mathbb{Z}$, $T_2\subseteq H_2\subseteq G\oplus\mathbb{Z}/|G|\mathbb{Z}$ with $H_1+H_2=G\oplus\mathbb{Z}/|G|\mathbb{Z}$, we have*

$$\begin{aligned}&\lim_{n\to\infty}|G|^{n+\lceil\alpha n\rceil-1}\sum_{F_1\in\mathcal{S}^1_{n,\delta}(H_1,T_1)}\sum_{F_2\in\mathcal{S}^1_{\lceil\alpha n\rceil,\delta}(H_2,T_2)}\mathbb{P}\left[(F_1,F_2)\circ M_n^{(\alpha)}=0\textit{ and }\Big|\gamma(M_n^{(\alpha)})-\tfrac{1}{p}n\Big|\leq\rho n\right]\\&\quad=\begin{cases}\frac{1}{|G|} & \textit{if } T_1=H_1=T_2=H_2=G\oplus\mathbb{Z}/|G|\mathbb{Z}\\ 0 & \textit{otherwise.}\end{cases}\end{aligned}$$

This will imply Proposition 2.2.5.

Proposition 2.2.5. Given $\frac{1}{p} < \alpha \le 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and a finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{E}_\rho[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), G)\right|] = \frac{1}{|G|}.$$

Proof of Proposition 2.2.5 assuming Proposition 2.6.1. Proposition 2.6.1 implies that

$$\lim_{n\to\infty} \mathbb{E}'_\rho[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), G)\right|] = \frac{1}{|G|}.$$

The result follows from Corollary 2.8.2. □

2.6.1 Main term

In this subsection, we consider the case

$$H_1 = H_2 = T_1 = T_2 = G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}.$$

These will contribute to the main term. In this case F_1 and F_2 are codes of distance δn_1 and δn_2 respectively with image $G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}$, we can therefore use Corollary 2.4.3.

Lemma 2.6.2. *Suppose $\frac{1}{p} < \alpha \le 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and $0 < \delta < \frac{1}{6\log_p(|G|)}$ and L_G, $c_{G,\delta}$ be the constants from Lemma 2.5.3. Suppose $\alpha n_1 \le n_2 \le n_1$. Denote $S_1 = \mathcal{S}^1_{n_1,\delta}(G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}, G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z})$ and $S_2 = \mathcal{S}^1_{n_2,\delta}(G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z}, G \oplus \mathbb{Z}/\left|G\right|\mathbb{Z})$. Then, for sufficiently large values of n_1 (depending on $G, \epsilon, \delta, \alpha$), we have*

$$\left| \left|G\right|^{n_1+n_2-1} \left(\sum_{F_1\in S_1} \sum_{F_2 \in S_2} \mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p} n_1\right| \le \rho n_1 \right] \right) - \frac{1}{|G|} \right|$$
$$\le 4n_1 \left|G\right| \exp\Big(- \frac{\epsilon\delta\alpha n_1}{|G|^4}\Big) + \frac{2}{|G|} \exp\big(- 2\rho^2 n_1\big) + \frac{2L_G}{|G|}\exp(-c_{G,\delta}\alpha n_1) + \frac{2L_G}{|G|} 2^{-\alpha n_1}.$$

Proof. We know from Corollary 2.4.3 that for sufficiently large values of n_1, for each $F_1 \in S_1$ and $F_2 \in S_2$, we have

$$\left|\mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right] - \frac{1}{|G|^{2(n_1+n_2)}}\right|$$
$$\leq 4n_1 \frac{1}{|G|^{2(n_1+n_2-1)}} \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big) + \frac{2}{|G|^{2(n_1+n_2)}} \exp\big(-2\rho^2 n_1\big).$$

We sum over these F_1 and F_2. As an upper bound we use $|S_1| \leq \left|\mathrm{Hom}^1(\mathbb{Z}_p^{n_1}, G \oplus \mathbb{Z}/\,|G|\,\mathbb{Z})\right| = |G|^{n_1}$, $|S_2| \leq \left|\mathrm{Hom}^1(\mathbb{Z}_p^{n_2}, G \oplus \mathbb{Z}/\,|G|\,\mathbb{Z})\right| = |G|^{n_2}$.

$$\left|\left(\sum_{F_1 \in S_1} \sum_{F_2 \in S_2} \mathbb{P}\left[(F_1, F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p}n_1\right| \leq \rho n_1\right]\right) - \frac{|S_1|\,|S_2|}{|G|^{2(n_1+n_2)}}\right|$$
$$\leq 4n_1 \frac{1}{|G|^{n_1+n_2-2}} \exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big) + 2\frac{1}{|G|^{n_1+n_2}} \exp\big(-2\rho^2 n_1\big).$$

By Lemma 2.5.3 we see that

$$|G|^{n_1} - L_G\,|G|^{n_1}\left(\exp(-c_{G,\delta} n_1) + 2^{-n_1}\right) \leq |S_1| \leq |G|^{n_1},$$

and

$$|G|^{n_2} - L_G\,|G|^{n_2}\left(\exp(-c_{G,\delta} n_2) + 2^{-n_2}\right) \leq |S_2| \leq |G|^{n_2}.$$

Therefore,

$$\left|\,|S_1|\,|S_2| - |G|^{n_1+n_2}\,\right| \leq L_G\,|G|^{n_1+n_2}\left(\exp(-c_{G,\delta} n_1) + 2^{-n_1} + \exp(-c_{G,\delta} n_2) + 2^{-n_2}\right).$$

This implies

$$\left|\frac{|S_1|\,|S_2|}{|G|^{n_1+n_2}} - 1\right| \leq 2L_G\Big(\exp(-c_{G,\delta}\alpha n_1) + 2^{-\alpha n_1}\Big).$$

We conclude that

$$\begin{aligned}
&\left| |G|^{n_1+n_2-1} \left(\sum_{F_1 \in S_1} \sum_{F_2 \in S_2} \mathbb{P}[(F_1,F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p} n_1\right| \le \rho n_1] \right) - \frac{1}{|G|} \right| \\
&\le |G|^{n_1+n_2-1} \left| \left(\sum_{F_1 \in S_1} \sum_{F_2 \in S_2} \mathbb{P}[(F_1,F_2) \circ M_{n_1,n_2} = 0 \text{ and } \left|\gamma(M_{n_1,n_2}) - \tfrac{1}{p} n_1\right| \le \rho n_1] \right) - \frac{|S_1|\,|S_2|}{|G|^{2(n_1+n_2)}} \right| \\
&\qquad + \frac{1}{|G|} \left| \frac{|S_1|\,|S_2|}{|G|^{n_1+n_2}} - 1 \right| \\
&\le 4 n_1 |G| \exp\Big(-\frac{\epsilon \delta \alpha n_1}{|G|^4} \Big) + 2 \frac{1}{|G|} \exp\big(-2\rho^2 n_1 \big) + 2 L_G \frac{1}{|G|} \Big(\exp(-c_{G,\delta} \alpha n_1) + 2^{-\alpha n_1} \Big).
\end{aligned}$$

The result follows. □

By setting $n_2 = \lceil \alpha n_1 \rceil$ and letting $n_1 \to \infty$, we obtain the following.

Proposition 2.6.3. *Suppose $\frac{1}{p} < \alpha \le 1$, $0 < \rho < \min(\frac{1}{p}, \alpha - \frac{1}{p})$ and $0 < \delta < \frac{1}{6 \log_p(|G|)}$. Denote $S_1 = \mathcal{S}^1_{n,\delta}(G \oplus \mathbb{Z}/|G|\mathbb{Z}, G \oplus \mathbb{Z}/|G|\mathbb{Z})$ and $S_2 = \mathcal{S}^1_{\lceil \alpha n \rceil,\delta}(G \oplus \mathbb{Z}/|G|\mathbb{Z}, G \oplus \mathbb{Z}/|G|\mathbb{Z})$. Then, we have*

$$\lim_{n\to\infty} |G|^{n+\lceil \alpha n \rceil - 1} \sum_{F_1 \in S_1} \sum_{F_2 \in S_2} \mathbb{P}[(F_1,F_2) \circ M_n^{(\alpha)} = 0 \textit{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p} n\right| \le \rho n] = \frac{1}{|G|}.$$

2.6.2 Error term

We are now left with the case when T_1, H_1, T_2, H_2, $G \oplus \mathbb{Z}/|G|\mathbb{Z}$ are not all the same. Since $H_1 + H_2 = G \oplus \mathbb{Z}/|G|\mathbb{Z}$, at least of the following must hold:

- $T_1 \subsetneq H_1$;
- $T_2 \subsetneq H_2$;
- $T_1 \ne T_2$.

We will actually split this further into the following cases:

- $T_1 \subsetneq H_1$;

- $T_2 \subsetneq H_2$;

- $T_1 \not\subseteq T_2$ and $T_2 = H_2$;

- $T_2 \not\subseteq T_1$, $T_2 = H_2$ and $\alpha \neq 1$;

- $T_1 = H_1$, $T_2 = H_2$, $T_1 \subsetneq T_2$ and $\alpha = 1$.

For $t \in \{1, 2\}$, denote

$$e_t = \begin{cases} 1 - \epsilon & \text{if } T_t \subsetneq H_t \\ 1 & \text{if } T_t = H_t. \end{cases}$$

We will consider $F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1, T_1)$ and $F_2 \in \mathcal{S}^1_{n_2,\delta}(H_2, T_2)$.

Proposition 2.6.4. *Suppose $\frac{1}{p} < \alpha \leq 1$ and $0 < \rho < \min(\alpha - \frac{1}{p}, \frac{1}{p})$. Consider π_2-full subgroups $T_1 \subseteq H_1 \subseteq G \oplus \mathbb{Z}/|G|\mathbb{Z}$ and $T_2 \subseteq H_2 \subseteq G \oplus \mathbb{Z}/|G|\mathbb{Z}$ that satisfy at least one of the following*

- *$T_1 \subsetneq H_1$;*

- *$T_2 \subsetneq H_2$;*

- *$T_1 \not\subseteq T_2$ and $T_2 = H_2$;*

- *$T_2 \not\subseteq T_1$, $T_2 = H_2$ and $\alpha \neq 1$.*

Assuming $\delta > 0$ is sufficiently small in terms of these, we have

$$\lim_{n\to\infty} |G|^{n+\lceil \alpha n\rceil - 1} \sum_{F_1 \in \mathcal{S}^1_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{\lceil \alpha n\rceil,\delta}(H_2,T_2)} \mathbb{P}\left[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = 0.$$

Proof. Denote $D_1 = [H_1 : T_1]$, $D_2 = [H_2 : T_2]$, $n_1 = n$ and $n_2 = \lceil \alpha n \rceil$. First, consider a fixed $S \subseteq [n_1]$. By Lemma 2.4.5 we know that

$$\sum_{F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{n_2,\delta}(H_2,T_2)} \mathbb{P}[(F_1,F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \Gamma(M_n^{(\alpha)}) = S]$$
$$\leq (\tfrac{1}{p})^{|S|} (\tfrac{1}{|G|})^{n_1 - |S|} \frac{e_1^{n_2} e_2^{|S|}}{|T_1|^{n_2} |T_2|^{|S|}} \left(1 + 4\,|G|^2\, n_1 \exp\Big(-\frac{\epsilon \delta \alpha n_1}{|G|^4}\Big)\right)$$
$$\times \sum_{F_2 \in \mathcal{S}^1_{n_2,\delta}(H_2,T_2)} \sum_{F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)} \prod_{i \in [n_1] \setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].$$

We will fix a choice of F_2, and bound the sum

$$\sum_{F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)} \prod_{i \in [n_1] \setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)].$$

We write $V = \mathbb{Z}_p^{n_1}$. For a subset $\sigma \subseteq [n_1]$, denote by V_σ the subgroup of V generated by u_i for $i \in \sigma$ and $V_{\backslash \sigma}$ to be the subgroup of V generated by u_i for $i \notin \sigma$. Each $F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)$, has some $\sigma \subseteq [n_1]$ with $|\sigma| = \delta \log_p(D_1) n_1$ such that $F_1(V_{\backslash\sigma}) \subseteq T_1$ and $F_1(V_\sigma) \subseteq H_1$.

We fix a choice of $\sigma \subseteq [n_1]$ (in addition to fixing F_2 and S).

- For $i \in S \cap \sigma$, since H_1 is π_2-full the number of choices for $F_1(u_i)$ is

$$\left|H_1 \cap \pi_2^{-1}(1)\right| = \frac{|H_1|}{|G|}.$$

- For $i \in S \setminus \sigma$, since T_1 is π_2-full the number of choices for $F_1(u_i)$ is

$$\left|T_1 \cap \pi_2^{-1}(1)\right| = \frac{|T_1|}{|G|}.$$

- For $i \in \sigma \setminus S$, $F_1(u_i) \in H_1 \cap \pi_2^{-1}(1)$,

$$\begin{aligned}\sum_{h \in H_1 \cap \pi_2^{-1}(1)} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = h] &= \sum_{k \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \sum_{h \in H_1 \cap \pi_2^{-1}(1)} \mathbb{P}[F_2(B_i) = kh] \\ &\leq \sum_{k \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[\pi_2(F_2(B_i)) = k] \\ &= \mathbb{P}[\pi_2(F_2(B_i)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times].\end{aligned}$$

  By Corollary 2.5.6, this is at most

$$\Big((1 - \tfrac{1}{p}) + \left|G\right|^2 \exp\Big(-\frac{\epsilon\delta n_2}{|G|^4}\Big)\Big).$$

- For $i \in (S \cup \sigma)^c$, $F_1(u_i) \in T_1 \cap \pi_2^{-1}(1)$, so

$$\begin{aligned}\sum_{h \in T_1 \cap \pi_2^{-1}(1)} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = h] &= \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) \in T_1 \cap \pi_2^{-1}(1)] \\ &= \mathbb{P}[F_2(B_i) \in T_1 \text{ and } \pi_2(F_2(B_i)) \in (\mathbb{Z}/\left|G\right|\mathbb{Z})^\times].\end{aligned}$$

  Denote

$$A = \begin{cases} |T_1 \cap T_2| & \text{if } T_2 = H_2 \\ \min(\left|T_1\right|, \left|T_2\right|) & \text{if } T_2 \subsetneq H_2. \end{cases}$$

  By Lemma 2.5.4 and Lemma 2.5.5, this is at most

$$\Big((1 - \tfrac{1}{p})\frac{A}{|T_2|} + \left|G\right|^2 \exp\Big(-\frac{\epsilon\delta n_2}{|G|^4}\Big)\Big).$$

We conclude that the sum over those F_1 corresponding to σ is bounded by

$$
\begin{aligned}
&\sum_{F_1:\sigma}\prod_{i\in[n_1]\setminus S}\sum_{l\in(\mathbb{Z}/|G|\mathbb{Z})^\times}\mathbb{P}[lF_2(B_i)=F_1(u_i)]\\
&\le\left(\frac{|H_1|}{|G|}\right)^{|S\cap\sigma|}\left(\frac{|T_1|}{|G|}\right)^{|S\setminus\sigma|}\left((1-\tfrac{1}{p})+|G|^2\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big)\right)^{|\sigma\setminus S|}\\
&\quad\times\left((1-\tfrac{1}{p})\frac{A}{|T_2|}+|G|^2\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big)\right)^{n_1-|S\cup\sigma|}.
\end{aligned}
$$

Once n_1 is large enough to ensure that

$$
\frac{|G|^2\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big)}{2^{\frac{1}{n_1}}-1}\le(1-\tfrac{1}{p})\frac{1}{|G|^2},
$$

then by Corollary 2.8.5, the expression above is bounded by

$$
\left(\frac{|H_1|}{|G|}\right)^{|S\cap\sigma|}\left(\frac{|T_1|}{|G|}\right)^{|S\setminus\sigma|}(1-\tfrac{1}{p})^{n_1-|S|}\left(\frac{A}{|T_2|}\right)^{n_1-|S\cup\sigma|}\left(1+2n_1\frac{|G|^2}{1-\frac{1}{p}}|G|^2\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big)\right).
$$

Note that

$$
\left(\frac{|H_1|}{|G|}\right)^{|S\cap\sigma|}\left(\frac{|T_1|}{|G|}\right)^{|S\setminus\sigma|}\le\left(\frac{|T_1|}{|G|}\right)^{|S|}D_1^{|\sigma|},
$$

$\left(\frac{A}{|T_2|}\right)^{n_1-|S\cup\sigma|}\le\left(\frac{A}{|T_2|}\right)^{n_1-|S|-|\sigma|}$ and for sufficiently large n_1

$$
\left(1+2n_1\frac{|G|^2}{1-\frac{1}{p}}|G|^2\exp\Big(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\Big)\right)\le 2.
$$

Therefore,

$$
\sum_{F_1:\sigma}\prod_{i\in[n_1]\setminus S}\sum_{l\in(\mathbb{Z}/|G|\mathbb{Z})^\times}\mathbb{P}[lF_2(B_i)=F_1(u_i)]\le 2(1-\tfrac{1}{p})^{n_1-|S|}\left(\frac{|T_1|}{|G|}\right)^{|S|}\left(\frac{A}{|T_2|}\right)^{n_1-|S|}\left(\frac{D_1\,|T_2|}{A}\right)^{|\sigma|}.
$$

By summing over $\sigma \subseteq [n_1]$ with $|\sigma| = \delta \log_p(D_1) n_1$, we see that

$$\sum_{F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)} \prod_{i \in [n_1] \setminus S} \sum_{l \in (\mathbb{Z}/|G|\mathbb{Z})^\times} \mathbb{P}[lF_2(B_i) = F_1(u_i)]$$
$$\leq \binom{n_1}{\delta \log_p(D_1) n_1} 2(1 - \tfrac{1}{p})^{n_1 - |S|} \left(\frac{|T_1|}{|G|}\right)^{|S|} \left(\frac{A}{|T_2|}\right)^{n_1 - |S|} \left(\frac{D_1 |T_2|}{A}\right)^{\delta \log_p(D_1) n_1}.$$

This implies that

$$\sum_{F_1 \in \mathcal{S}^1_{n_1,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{n_2,\delta}(H_2,T_2)} \mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \Gamma(M_n^{(\alpha)}) = S]$$
$$\leq (\tfrac{1}{p})^{|S|} (\tfrac{1}{|G|})^{n_1 - |S|} \frac{e_1^{n_2} e_2^{|S|}}{|T_1|^{n_2} |T_2|^{|S|}} \left(1 + 4 |G|^2 n_1 \exp\Big(-\frac{\epsilon \delta \alpha n_1}{|G|^4}\Big)\right)$$
$$\times \binom{n_2}{\delta n_2 \log_p(D_2)} \frac{|T_2|^{n_2}}{|G|^{n_2}} D_2^{\delta n_2 \log_p(D_2)}$$
$$\times \binom{n_1}{\delta \log_p(D_1) n_1} 2(1 - \tfrac{1}{p})^{n_1 - |S|} \left(\frac{|T_1|}{|G|}\right)^{|S|} \left(\frac{A}{|T_2|}\right)^{n_1 - |S|} \left(\frac{D_1 |T_2|}{A}\right)^{\delta \log_p(D_1) n_1}.$$

Rearranging the terms and using the fact that $\binom{a}{b} \leq 2^{2\sqrt{ab}}$, we see that the above expression is at most

$$2(\tfrac{1}{|G|})^{n_1 + n_2} (\tfrac{1}{p})^{|S|} (1 - \tfrac{1}{p})^{n_1 - |S|} e_1^{n_2} e_2^{|S|} \left(\frac{A}{|T_1|}\right)^{n_2 - |S|} \left(\frac{A}{|T_2|}\right)^{n_1 - n_2}$$
$$\times 2^{2n_2 \sqrt{\delta \log_p(D_2)}} 2^{2n_1 \sqrt{\delta \log_p(D_1)}} D_2^{\delta n_2 \log_p(D_2)} \left(\frac{D_1 |T_2|}{A}\right)^{\delta \log_p(D_1) n_1} \left(1 + 4 |G|^2 n_1 \exp\Big(-\frac{\epsilon \delta \alpha n_1}{|G|^4}\Big)\right).$$

Since $e_1, e_2, \frac{A}{|T_1|} \frac{A}{|T_2|} \leq 1$, $n_2 = \lceil \alpha n \rceil$ and $(\frac{1}{p} - \rho) n \leq |S| \leq (\frac{1}{p} + \rho) n$, we see that

$$e_1^{n_2} e_2^{|S|} \left(\frac{A}{|T_1|}\right)^{n_2 - |S|} \left(\frac{A}{|T_2|}\right)^{n_1 - n_2} \leq \left(e_1^{\alpha} e_2^{\frac{1}{p} - \rho} \left(\frac{A}{|T_1|}\right)^{\alpha - \frac{1}{p} - \rho} \left(\frac{A}{|T_2|}\right)^{1 - \alpha}\right)^n \frac{|T_2|}{A}.$$

Next, note that

$$2^{2n_2\sqrt{\delta \log_p(D_2)}} 2^{2n_1\sqrt{\delta \log_p(D_1)}} D_2^{\delta n_2 \log_p(D_2)} \left(\frac{D_1 |T_2|}{A}\right)^{\delta \log_p(D_1) n_1}$$
$$\leq \left(2^{2\sqrt{2\log_p(|G|)}} 2^{2\sqrt{2\log_p(|G|)}} |G|^{4\log_p(|G|)} |G|^{8\log_p(|G|)}\right)^{n\sqrt{\delta}}.$$

Further note that for sufficiently large n, we have

$$\left(1 + 4n_1 |G|^2 \exp\left(-\frac{\epsilon\delta\alpha n_1}{|G|^4}\right)\right) < 2.$$

We write

$$B = 2^{4(2\log_p(|G|))^{1/2}} |G|^{12\log_p(|G|)}.$$

Then we see that

$$\sum_{F_1 \in \mathcal{S}^1_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{\lceil \alpha n\rceil,\delta}(H_2,T_2)} \mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \Gamma(M_n^{(\alpha)}) = S]$$
$$\leq 4|G|^2 \frac{1}{|G|^{n+\lceil \alpha n\rceil}} (\tfrac{1}{p})^{|S|}(1-\tfrac{1}{p})^{n-|S|} \left(e_1^\alpha e_2^{\frac{1}{p}-\rho}\left(\frac{A}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho}\left(\frac{A}{|T_2|}\right)^{1-\alpha} B^{\sqrt{\delta}}\right)^n.$$

By summing over different S, we see that

$$\sum_{F_1 \in \mathcal{S}^1_{n,\delta}(H_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{\lceil \alpha n\rceil,\delta}(H_2,T_2)} \mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n]$$
$$\leq 4|G|^2 \frac{1}{|G|^{n+\lceil \alpha n\rceil}} \left(e_1^\alpha e_2^{\frac{1}{p}-\rho}\left(\frac{A}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho}\left(\frac{A}{|T_2|}\right)^{1-\alpha} B^{\sqrt{\delta}}\right)^n.$$

Note that e_1, e_2, $\frac{A}{|T_1|}$ and $\frac{A}{|T_2|}$ are all at most one. Moreover, at least one of the following holds

- $T_1 \subsetneq H_1$. In this case $e_1 < 1$ and $\alpha > 0$, so $e_1^\alpha < 1$.

- $T_2 \subsetneq H_2$. In this case $e_2 < 1$ and $\frac{1}{p} - \rho > 0$, so $e_2^{\frac{1}{p}-\rho} < 1$.

- $T_1 \not\subseteq T_2$ and $T_2 = H_2$. In this case $A = |T_1 \cap T_2|$, $\frac{|T_1 \cap T_2|}{|T_1|} < 1$ and $\alpha - \frac{1}{p} - \rho > 0$, so $\left(\frac{A}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho} < 1$.

- $T_2 \not\subseteq T_1$, $T_2 = H_2$ and $\alpha \neq 1$. In this case $A = |T_1 \cap T_2|$, $\frac{|T_1 \cap T_2|}{|T_2|} < 1$ and $1 - \alpha > 0$, so $\left(\frac{A}{|T_2|}\right)^{1-\alpha} < 1$.

Therefore,

$$e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{A}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{A}{|T_2|}\right)^{1-\alpha} < 1.$$

We can therefore choose a sufficiently small δ to ensure that

$$e_1^{\alpha} e_2^{\frac{1}{p}-\rho} \left(\frac{A}{|T_1|}\right)^{\alpha-\frac{1}{p}-\rho} \left(\frac{A}{|T_2|}\right)^{1-\alpha} B^{\sqrt{\delta}} < 1.$$

The result follows. $\square$

Now we are only left with the case $T_1 = H_1$, $T_2 = H_2$, $T_1 \subsetneq T_2$ and $\alpha = 1$.

Proposition 2.6.5. *Suppose $\alpha = 1$ and $0 < \rho < \min(\alpha - \frac{1}{p}, \frac{1}{p})$. Consider π_2-full subgroups $T_1 \subsetneq T_2 \subseteq G \oplus \mathbb{Z}/|G|\mathbb{Z}$. For $\delta > 0$, we have*

$$\lim_{n\to\infty} |G|^{2n-1} \sum_{F_1 \in \mathcal{S}^1_{n,\delta}(T_1,T_1)} \sum_{F_2 \in \mathcal{S}^1_{n,\delta}(T_2,T_2)} \mathbb{P}\left[(F_1, F_2) \circ M_n^{(\alpha)} = 0 \text{ and } \left|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\right| \leq \rho n\right] = 0.$$

Proof. Since $\alpha = 1$, $n_1 = n_2 = n$. We have $e_1 = e_2 = 1$, $F_1 \in \mathcal{S}^1_{n,\delta}(T_1, T_1)$ are codes of distance δn with image T_1 and $F_2 \in \mathcal{S}^1_{n,\delta}(T_2, T_2)$ are codes of distance δn with image T_2.

By the independence of columns of M_{n_1,n_2}, we have

$$\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0] = \prod_{i \in [n_1]} \mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \prod_{j \in [n_2]} \mathbb{P}[F_1(A_j) = -d_j F_2(v_j)].$$

For each $i \in [n]$, we know by Corollary 2.3.6 that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \leq \frac{1}{|T_2|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big).$$

For each $j \in [n]$, we know from Corollary 2.3.6 that

$$\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] \leq \frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big).$$

However, if $F_2(v_j) \in T_2 \setminus T_1$, then we can get a tighter upper bound. Since $F_1(A_j)$ can only take values in T_1, if $F_1(A_j) = -d_j F_2(v_j)$ then $d_j F_2(v_j) \in T_1$. If $F_2(v_j) \notin T_1$, this forces $d_j \equiv 0 \pmod p$. We conclude that if $F_2(v_j) \in T_2 \setminus T_1$, then

$$\begin{aligned}
\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] &= \mathbb{P}[F_1(A_j) = -d_j F_2(v_j) \mid d_j F_2(v_j) \in T_1]\mathbb{P}[d_j F_2(v_j) \in T_1] \\
&\leq \left(\frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big)\right) \mathbb{P}[d_j \equiv 0 \pmod p] \\
&= \frac{1}{p}\left(\frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big)\right).
\end{aligned}$$

Since F_2 is a code of distance δn with image T_2, we know that

$$|\{j \in [n] : F_2(v_j) \notin T_1\}| \geq \delta n.$$

It follows that

$$\mathbb{P}[(F_1, F_2) \circ M_{n_1,n_2} = 0] \leq \left(\frac{1}{|T_2|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big)\right)^n \Big(\frac{1}{p}\Big)^{\delta n} \left(\frac{1}{|T_1|} + \exp\Big(-\frac{\epsilon \delta n}{|G|^4}\Big)\right)^n.$$

Once n is large enough to ensure,

$$\frac{\exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big)}{2^{\frac{1}{2n}}-1} < \frac{1}{|G|^2},$$

then by Corollary 2.8.5 we know that

$$\mathbb{P}[(F_1,F_2)\circ M_n^{(\alpha)}=0] \le \Big(\frac{1}{p}\Big)^{\delta n}\frac{1}{|T_2|^n\,|T_1|^n}\left(1+4n\,|G|^2\exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big)\right).$$

Since $\left|\mathcal{S}^1_{n,\delta}(T_1,T_1)\right| \le \frac{|T_1|^n}{|G|^n}$ and $\left|\mathcal{S}^1_{n,\delta}(T_2,T_2)\right| \le \frac{|T_2|^n}{|G|^n}$, we conclude that

$$\begin{aligned}
&\sum_{F_1\in\mathcal{S}^1_{n,\delta}(T_1,T_1)}\ \sum_{F_2\in\mathcal{S}^1_{n,\delta}(T_2,T_2)} \mathbb{P}\left[(F_1,F_2)\circ M_n^{(\alpha)}=0 \text{ and } \left|\gamma(M_n^{(\alpha)})-\tfrac{1}{p}n\right|\le\rho n\right]\\
&\le \sum_{F_1\in\mathcal{S}^1_{n,\delta}(T_1,T_1)}\ \sum_{F_2\in\mathcal{S}^1_{n,\delta}(T_2,T_2)} \mathbb{P}[(F_1,F_2)\circ M_n^{(\alpha)}=0]\\
&\le \frac{1}{|G|^{2n}}\Big(\frac{1}{p}\Big)^{\delta n}\left(1+4n\,|G|^2\exp\Big(-\frac{\epsilon\delta n}{|G|^4}\Big)\right).
\end{aligned}$$

The result follows. $\square$

Notice that Proposition 2.6.3, Proposition 2.6.4 and Proposition 2.6.5 together prove Proposition 2.6.1. We have previously seen that Proposition 2.6.1 implies Proposition 2.2.5, which implies Theorem 2.1.8, which in turn implies Theorem 2.1.5.

2.7 Raw moments sometimes diverge to infinity

We consider the special case of $M_n^{(\alpha)}$ when all a_{ij} and b_{ij} are Haar-uniform and show that certain moments blow up to infinity.

Proposition 2.7.1. *Consider $0<\alpha<1$ and $m>\frac{2-\alpha}{1-\alpha}$. If all a_{ij} and b_{ij} in $M_n^{(\alpha)}$ are*

Haar-uniform, then we have

$$\lim_{n\to\infty} \mathbb{E}[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), (\mathbb{Z}/p\mathbb{Z})^m)\right|] = \infty.$$

Proof. Denote $G = (\mathbb{Z}/p\mathbb{Z})^m$, $n_1 = n$ and $n_2 = \lceil \alpha n \rceil$. We know that

$$\mathbb{E}[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), (\mathbb{Z}/p\mathbb{Z})^m)\right|] = \sum_{F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)} \sum_{F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G)} \mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0].$$

Since the columns of $M_n^{(\alpha)}$ are independent, we see that

$$\mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0] = \prod_{i=1}^{n_1} \mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \prod_{j=1}^{n_2} \mathbb{P}[F_1(A_j) = -d_j F_2(v_j)].$$

Let H be a subgroup of G isomorphic to $\mathbb{Z}/p\mathbb{Z}$. As a lower bound, we restrict ourselves to $F_1 \in \mathrm{Sur}(\mathbb{Z}_p^{n_1}, G)$ and $F_2 \in \mathrm{Sur}(\mathbb{Z}_p^{n_2}, H)$.

By Lemma 2.3.1, we know that

$$\mathbb{P}[F_1(A_j) = -d_j F_2(v_j)] = \frac{1}{|G|} = \frac{1}{p^m}.$$

- If $F_1(u_i) \in H$, then by Lemma 2.3.1, we know that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] = \frac{1}{p}.$$

- If $F_1(u_i) \notin H$, then

$$\mathbb{P}[c_i F_1(u_i) \in H] = \mathbb{P}[c_i \equiv 0 \pmod{p}] = \frac{1}{p}.$$

Therefore, by Lemma 2.3.1, we know that

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] = \mathbb{P}[F_2(B_i) = -c_i F_1(u_i) \mid c_i F_1(u_i) \in H]\mathbb{P}[c_i F_1(u_i) \in H] = \frac{1}{p^2}.$$

We see that regardless of whether $F_1(u_i)$ is in H or not we have

$$\mathbb{P}[F_2(B_i) = -c_i F_1(u_i)] \geq \frac{1}{p^2}.$$

We conclude that

$$\mathbb{P}[(F_1, F_2) \circ M_n^{(\alpha)} = 0] \geq p^{-m\lceil \alpha n \rceil - 2n} \geq p^{-(m\alpha+2)n-m}.$$

Since $\left|\mathrm{Sur}(\mathbb{Z}_p^{n_1}, G)\right| = p^{mn}(1 + o(1))$ and $\left|\mathrm{Sur}(\mathbb{Z}_p^{n_2}, H)\right| = p^{\alpha n}(1 + o(1))$, we conclude that

$$\begin{aligned}\mathbb{E}[\left|\mathrm{Hom}(\mathrm{Coker}(M_n^{(\alpha)}), (\mathbb{Z}/p\mathbb{Z})^m)\right|] &\geq p^{-(m\alpha+2)n-m} p^{(m+\alpha)n}(1 + o(1)) \\ &= p^{-m}(1 + o(1))\big(p^{m(1-\alpha)+\alpha-2}\big)^n.\end{aligned}$$

Since $m > \frac{2-\alpha}{1-\alpha}$, this goes to infinity as $n \to \infty$. $\square$

2.8 Technical Lemmas

Lemma 2.8.1. *Given $\rho > 0$, we have*

$$\left|1 - \sum_{k:\left|k - \frac{1}{p}n\right| \leq \rho n} \binom{n}{k} \frac{1}{p^k}\Big(1 - \frac{1}{p}\Big)^{n-k}\right| \leq 2\exp\big(-2\rho^2 n\big).$$

Proof. The result follows from Hoeffding's inequality. $\square$

Corollary 2.8.2. *Given $\rho > 0$, we have*

$$\lim_{n\to\infty} \mathbb{P}\Big[\Big|\gamma(M_n^{(\alpha)}) - \tfrac{1}{p}n\Big| \leq \rho n\Big] = 1.$$

Lemma 2.8.3. *Given $\rho > 0$, we have*

$$\lim_{n\to\infty} \mathbb{P}[|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n| \leq \rho n] = 1.$$

Proof. Denote $n_2 = \lceil \alpha n \rceil$. For each $1 \leq i \leq n$, we denote

$$\beta_i = \begin{cases} 1 & \text{if } \sum_{j=1}^{n_2} b_{ij} \equiv 0 \pmod p \\ 0 & \text{if } \sum_{j=1}^{n_2} b_{ij} \not\equiv 0 \pmod p. \end{cases}$$

Therefore $\gamma(L_n^{(\alpha)}) = \sum_{i=1}^n \beta_i$.

Consider the map F_0 from $\mathbb{Z}_p^{n_2}$ to $\mathbb{Z}/p\mathbb{Z}$ that sends each basis vector to 1. So $\sum_j b_{ij} \equiv 0 \pmod p$ if and only if $F_0(B_i) = 0$. Note that F_0 is a code of distance n_2 with image $\mathbb{Z}/p\mathbb{Z}$. Lemma 2.3.4 tells us that for each i,

$$\left|\mathbb{P}[F_0(B_i) = 0] - \frac{1}{p}\right| \leq \exp\Big(-\frac{\epsilon n_2}{p^2}\Big) \leq \exp\Big(-\frac{\epsilon \alpha n}{p^2}\Big).$$

Now,

$$\mathbb{E}[\gamma(L_n^{(\alpha)})] = \sum_{i=1}^n \mathbb{E}[\beta_i] = \sum_{i=1}^n \mathbb{P}[F_0(B_i) = 0],$$

and hence

$$\left|\mathbb{E}[\gamma(L_n^{(\alpha)})] - \frac{1}{p}n\right| \leq n \exp\Big(-\frac{\epsilon \alpha n}{p^2}\Big).$$

Next,

$$\mathrm{Var}(\beta_i) = \mathbb{P}[F_0(B_i) = 0](1 - \mathbb{P}[F_0(B_i) = 0]) \leq 1.$$

Moreover, since the β_i are independent, it follows that

$$\mathrm{Var}(\gamma(L_n^{(\alpha)})) = \sum_{i=1}^{n} \mathrm{Var}(\beta_i) \leq n.$$

Notice that

$$\mathbb{E}\Big[\big(\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n\big)^2\Big] = \mathrm{Var}(\gamma(L_n^{(\alpha)})) + \big(\mathbb{E}[\gamma(L_n^{(\alpha)})] - \tfrac{1}{p}n\big)^2 \leq n + n^2 \exp\Big(-\frac{2\epsilon\alpha n}{p^2}\Big).$$

So by Chebyshev's inequality, we have

$$\mathbb{P}[|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n| \geq \rho n] \leq \frac{\mathbb{E}\big[\big(\gamma(L_n^{(\alpha)}) - \frac{1}{p}n\big)^2\big]}{(\rho n)^2} \leq \frac{n + n^2 \exp\Big(-\frac{2\epsilon\alpha n}{p^2}\Big)}{\rho^2 n^2}.$$

This implies that

$$\lim_{n\to\infty} \mathbb{P}[|\gamma(L_n^{(\alpha)}) - \tfrac{1}{p}n| \geq \rho n] = 0. \qquad \square$$

Lemma 2.8.4. *Suppose we have $n \geq 2$, $0 < k_0 \leq x_1, x_2, \ldots, x_n$ and $0 < y < k_0(2^{1/n} - 1)$, then we have*

$$\Big(1 - \frac{2ny}{k_0}\Big)\prod_{i=1}^{n} x_i \leq \prod_{i=1}^{n}(x_i - y) \leq \prod_{i=1}^{n}(x_i + y) \leq \Big(1 + \frac{2ny}{k_0}\Big)\prod_{i=1}^{n} x_i.$$

Proof. Consider $f_1(t) = \prod_{i=1}^{n}(x_i + t)$, $g_1(t) = (1 + \frac{2nt}{k_0})\prod_{i=1}^{n} x_i$, $f_2(t) = \prod_{i=1}^{n}(x_i - t)$ and

$g_2(t) = (1 - \frac{2nt}{k_0}) \prod_{i=1}^n x_i$. Now we have $f_1(0) = g_1(0)$ and for $0 \leq t \leq k_0(2^{1/n} - 1)$, we have

$$
\begin{aligned}
f_1'(t) &= \sum_{j=1}^{n} \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (x_i + t) \leq \frac{n}{k_0} \prod_{1 \leq i \leq n} (x_i + t) = \frac{n}{k_0} \prod_{1 \leq i \leq n} x_i \prod_{1 \leq i \leq n} (1 + \frac{t}{x_i}) \\
&\leq \frac{n}{k_0} \Big(\prod_{1 \leq i \leq n} x_i \Big) \Big(1 + \frac{t}{k_0} \Big)^n \leq \frac{2n}{k_0} \Big(\prod_{1 \leq i \leq n} x_i \Big) = g_1'(t).
\end{aligned}
$$

We can therefore conclude that $f_1(y) \leq g_1(y)$. Next, we have $f_2(0) = g_2(0)$ and for $0 \leq t \leq k_0(2^{1/n} - 1)$, we have

$$
-f_2'(t) = \sum_{j=1}^{n} \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (x_i - t) \leq \frac{n}{k_0 - t} \prod_{1 \leq i \leq n} (x_i - t) \leq \frac{2n}{k_0} \prod_{1 \leq i \leq n} x_i = -g_2'(t).
$$

We conclude that $g_2(y) \leq f_2(y)$. $\square$

Corollary 2.8.5. *Suppose we have $n \geq 2$ and real numbers $k_0, x_1, \ldots, x_n, x_1', \ldots, x_n', y$ for which $0 < k_0 \leq x_1, x_2, \ldots, x_n$, $0 < y < k_0(2^{1/n} - 1)$ and $|x_i' - x_i| \leq y$, then we have*

$$
\left| \prod_{i=1}^n x_i' - \prod_{i=1}^n x_i \right| \leq \frac{2ny}{k_0} \prod_{i=1}^n x_i.
$$

Acknowledgments

We thank Nathan Kaplan for introducing me to this problem and for many helpful discussions about the problem. We acknowledge support from NSF Grant DMS 2154223.

Chapter 3

Distribution of Sandpile Groups of Random Bipartite Graphs

Abstract

Fix a prime p and a constant $\frac{1}{p} < \alpha \leq 1$. Consider the random Erdős–Rényi bipartite graph $G_\alpha(n, u)$ with bipartition (V_1, V_2) of sizes $|V_1| = n$ and $|V_2| = \lceil \alpha n \rceil$, and edge probability $0 < u < 1$. The authors of [1] and [10] conjectured a limiting distribution for the p-Sylow subgroup of the sandpile group of $G_\alpha(n, u)$ as $n \to \infty$. We prove this conjecture for odd primes p.

Similar results have previously been proved by computing the expected number of surjections from the random abelian p-group to H, for each finite abelian p-group H. However, in our setting, these surjective moments often diverge to infinity, despite the conjectured limiting distribution having finite moments. We resolve this issue by discarding the graphs for which too many vertices have degrees divisible by p. Once we remove the contribution of this rare set of graphs, then the surjective moments converge to the expected values. When p is odd,

applying Wood's universality theorem yields the desired convergence in distribution.

For $p = 2$, our computed moments (after excluding the rare set of graphs) match those of the conjectured distribution. However, these moments do not uniquely determine a distribution.

3.1 Introduction

Let Γ be a graph on vertices $1, \dots, n$ without loops. Write $\deg(i, j)$ for the number of edges between i and j, and $\deg(j) = \sum_{i:i\neq j} \deg(i, j)$. Define the Laplacian $L(\Gamma)$ by

$$L_{ij} = \begin{cases} \deg(i,j), & i \neq j, \\ -\deg(j), & i = j, \end{cases} \qquad \text{so that} \qquad \sum_{i=1}^{n} L_{ij} = 0 \ \text{ for all } j.$$

Let $\mathbb{Z}_0^n$ be the subset of $\mathbb{Z}^n$ consisting of vectors that sum up to 0. Hence $L : \mathbb{Z}^n \to \mathbb{Z}^n$ satisfies $\operatorname{Im}(L) \subseteq \mathbb{Z}_0^n$. The *sandpile group* of Γ is $S_\Gamma := \mathbb{Z}_0^n / \operatorname{Im}(L)$. If Γ is connected, then $\operatorname{corank}(L) = 1$ and S_Γ is a finite abelian group.

Let $G(n, v)$ denote the Erdős-Rényi random graph on n vertices in which each pair (i, j) with $i \neq j$ is included independently with probability $v \in (0, 1)$. For fixed v, $G(n, v)$ is connected with probability tending to 1 as $n \to \infty$. Consequently, the sandpile group $S_{G(n,v)}$ is a finite abelian group with probability tending to 1.

Wood in [23, Theorem 1.1] shows that as $n \to \infty$, the distribution of Sylow p-subgroups of the sandpile group of an Erdős-Rényi random graph with n vertices converges to $P^{\mathrm{Sym}}_{\infty,p}$. The probability distribution $P^{\mathrm{Sym}}_{\infty,p}$ on finite abelian p-groups is defined as follows

$$P^{\mathrm{Sym}}_{\infty,p}(G) := \frac{|\{\text{symmetric, bilinear, perfect pairings } G \times G \to \mathbb{C}^\times\}|}{|G|\,|\operatorname{Aut}(G)|} \prod_{k \geq 0} (1 - p^{-1-2k}).$$

Theorem 3.1.1. *[23, Theorem 1.1] Consider a finite abelian p-group G. Then for a random* *graph* $G(n,v)$,

$$\lim_{n\to\infty} \mathbb{P}[(S_{G(n,v)})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

Mészáros in [15] determined the distribution of Sylow p-subgroups of sandpile groups of random d-regular graphs on n vertices, as $n \to \infty$. Suppose $d \geq 3$ and n is even. The random d-regular graph H_n is obtained by taking the union of d independent uniform random perfect matchings on the set of n vertices. Given a finite abelian p-group G, its *rank* is $\log_p(|G/pG|)$.

Theorem 3.1.2. *[15, Theorem 1.2] Consider a prime p and a finite abelian p-group G.*

1. *If d is odd, or d is even and p is odd, we have*

$$\lim_{n\to\infty} \mathbb{P}[(S_{H_n})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

2. *Suppose d is even and $p = 2$. Then $(S_{H_n})_2$ always has odd rank. Moreover, if G is a finite abelian 2-group of odd rank, then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{H_n})_2 \cong G] = |G/2G|\, P^{\mathrm{Sym}}_{\infty,2}(G).$$

We focus on the study of Sylow p-subgroups of random bipartite graphs. Let $n_1 \geq n_2$ be positive integers and u be a fixed real number $0 < u < 1$. The Erdős-Rényi random bipartite graph $G(n_1, n_2, u)$ is a bipartite graph with vertex sets V_1 of size n_1 and V_2 of size n_2, where each of the $n_1 n_2$ potential edges between a vertex in V_1 and a vertex in V_2 is included independently with probability u. We are most interested in the case where n_1 and n_2 go to infinity together and $n_2 = \lceil \alpha n_1 \rceil$ for a fixed constant $0 < \alpha \leq 1$. We denote $G_\alpha(n_1, u) = G(n_1, \lceil \alpha n_1 \rceil, u)$. Let $S_{G_\alpha(n,u)}$ denote the sandpile group of the graph $G_\alpha(n,u)$. In [1], Bhargava, de Pascale, and Koenig give a conjecture for the distribution of p-Sylow subgroups of $S_{G_\alpha(n,u)}$ for odd p. In [10], the authors gave the corresponding conjecture for $p = 2$.

Conjecture 3.1.3. *Let p be a prime, $0 < u < 1$ and $\frac{1}{p} < \alpha \leq 1$ and G be a finite abelian p-group.*

1. *If p is odd, then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G_\alpha(n,u)})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

2. *If $p = 2$, then*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G_\alpha(n,u)})_2 \cong G] = \frac{|G/2G|}{2} P^{\mathrm{Sym}}_{\infty,2}(G).$$

Our main result is to prove Conjecture 3.1.3 for odd primes p.

Theorem 3.1.4. *Let p be an odd prime, $0 < u < 1$ and $\frac{1}{p} < \alpha \leq 1$ and G be a finite abelian p-group. Then we have*

$$\lim_{n\to\infty} \mathbb{P}[(S_{G_\alpha(n,u)})_p \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

The authors of [10] also conjectured the limiting distribution of ranks of $(S_{G_\alpha(n,u)})_p$. For this we denote the q-shifted factorials

$$(x;q)_i := (1-x)(1-xq)\cdots(1-xq^{i-1}), \quad (x;q)_\infty := \prod_{j=0}^{\infty}(1-xq^j).$$

Conjecture 3.1.5. *[10] Let p be prime, $\frac{1}{p} < \alpha \leq 1$, and r be a nonnegative integer.*

1. *If p is odd, then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G(n,\alpha,u)})_p) = r] = \frac{1}{(-p^{-1};p^{-1})_\infty} p^{-\binom{r+1}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

2. *If $p = 2$, we have*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G(n,\alpha,u)})_2) = r] = \frac{1}{(-1;p^{-1})_\infty} p^{-\binom{r}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

Our other main result is to prove Conjecture 3.1.5 for all primes, including $p = 2$.

Theorem 3.1.6. *Let p be prime, $\frac{1}{p} < \alpha \leq 1$, and r be a nonnegative integer.*

1. *If p is odd, then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G(n,\alpha,u)})_p) = r] = \frac{1}{(-p^{-1};p^{-1})_\infty} p^{-\binom{r+1}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

2. *If $p = 2$, we have*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}((S_{G(n,\alpha,u)})_2) = r] = \frac{1}{(-1;p^{-1})_\infty} p^{-\binom{r}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

3.1.1 Random matrix model

Let $\mathbb{Z}_p$ be the ring of p-adic integers. Fix $0 < \epsilon < 1$ for the rest of the paper. A probability measure μ on $\mathbb{Z}_p$ is called *ϵ-balanced* if for each $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\mu[\{x \in \mathbb{Z}_p : x \equiv a \pmod{p}\}] < 1 - \epsilon.$$

For the rest of this paper, fix a ϵ-balanced probability measure μ.

We consider a random matrix model for the Laplacian of $G_\alpha(n,u)$ as a random matrix $L_{n_1,n_2} \in \mathbb{M}_{n_1+n_2}(\mathbb{Z}_p)$ as follows:

$$L_{n_1,n_2} = \begin{bmatrix} -\sum a_{1j} & 0 & \dots & 0 & a_{11} & a_{12} & \dots & a_{1n_2} \\ 0 & -\sum a_{2j} & \dots & 0 & a_{21} & a_{22} & \dots & a_{2n_2} \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \dots & -\sum a_{n_1j} & a_{n_11} & a_{n_12} & \dots & a_{n_1n_2} \\ a_{11} & a_{21} & \dots & a_{n_11} & -\sum a_{i1} & 0 & \dots & 0 \\ a_{12} & a_{22} & \dots & a_{n_12} & 0 & -\sum a_{i2} & \dots & 0 \\ \vdots & & & \vdots & \vdots & & \ddots & \vdots \\ a_{1n_2} & a_{2n_2} & \dots & a_{n_1n_2} & 0 & 0 & \dots & -\sum a_{in_2} \end{bmatrix},$$

where all a_{ij} are independent random variables, distributed according to μ. Let Z_n consist of the vectors in $\mathbb{Z}_p^n$ whose entries sum to 0. We have $L_{n_1,n_2} \in \operatorname{Hom}(\mathbb{Z}_p^{n_1+n_2}, \mathbb{Z}_p^{n_1+n_2})$ and $\operatorname{Im}(L_{n_1,n_2}) \subseteq Z_{n_1+n_2}$. We denote $G(L_{n_1,n_2}) = Z_{n_1+n_2}/\operatorname{Im}(L_{n_1,n_2})$. For $0 < \alpha \leq 1$, we denote $L_{n,\lceil \alpha n \rceil}$ as $L_n^{(\alpha)}$.

In particular, if μ was the measure such that $\mu(\{1\}) = v$ and $\mu(\{0\}) = 1-v$, then $L_n^{(\alpha)}$ would be the random matrix arising from the Laplacian of the random graph $\vec{G}_\alpha(n,v)$. Moreover, in the (high probability) event that $\vec{G}_\alpha(n,v)$ is connected, the random finite abelian p-group $G(L_n^{(\alpha)})$ would become isomorphic to the p-Sylow subgroup of $S_{\vec{G}_\alpha(n,v)}$.

We will prove the following.

Theorem 3.1.7. *Let p be an odd prime, $\frac{1}{p} < \alpha \leq 1$ and G be a finite abelian p-group. Then we have*

$$\lim_{n\to\infty} \mathbb{P}[G(L_n^{(\alpha)}) \cong G] = P^{\mathrm{Sym}}_{\infty,p}(G).$$

Theorem 3.1.8. *Let p be prime, $\frac{1}{p} < \alpha \leq 1$, and r be a nonnegative integer.*

1. *If p is odd, then*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}(G(L_n^{(\alpha)})) = r] = \frac{1}{(-p^{-1}; p^{-1})_\infty} p^{-\binom{r+1}{2}} \frac{1}{(p^{-1}; p^{-1})_r}.$$

2. *If $p = 2$, we have*

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}(G(L_n^{(\alpha)})) = r] = \frac{1}{(-1; p^{-1})_\infty} p^{-\binom{r}{2}} \frac{1}{(p^{-1}; p^{-1})_r}.$$

It is clear that Theorem 3.1.7 implies Theorem 3.1.4 at once and Theorem 3.1.8 implies Theorem 3.1.6.

3.2 Strategy

Previous results about the distribution of sandpile groups of random graphs and cokernels of random matrices have been proven using the following strategy. Suppose G_n is a sequence of random finite abelian p-groups and ν is the conjectured limiting distribution as $n \to \infty$. The first step is to show that the surjective moments match. That is, for every finite abelian p-group H, we have

$$\lim_{n\to\infty} \mathbb{E}[|\operatorname{Sur}(G_n, H)|] = \mathbb{E}[|\operatorname{Sur}(X, H)|], \tag{3.1}$$

where X is a random finite abelian p-group chosen according to ν. The next step is to show a universality result that if (3.1) is satisfied, then it implies that for every finite abelian p-group H

$$\lim_{n\to\infty} \mathbb{P}[G_n \cong H] = \nu(H).$$

The surjective moments of $P^{\mathrm{Sym}}_{\infty,p}$ were computed by Clancy, Kaplan, Leake, Payne, and Wood in [6].

Theorem 3.2.1. *[6, Theorem 11] Suppose p is a prime and G is a finite abelian p-group. Let X be a random finite abelian p-group distributed according to $P^{\mathrm{Sym}}_{\infty,p}$. Then we have*

$$\mathbb{E}[|\mathrm{Sur}(X,G)|] = \left|\Lambda^2 G\right|.$$

The authors of [10] compute the surjective moments of several families of distributions. One of them is defined in terms of a parameter $-1 \leq a \leq 1$ as

$$P^{M,1}_{p,a}(G) := \begin{cases} \frac{1-a}{2} \times |G/pG| \times P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } \log_p(G/pG) \text{ is odd,} \\ \frac{1+a}{2} \times |G/pG| \times P^{\mathrm{Sym}}_{\infty,p}(G) & \text{if } \log_p(G/pG) \text{ is even.} \end{cases}$$

The superscript M is for 'Mészáros'. This is to highlight the fact that the measure $P^{M,1}_{p,-1}$ occurs in the special case of Theorem 3.1.2 where d is even and $p = 2$. Also note that the measure $P^{M,1}_{p,0}$ occurs in Conjecture 3.1.3 when $p = 2$.

The surjective moments of $P^{M,1}_{p,a}$ are as follows.

Theorem 3.2.2. *[10, Theorem 9] Suppose p is a prime, $-1 \leq a \leq 1$ and G is a finite abelian p-group. Let X be a random finite abelian p-group distributed according to $P^{M,1}_{p,a}$. Then we have*

$$\mathbb{E}[|\mathrm{Sur}(X,G)|] = |G/pG| \times \left|\Lambda^2 G\right|.$$

In particular, the moments do not depend on a. Moreover,

$$\mathbb{P}[\mathrm{rank}(X) \text{ is odd}] = \frac{1-a}{2}.$$

Based on this, we should expect that for each finite abelian p-group H, we have

$$\lim_{n\to\infty} \mathbb{E}\left[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), H)\right|\right] = \begin{cases} |\Lambda^2 H| & \text{if } p \text{ is odd,} \\ \\ |H/2H| \times |\Lambda^2 H| & \text{if } p = 2. \end{cases}$$

However, this is not always the case, as we will show in Section 3.8. These limits sometimes blow up to infinity. The issue here is that a small subset of matrices contribute greatly to the surjective moments while contributing minimally to the distribution. We can get around this problem by restricting ourselves to a subset of the matrices whose probability goes to 1 as $n \to \infty$, and computing the moments on this subset. An identical issue arises in [22] where the author studies the distribution of sandpile groups of random directed bipartite graphs.

3.2.1 Good subset of matrices

Given $\rho > 0$, we define

$$\mathcal{E}_{n,\rho} = \left\{ \begin{bmatrix} t_1 \\ \vdots \\ t_n \end{bmatrix} \in (\mathbb{Z}/p\mathbb{Z})^n : |\{i \in [n] : t_i = 0\}| < \left(\frac{1}{p} + \rho\right) n \right\}.$$

Define

$$\eta(L_{n_1,n_2}) = \begin{bmatrix} \sum_j a_{1j} \pmod p \\ \vdots \\ \sum_j a_{n_1 j} \pmod p \end{bmatrix} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}.$$

Even though a_{ij} are not necessarily Haar uniform, as n_2 gets bigger $\sum_{j=1}^{n_2} a_{ij}$ would get close to being uniformly distributed $\mod p$. Therefore, as n_1 and n_2 get big, we should expect

$\eta(L_{n_1,n_2}) \in \mathcal{E}_{n_1,\rho}$ with a high probability. It is shown in Lemma 3.9.8 that this is indeed the case.

Given a function f that takes L_{n_1,n_2} as input, we denote the conditional expectation as

$$\mathbb{E}_\rho[f(L_{n_1,n_2})] = \mathbb{E}[f(L_{n_1,n_2}) \mid \eta(L_{n_1,n_2}) \in \mathcal{E}_{n_1,\rho}].$$

We also denote the expectation restricted to the event $\eta(L_{n_1,n_2}) \in \mathcal{E}_{n_1,\rho}$ as

$$\mathbb{E}'_\rho[f(L_{n_1,n_2})] = \mathbb{P}[\eta(L_{n_1,n_2}) \in \mathcal{E}_{n_1,\rho}] \times \mathbb{E}_\rho[f(L_{n_1,n_2})].$$

Once we restrict ourselves to this subset, then the issue of moments blowing up to infinity gets resolved and we get the right moments.

Proposition 3.2.3. *Let p be a prime, $\frac{1}{p} < \alpha \leq 1$. Given $0 < \rho < \alpha - \frac{1}{p}$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), G)\right|\right] = \begin{cases} |\Lambda^2 G| & \textit{if } p \textit{ is odd,} \\ |G/2G| \times |\Lambda^2 G| & \textit{if } p = 2. \end{cases}$$

Note that the restriction $\rho < \alpha - \frac{1}{p}$ is to avoid the matrices for which

$$\left|\left\{i \in [n] : \sum_j a_{ij} \equiv 0 \pmod{p}\right\}\right| > n_2 = \lceil \alpha n \rceil.$$

These are the matrices responsible for the large surjective moments. If $\alpha = 1$, then no matrix can have

$$\left|\left\{i \in [n] : \sum_j a_{ij} \equiv 0 \pmod{p}\right\}\right| > n_2 = n.$$

In fact, if $\alpha = 1$, then the issue of moments blowing up does not arise and one could work directly with the raw moments $\lim_{n\to\infty} \mathbb{E}[\left| \operatorname{Sur}(G(L_n^{(1)}), G) \right|]$.

Once we have the moments, we can show that the desired distribution occurs for odd p using the following result of Wood.

Theorem 3.2.4. *[23, Theorem 8.2] If X_n is a sequence of random abelian p-groups and Y is a random abelian p-group such that for every finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}[|\operatorname{Sur}(X_n, G)|] = \mathbb{E}[|\operatorname{Sur}(Y, G)|] \leq \left|\Lambda^2 G\right|.$$

Then for every finite abelian p-group G, we have

$$\lim_{n\to\infty} \mathbb{P}[X_n \cong G] = \mathbb{P}[Y \cong G].$$

We now show that Proposition 3.2.3 implies Theorem 3.1.7.

Proof of Theorem 3.1.7 assuming Proposition 3.2.3. For each n, let G_n be a random finite abelian p-group distributed as

$$\mathbb{P}[G_n \cong G] = \mathbb{P}\Big[G(L_n^{(\alpha)}) \cong G \mid \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}\Big].$$

Therefore, Proposition 3.2.3 says that

$$\lim_{n\to\infty} \mathbb{E}[|\operatorname{Sur}(G_n, G)|] = \left|\Lambda^2 G\right|.$$

Therefore, from Theorem 3.2.1 and Theorem 3.2.4, we see that for each finite abelian p-group

G, we have

$$\lim_{n\to\infty} \mathbb{P}[G(L_n^{(\alpha)}) \cong G \mid \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = \lim_{n\to\infty} \mathbb{P}[G_n \cong G] = P_{\infty,p}^{\mathrm{Sym}}(G).$$

Note that

$$\begin{aligned}\mathbb{P}[G(L_n^{(\alpha)}) \cong G] &= \mathbb{P}[G(L_n^{(\alpha)}) \cong G \mid \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \\ &\quad + \mathbb{P}[G(L_n^{(\alpha)}) \cong G \mid \eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}].\end{aligned}$$

The result follows since Lemma 3.9.8 says that $\lim_{n\to\infty} \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 1$. □

This shows that for odd p, Conjecture 3.1.3 will follow once we prove Proposition 3.2.3. The following result of Wood computes the distribution of ranks of a random finite abelian p-group distributed according to $P_{\infty,p}^{\mathrm{Sym}}$.

Proposition 3.2.5. *[23, Corollary 9.4] If X is a random finite abelian p-group chosen according to $P_{\infty,p}^{\mathrm{Sym}}$, then*

$$\mathbb{P}[\mathrm{rank}(X) = r] = \frac{1}{(-p^{-1};p^{-1})_\infty} p^{-\binom{r+1}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

We see from this that for odd p, Conjecture 3.1.3 implies Conjecture 3.1.5.

For $p = 2$, we will compute the surjective moments while proving Proposition 3.2.3. However, Theorem 3.2.2 shows that there is a one parameter family of measures with the same surjective moments, and possibly there could be more. The measures within this family can be distinguished based on $\mathbb{P}[\mathrm{rank}(X) \text{ is odd}]$. We will prove the following which provides further evidence for Conjecture 3.1.3 being true at $p = 2$ as well.

Proposition 3.2.6. *Suppose $p = 2$. For any $0 < \alpha \leq 1$,*

$$\lim_{n\to\infty} \mathbb{P}\left[\operatorname{rank}(G(L_n^{(\alpha)})) \text{ is odd}\right] = \frac{1}{2}.$$

Wood shows in [25] that if the surjective moments are $|G/pG| \times |\Lambda^2 G|$, then the probability of odd rank determines the distribution of the ranks.

Theorem 3.2.7. *[25, Corollary 2.12] If X_n is a sequence of random abelian p-groups such that for each $k \in \mathbb{Z}_{\geq 0}$, we have*

$$\lim_{n\to\infty} \mathbb{E}[\left|\operatorname{Sur}(X_n, (\mathbb{Z}/p\mathbb{Z})^k)\right|] = \left|(\mathbb{Z}/p\mathbb{Z})^k\right| \times \left|\Lambda^2(\mathbb{Z}/p\mathbb{Z})^k\right|,$$

and there is $v \in [-1, 1]$ such that

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}(X_n) \text{ is odd}] = v.$$

Then for every $r \in \mathbb{Z}_{\geq 0}$, we have

$$\lim_{n\to\infty} \mathbb{P}[\operatorname{rank}(X_n) = r] = \begin{cases} 2v\frac{1}{(-1;p^{-1})_\infty}p^{-\binom{r}{2}}\frac{1}{(p^{-1};p^{-1})_r} & \text{if } r \text{ is odd,} \\ 2(1-v)\frac{1}{(-1;p^{-1})_\infty}p^{-\binom{r}{2}}\frac{1}{(p^{-1};p^{-1})_r} & \text{if } r \text{ is even.} \end{cases}$$

Proof of Theorem 3.1.6 assuming Proposition 3.2.3 and Proposition 3.2.6. We consider the cases of odd primes and $p = 2$ separately.

1. First consider the case of odd prime p. We have shown that Proposition 3.2.3 implies Theorem 3.1.4. By Proposition 3.2.5 this implies the limiting distribution of ranks, proving Theorem 3.1.6 for odd p.

2. Next, consider the case $p = 2$. For each n, let G_n be a random finite abelian p-group

distributed as

$$\mathbb{P}[G_n \cong G] = \mathbb{P}\Big[G(L_n^{(\alpha)}) \cong G \mid \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}\Big].$$

Therefore, Proposition 3.2.3 says that

$$\lim_{n\to\infty} \mathbb{E}[|\mathrm{Sur}(G_n, G)|] = |G/2G| \times \left|\Lambda^2 G\right|.$$

Proposition 3.2.6 says that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}\right] = \frac{1}{2}.$$

The law of total probability tells us that

$$\begin{aligned}\mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}\right] &= \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}|\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}\right] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \\ &\quad + \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}|\eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}\right] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}].\end{aligned}$$

Lemma 3.9.8 says that $\lim_{n\to\infty} \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 1$, so we see that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{rank}(X_n) \text{ is odd}\right] = \frac{1}{2}.$$

Now, Theorem 3.2.7 tells us that

$$\lim_{n\to\infty} \mathbb{P}[\mathrm{rank}(X_n) = r] = \frac{1}{(-1;p^{-1})_\infty} p^{-\binom{r}{2}} \frac{1}{(p^{-1};p^{-1})_r}.$$

Again, by the law of total probability, we see that

$$\begin{aligned}\mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) = r\right] &= \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) = r|\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}\right] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \\ &\quad + \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) = r|\eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}\right] \times \mathbb{P}[\eta(L_n^{(\alpha)}) \notin \mathcal{E}_{n,\rho}].\end{aligned}$$

Since $\lim_{n\to\infty} \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 1$, the result follows. $\square$

We suspect that for $p = 2$, Proposition 3.2.3 and Proposition 3.2.6 should uniquely determine the distribution of finite abelian 2-groups, not just the distribution of ranks. This would imply Conjecture 3.1.3 for $p = 2$. However, we have not been able to prove this.

3.2.2 Hom-moments

The notation $H \trianglelefteq G$ means H is a subgroup of G. We say that T is a translated subgroup of G, if T is a coset of some subgroup of G. The notation $T \trianglelefteq_{\mathrm{tr}} G$ will mean that T is a translated subgroup of G. If T is a coset of a subgroup H, then we will denote $\mathcal{G}(T) = H$. We will sometimes consider chains of translated subgroups. By $T \trianglelefteq_{\mathrm{tr}} S \trianglelefteq_{\mathrm{tr}} G$, we mean that T and S are translated subgroups of G and T is a subset of S.

If G is a finite abelian p-group, then $\Lambda^2 G$ is the quotient of $G \otimes G$ by the subgroup generated by elements of the form $f \otimes f$. We define $\Delta^2 G$ to be the quotient of $G \otimes G$ by the subgroup generated by elements of the form $f \otimes g + g \otimes f$. It is clear that

$$\left|\Delta^2 G\right| = \begin{cases} |\Lambda^2 G| & \text{if } p \text{ is odd,} \\ \\ |\Lambda^2 G| \times |G/2G| & \text{if } p = 2. \end{cases}$$

The following result implies Proposition 3.2.3. Note that we are replacing $G(L_n^{(\alpha)})$ with $\mathrm{Coker}(L_n^{(\alpha)})$ and surjective moments with Hom-moments.

Proposition 3.2.8. *Let p be a prime, $\frac{1}{p} < \alpha \leq 1$. Given $0 < \rho < \alpha - \frac{1}{p}$ and a finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G)\right|\right] = \sum_{T \trianglelefteq_{tr} G} \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)|\,.$$

Proof of Proposition 3.2.3 assuming Proposition 3.2.8. Notice that $\mathbb{Z}_p^{n_1+n_2} = Z_{n_1+n_2} \oplus \mathbb{Z}_p$, so

$\mathrm{Coker}(L_{n_1,n_2}) \cong G(L_{n_1,n_2}) \oplus \mathbb{Z}_p$. Hence, for any finite abelian p-group G, we have

$$\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G))\right| = \left|\mathrm{Hom}(G(L_n^{(\alpha)}), G)\right| \times |G|\,.$$

Therefore, Proposition 3.2.8 implies that

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Hom}(G(L_n^{(\alpha)}), G)\right|\right] &= \frac{1}{|G|}\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G)\right|\right] \\ &= \frac{1}{|G|}\sum_{T\trianglelefteq_{\mathrm{tr}} G} \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)|\,.\end{aligned}$$

Now, for each $H \trianglelefteq G$, there are $\frac{|G|}{|H|}$ translated subgroups $T \trianglelefteq_{\mathrm{tr}} G$ for which $\mathcal{G}(T) = H$. Therefore,

$$\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Hom}(G(L_n^{(\alpha)}), G)\right|\right] = \frac{1}{|G|}\sum_{H\trianglelefteq G} \frac{|G|}{|H|}\left|\Delta^2 H\right| \times |H| = \sum_{H\trianglelefteq G}\left|\Delta^2 H\right|.$$

Since

$$\left|\mathrm{Hom}(G(L_n^{(\alpha)}), G)\right| = \sum_{H\trianglelefteq G}\left|\mathrm{Sur}(G(L_n^{(\alpha)}), H)\right|,$$

by induction on the size of G, we see that

$$\lim_{n\to\infty} \mathbb{E}_\rho\left[\left|\mathrm{Sur}(G(L_n^{(\alpha)}), G)\right|\right] = \left|\Delta^2 G\right|. \qquad \square$$

Therefore, for odd p, Conjecture 3.1.3 will follow once we prove Proposition 3.2.8.

3.2.3 Decomposing Expectation

Each map in $\mathrm{Hom}(\mathrm{Coker}(L_{n_1,n_2}), G)$ can be lifted to a map in $\mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)$. Moreover, $F \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)$ descends to a map in $\mathrm{Hom}(\mathrm{Coker}(L_{n_1,n_2}), G)$ if and only if $F \circ L_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)$. Moreover,

$$\mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G) = \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G) \oplus \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G).$$

Therefore,

$$\begin{aligned}
&\mathbb{E}'_\rho[|\mathrm{Hom}(\mathrm{Coker}(L_{n_1,n_2}), G)|] \\
&= \sum_{F \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G)} \mathbb{P}\big[F \circ L_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G), \eta(L_{n_1,n_2}) \in \mathcal{E}_{n,\rho}\big] \\
&= \sum_{F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n1}, G)} \sum_{F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n2}, G)} \mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = 0 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1+n_2}, G), \eta(L_{n_1,n_2}) \in \mathcal{E}_{n,\rho}].
\end{aligned}$$

Since G is a finite abelian p-group, it is also a $\mathbb{Z}_p$-module. Given a subset $X \subseteq G$, the subgroup of G generated by X is denoted by

$$\langle X \rangle = \left\{ \sum a_k x_k : a_k \in \mathbb{Z}_p, x_k \in X \right\}.$$

For a subset $X \subseteq G$, we denote the smallest translated subgroup containing X by

$$\langle X \rangle_1 = \left\{ \sum a_k x_k : a_k \in \mathbb{Z}_p, x_k \in X, \sum a_k = 1 \right\}.$$

Let $[n] = \{1, \ldots, n\}$. Denote the standard basis of $\mathbb{Z}_p^n$ by $e_1, \ldots, e_n$. For $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$, by abuse of notation we denote

$$\mathrm{set}(F) = \{F(e_i) : i \in [n]\}, \qquad \langle F \rangle = \langle F(e_i) : i \in [n] \rangle, \qquad \langle F \rangle_1 = \langle F(e_i) : i \in [n] \rangle_1.$$

Definition 3.2.9. Let T be a translated subgroup of G. We say that $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ is a *translated code* of distance d with image T, if for every $\sigma \subseteq [n]$ with $|\sigma| < d$, we have

$$\langle F(e_i) : i \in [n] \setminus \sigma \rangle_1 = T.$$

Note that if $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ is a *translated code* of distance d with image T, then $\langle F \rangle_1 = T$. If $T_2 \trianglelefteq_{\mathrm{tr}} T_1 \trianglelefteq_{\mathrm{tr}} G$ is a chain of translated subgroups, then we denote $[T_1 : T_2] = \frac{|T_1|}{|T_2|}$.

This is closely related to the notion of *code* introduced by Wood in [23]. In fact $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ is a translated code of distance d with image T, if and only if for any $g \in T$, the map $-g + F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$ is a code of distance d with image $\mathcal{G}(T)$.

Definition 3.2.10. Given $\delta > 0$ and $F \in \mathrm{Hom}(\mathbb{Z}_p^n, G)$, the δ-depth of F is defined to be the largest positive integer D, for which there is a subset $\sigma \subseteq [n]$ with $|\sigma| < \log_p(D)\delta n$ such that

$$[\langle F \rangle_1 : \langle F(e_i) : i \in [n] \setminus \sigma \rangle_1] = D,$$

or 1 if there is no such σ.

If such a σ exists, then we say that F is of δ-type $(\langle F \rangle_1, \langle F(e_i) : i \in [n] \setminus \sigma \rangle_1)$. If there is no such σ, then we set the δ-type to be $(\langle F \rangle_1, \langle F \rangle_1)$.

Our definition of δ-depth is closely related to, but conflicts with the definition provided by Wood in [23].

Note that if F has δ-depth 1, then it is a translated code of distance δn. Given a chain of translated subgroups $T \trianglelefteq_{\mathrm{tr}} S \trianglelefteq_{\mathrm{tr}} G$, we denote

$$\mathcal{S}_{n,\delta}(S,T) := \{F \in \mathrm{Hom}(\mathbb{Z}_p^n, G) : \delta - \text{type } (S,T)\}.$$

This gives a cover

$$\mathrm{Hom}(\mathbb{Z}_p^n, G) = \bigcup_{T \trianglelefteq_{\mathrm{tr}} S \trianglelefteq_{\mathrm{tr}} G} \mathcal{S}_{n,\delta}(S,T).$$

In general, this union need not be disjoint, since a given F may have δ-type (S,T) for more than one choice of T. However, the pieces $\mathcal{S}_{n,\delta}(S,S)$ consist of translated codes with image S, and these pieces are pairwise disjoint.

Proposition 3.2.8 will follow from the following result.

Proposition 3.2.11. *Let p be a prime, $\frac{1}{p} < \alpha \leq 1$, $0 < \rho < \alpha - \frac{1}{p}$ and G be a finite abelian p-group. Consider chains of translated subgroups $T_1 \trianglelefteq_{tr} S_1 \trianglelefteq_{tr} G$, $T_2 \trianglelefteq_{tr} S_2 \trianglelefteq_{tr} G$. We have*

$$\begin{aligned}\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(S_1,T_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(S_2,T_2)} & \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \\ &= \begin{cases} |\Delta^2 \mathcal{G}(T_1)| \times |\mathcal{G}(T_1)| & \text{if } T_1 = T_2 = S_1 = S_2, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Proof of Proposition 3.2.8 assuming Proposition 3.2.11. Proposition 3.2.11 implies at once that

$$\lim_{n\to\infty} \mathbb{E}'_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G)\right|\right] = \sum_{T \trianglelefteq_{\mathrm{tr}} G} \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)|.$$

Since

$$\mathbb{E}'_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G)\right|\right] = \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \times \mathbb{E}_\rho\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), G)\right|\right],$$

the result follows from Lemma 3.9.8. $\square$

3.2.4 Characters

Denote the standard basis of $\mathbb{Z}_p^{n_1}$ as $e_1, \ldots, e_{n_1}$ and the standard basis of $\mathbb{Z}_p^{n_2}$ as $\epsilon_1, \ldots, \epsilon_{n_2}$. Since $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$, $F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G)$ are determined by their values on the basis, we can treat them as functions in $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$ with $F_1(i) = F_1(e_i)$ and $F_2(j) = F_2(\epsilon_j)$.

For $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$, denote $T_1 = \langle F_1 \rangle_1$, $T_2 = \langle F_2 \rangle_1$. Then $(F_1, F_2) \circ L_{n_1,n_2}$ is as follows

$$\begin{aligned} ((F_1, F_2) \circ L_{n_1,n_2})(e_i) &= \sum_{j=1}^{n_2} a_{ij}(F_2(j) - F_1(i)) \in \langle -F_1(i) + T_2 \rangle \,, \\ ((F_1, F_2) \circ L_{n_1,n_2})(\epsilon_j) &= \sum_{i=1}^{n_1} a_{ij}(F_1(i) - F_2(j)) \in \langle -F_2(j) + T_1 \rangle \,. \end{aligned} \tag{3.2}$$

Given a translated subgroup $T \trianglelefteq_{\mathrm{tr}} G$ and $F \in \mathrm{Hom}([n], G)$, we define $\mathcal{C}_n(T, F)$ to be the set of maps

$$F' : [n] \to \bigcup_{i=1}^{n} \langle -F(i) + T \rangle \,,$$

for which each $F'(i) \in \langle -F(i) + T \rangle$. Clearly,

$$|\mathcal{C}_n(T, F)| = \prod_{i=1}^{n} |\langle -F(i) + T \rangle| \,.$$

Note that $(F_1, F_2) \circ L_{n_1,n_2} \in \mathcal{C}_{n_1}(\langle F_2 \rangle_1, F_1) \times \mathcal{C}_{n_2}(\langle F_1 \rangle_1, F_2)$.

Denote

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times);$$

this is a multiplicative group.

For a translated subgroup $T \trianglelefteq_{\text{tr}} G$ and an element $g \in G$ such that $g \notin T$, we construct a character of $\langle -g+T \rangle$ which will help us determine which (F_1', F_2') can occur as $(F_1, F_2) \circ L_{n_1,n_2}$ if we are given that $\eta(L_{n_1,n_2}) = \vec{t}$.

Lemma 3.2.12. *Given a translated subgroup $T \trianglelefteq_{tr} G$ and an element $g \in G$ such that $g \notin T$, there is a character $\chi_{T,g} \in \langle -g+T \rangle^*$ such that for every $x \in -g+T$, $\chi_{T,g}(x) = \zeta_p$.*

Proof. To show this we need to show that whenever we have $h_1, \ldots, h_m \in T$ and $a_1, \ldots, a_m \in \mathbb{Z}_p$ for which $\sum_k a_k(-g+h_k) = 0$, then $\prod_k \zeta_p^{a_k} = 1$.

Suppose $\sum_k a_k(-g+h_k) = 0$, then $(\sum_k a_k)g = \sum_k a_k h_k$. Now, if $\sum_k a_k \not\equiv 0 \pmod{p}$, then it is a unit, which means

$$g = \sum_l \frac{a_l}{\sum_k a_k} h_l \in T.$$

This is a contradiction, so $\sum_k a_k \equiv 0 \pmod{p}$. Thus $\prod_k \zeta_p^{a_k} = 1$. $\square$

Lemma 3.2.13. *Suppose $\eta(L_{n_1,n_2}) = \vec{t} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. Consider $F_1 \in \mathrm{Hom}([n_1], G)$ and $F_2 \in \mathrm{Hom}([n_2], G)$ such that $\langle F_1 \rangle_1 = T_1$ and $\langle F_2 \rangle_1 = T_2$. If*

$$(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2') \in \mathcal{C}_{n_1}(\langle F_2 \rangle_1, F_1) \times \mathcal{C}_{n_2}(\langle F_1 \rangle_1, F_2),$$

then for every $i \in [n_1]$, if $F_1(i) \notin T_2$, then $\chi_{T_2,F_1(i)}(F_1'(i)) = \zeta_p^{t_i}$.

Proof. Since $\eta(L_{n_1,n_2}) = \vec{t}$, we know that $\sum_{j\in[n_2]} a_{ij} \equiv t_i \pmod{p}$. Also since $(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2')$, we know that

$$\sum_{j\in[n_2]} a_{ij}(-F_1(i) + F_2(j)) = F_1'(i).$$

This implies that

$$\chi_{T_2,F_1(i)}(F_1'(i)) = \chi_{T_2,F_1(i)}\left(\sum_{j\in[n_2]} a_{ij}(-F_1(i)+F_2(j))\right)$$
$$= \prod_{j\in[n_2]} \chi_{T_2,F_1(i)}\left(-F_1(i)+F_2(j)\right)^{a_{ij}} = \prod_{j\in[n_2]} \zeta_p^{a_{ij}} = \zeta_p^{t_i}. \qquad \square$$

This lemma implies that if there is an index $i \in [n_1]$, such that $F_1(i) \in T_1 \setminus T_2$ and $t_i \neq 0$ then

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = 0, \eta(L_{n_1,n_2}) = \vec{t}] = 0.$$

This indicates that if $T_1 \setminus T_2 \neq \emptyset$, then we should expect

$$\sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,T_1)} \sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,T_2)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}]$$

to be much larger for $\vec{t} \notin \mathcal{E}_{n,\rho}$ than for $\vec{t} \in \mathcal{E}_{n,\rho}$. This suggests that restricting to the event $\vec{t} \in \mathcal{E}_{n,\rho}$, might prevent the moments from blowing up to ∞.

3.2.5 Coefficients

Given a translated subgroup $T \trianglelefteq_{\mathrm{tr}} G$ and $F \in \mathrm{Hom}([n], G)$, we define $\mathcal{C}_n^*(T,F)$ to be the set of the maps

$$C : [n] \to \bigcup_{i=1}^{n} \langle -F(i) + T\rangle^*,$$

for which each $C(i) \in \langle -F(i) + T\rangle^*$. Clearly,

$$|\mathcal{C}_n^*(T,F)| = \prod_{i=1}^{n} |\langle -F(i) + T\rangle|.$$

For any $F_1' \in \mathcal{C}_{n_1}(\langle F_2\rangle_1, F_1)$, $F_2' \in \mathcal{C}_{n_2}(\langle F_1\rangle_1, F_2)$, by (3.2), we have

$$\begin{aligned}
&\mathbb{1}_{(F_1,F_2)\circ L_{n_1,n_2}=(F_1',F_2')} \\
&= \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|}\frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|}\sum_{C_1\in\mathcal{C}^*_{n_1}(\langle F_2\rangle_1,F_1)}\sum_{C_2\in\mathcal{C}^*_{n_2}(\langle F_1\rangle_1,F_2)} \\
&\quad \prod_{i=1}^{n_1} C_1(i)\Big((F_1,F_2)\circ L_{n_1,n_2}(e_i) - F_1'(i)\Big)\prod_{j=1}^{n_2} C_2(j)\Big((F_1,F_2)\circ L_{n_1,n_2}(\epsilon_j) - F_2'(j)\Big) \\
&= \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|}\frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|}\sum_{C_1\in\mathcal{C}^*_{n_1}(\langle F_2\rangle_1,F_1)}\sum_{C_2\in\mathcal{C}^*_{n_2}(\langle F_1\rangle_1,F_2)}\prod_{i=1}^{n_1} C_1(i)(-F_1'(i)) \\
&\quad \prod_{j=1}^{n_2} C_2(j)(-F_2'(j))\prod_{i=1}^{n_1}\prod_{j=1}^{n_2}\Big(C_1(i)\big(F_2(j)-F_1(i)\big)C_2(j)\big(F_1(i)-F_2(j)\big)\Big)^{a_{ij}}.
\end{aligned} \tag{3.3}$$

We denote

$$E[F_1,F_2,C_1,C_2](i,j) = C_1(i)\big(F_2(j)-F_1(i)\big)C_2(j)\big(F_1(i)-F_2(j)\big).$$

Suppose $\vec{x} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$ is a random vector, then for fixed $\vec{t} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$, we have

$$\mathbb{1}_{\vec{x}=\vec{t}} = \frac{1}{p^{n_1}}\sum_{\vec{s}\in(\mathbb{Z}/p\mathbb{Z})^{n_1}} \zeta_p^{\vec{s}\cdot(\vec{x}-\vec{t})}.$$

Therefore, for $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$, $\vec{t} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$, $F_1' \in \mathcal{C}_{n_1}(\langle F_2\rangle_1, F_1)$ and $F_2' \in \mathcal{C}_{n_2}(\langle F_1\rangle_1, F_2)$, we have

$$\begin{aligned}
&\mathbb{P}[(F_1,F_2)\circ L_{n_1,n_2} = (F_1',F_2') \text{ and } \eta(L_{n_1,n_2}) = \vec{t}] \\
&= \mathbb{E}[\mathbb{1}_{(F_1,F_2)\circ L_{n_1,n_2}=(F_1',F_2')}\mathbb{1}_{\eta(L_{n_1,n_2})=\vec{t}}] \\
&= \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|}\frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|}\frac{1}{p^{n_1}}\sum_{C_1\in\mathcal{C}^*_{n_1}(\langle F_2\rangle_1,F_1)}\sum_{C_2\in\mathcal{C}^*_{n_2}(\langle F_1\rangle_1,F_2)}\sum_{\vec{s}\in(\mathbb{Z}/p\mathbb{Z})^{n_1}} \\
&\quad \zeta_p^{-\vec{s}\cdot\vec{t}}\prod_{i=1}^{n_1} C_1(i)(-F_1'(i))\prod_{j=1}^{n_2} C_2(j)(-F_2'(j))\mathbb{E}\left[\prod_{i=1}^{n_1}\prod_{j=1}^{n_2}\Big(E[F_1,F_2,C_1,C_2](i,j)\Big)^{a_{ij}}\prod_{i=1}^{n_1}\zeta_p^{s_i\sum_{j=1}^{n_2}a_{ij}}\right].
\end{aligned}$$

We denote

$$
\begin{aligned}
E'[F_1, F_2, C_1, C_2, \vec{s}](i, j) &= E[F_1, F_2, C_1, C_2](i, j)\zeta_p^{s_i} \\
&= C_1(i)\big(F_2(j) - F_1(i)\big)C_2(j)\big(F_1(i) - F_2(j)\big)\zeta_p^{s_i}.
\end{aligned}
$$

Since the a_{ij} are independent, we see that

$$
\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2') \text{ and } \eta(L_{n_1,n_2}) = \vec{t}] \\
&= \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|} \frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|} \frac{1}{p^{n_1}} \sum_{C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)} \sum_{C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)} \sum_{\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}} \\
&\qquad \zeta_p^{-\vec{s}\cdot\vec{t}} \prod_{i=1}^{n_1} C_1(i)(-F_1'(i)) \prod_{j=1}^{n_2} C_2(j)(-F_2'(j)) \prod_{i=1}^{n_1}\prod_{j=1}^{n_2} \mathbb{E}\left[E'[F_1, F_2, C_1, C_2, \vec{s}](i, j)^{a_{ij}}\right].
\end{aligned} \tag{3.4}
$$

Definition 3.2.14. Given $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$, $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$, we say that (C_1, C_2) is $(F_1, F_2, \vec{s})$-*special* if for every $i \in [n_1]$ and every $j \in [n_2]$, we have $E'[F_1, F_2, C_1, C_2, \vec{s}](i, j) = 1$.

Thus, as a heuristic,

$$
\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = 0 \text{ and } \eta(L_{n_1,n_2}) = \vec{t}] \\
&\approx \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right| \times \left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right| p^{n_1}} \sum_{\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}} \zeta_p^{-\vec{s}\cdot\vec{t}} \left|\{(C_1, C_2) : (F_1, F_2, \vec{s})\text{-special}\}\right|.
\end{aligned}
$$

This would be an exact equation if all a_{ij} were Haar uniform.

In general, if the a_{ij} are not necessarily Haar uniform, then $\mathbb{E}\left[E'[F_1, F_2, C_1, C_2, \vec{s}](i, j)^{a_{ij}}\right]$ might not be exactly zero. However, the following lemma of Wood suggests that it would be small as long as a_{ij} are ϵ-balanced.

Lemma 3.2.15. *[23, Lemma 4.2] If $\xi \neq 1$ is a b^{th} root of unity and $a \in \mathbb{Z}_p$ is ϵ-balanced,*

then

$$|\mathbb{E}[\xi^a]| \leq \exp\left(-\frac{\epsilon}{b^2}\right).$$

In [23], Wood divides the set of non-special $C \in \text{Hom}([n], G^*)$ based on a constant $\gamma > 0$ into those that are robust and not robust. She shows that most C are robust, and that for robust C, at least quadratically many of the coefficients $E(i,j)$ are not 1. On the other hand for the few C that are not special and not robust, at least linearly many of the coefficients $E(i,j)$ are not 1.

We follow a similar approach to Wood, but we need to partition $\mathcal{C}^*_{n_1}(T_2, F_1)$, $\mathcal{C}^*_{n_2}(T_1, F_2)$ and $(\mathbb{Z}/p\mathbb{Z})^{n_1}$. We will need slightly different definitions of robustness for the three.

Definition 3.2.16.

1. Given a translated subgroup T of G, $F \in \text{Hom}([n], G)$ and $C \in \mathcal{C}^*_n(T, F)$, we say that C is (d, F)-*robust* if for every $\sigma \subseteq [n]$ with $|\sigma| < d$, there are $i_1, i_2 \in [n] \setminus \sigma$ such that $F(i_1) = F(i_2)$ and $C(i_1) \neq C(i_2)$.

2. Given a translated subgroup T of G, $F \in \text{Hom}([n], G)$, $C \in \mathcal{C}^*_n(T, F)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$, we say that C is $(d, F, \vec{s})$-*robust* if for every $\sigma \subseteq [n]$ with $|\sigma| < d$, there are $i_1, i_2 \in [n] \setminus \sigma$ such that $F(i_1) = F(i_2)$, $s_{i_1} = s_{i_2}$ and $C(i_1) \neq C(i_2)$.

3. Given $F \in \text{Hom}([n], G)$, $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$ and a translated subgroup $T \trianglelefteq_{\text{tr}} G$, we say that $\vec{s}$ is (d, F, T)-robust, if for every $\sigma \subseteq [n]$ with $|\sigma| < d$, there are $i_1, i_2 \in [n] \setminus \sigma$ such that $F(i_1) = F(i_2) \in T$ and $s_{i_1} \neq s_{i_2}$.

3.3 Robust C_1 or C_2

In this section, we consider $F_1 \in \text{Hom}([n_1], G)$, $F_2 \in \text{Hom}([n_2], G)$, $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2 \rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1 \rangle_1, F_2)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$ such that F_1 and F_2 are translated codes and at least one of C_1, C_2 or $\vec{s}$ is robust. Our goal is to show that in this case quadratically many of the coefficients $E'[F_1, F_2, C_1, C_2, \vec{s}](i, j)$ are $\neq 1$.

Lemma 3.3.1. *Suppose $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$, $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2 \rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1 \rangle_1, F_2)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. Suppose $\tau_1 \subseteq [n_1]$ and $\tau_2 \subseteq [n_2]$ are such that for each $i \in \tau_1$, $j \in \tau_2$*

$$E'[F_1, F_2, C_1, C_2, \vec{s}](i, j) = 1.$$

Denote $T_1 = \langle F_1(i) : i \in \tau_1 \rangle_1 \subseteq \langle F_1 \rangle_1$ and $T_2 = \langle F_2(j) : j \in \tau_2 \rangle_1 \subseteq \langle F_2 \rangle_1$. Then the following hold:

1. *If $T_1 = \langle F_1 \rangle_1$, then for every $j_1, j_2 \in \tau_2$ with $F_2(j_1) = F_2(j_2)$, we have $C_2(j_1) = C_2(j_2)$.*
2. *If $T_2 = \langle F_2 \rangle_1$, then for every $i_1, i_2 \in \tau_1$ with $F_1(i_1) = F_1(i_2)$ and $s_{i_1} = s_{i_2}$, we have $C_1(i_1) = C_1(i_2)$.*
3. *For every $i_1, i_2 \in \tau_1$ with $F_1(i_1) = F_1(i_2) \in T_2$, we have $s_{i_1} = s_{i_2}$.*

Proof. First, assume $T_1 = \langle F_1 \rangle_1$ and consider $j_1, j_2 \in \tau_2$ with $F_2(j_1) = F_2(j_2) = h$. For each $i \in \tau_1$, we know that

$$C_2(j_1)(F_1(i) - h) = C_1(i)(F_1(i) - h)\zeta_p^{-s_i},$$

and

$$C_2(j_2)(F_1(i) - h) = C_1(i)(F_1(i) - h)\zeta_p^{-s_i},$$

meaning

$$C_2(j_1)(-h + F_1(i)) = C_2(j_2)(-h + F_1(i)).$$

It follows that for every $x \in -h+T_1$, we have $C_2(j_1)(x) = C_2(j_2)(x)$. Since $T_1 = \langle F_1 \rangle_1$ and the characters $C_2(j_1)$ and $C_2(j_2)$ are defined on $\langle -h + \langle F_1 \rangle_1 \rangle$, we see that $C_2(j_1) = C_2(j_2)$.

Next, assume that $T_2 = \langle F_2 \rangle_1$ and consider $i_1, i_2 \in \tau_1$ with $F_1(i_1) = F_1(i_2) = g$ and $s_{i_1} = s_{i_2}$. For each $j \in \tau_2$, we have

$$C_1(i_1)(-g + F_2(j)) = C_2(j)(-g + F_2(j))\zeta_p^{-s_{i_1}},$$

and

$$C_1(i_2)(-g + F_2(j)) = C_2(j)(-g + F_2(j))\zeta_p^{-s_{i_2}},$$

meaning

$$C_1(i_1)(-g + F_2(j)) = C_1(i_2)(-g + F_2(j)).$$

It follows that for every $x \in -g+T_2$, we have $C_1(i_1)(x) = C_1(i_2)(x)$. Since $T_2 = \langle F_2 \rangle_1$ and the characters $C_1(i_1)$ and $C_1(i_2)$ are defined on $\langle -g + \langle F_2 \rangle_1 \rangle$, we see that $C_1(i_1) = C_1(i_2)$.

For the last part, consider $i_1, i_2 \in \tau_1$ for which $F_1(i_1) = F_1(i_2) \in T_2$. Denote $F_1(i_1) = F_1(i_2) = g$. For each $j \in \tau_2$, we have

$$C_1(i_1)(-g + F_2(j)) = C_2(j)(-g + F_2(j))\zeta_p^{-s_{i_1}},$$

and

$$C_1(i_2)(-g + F_2(j)) = C_2(j)(-g + F_2(j))\zeta_p^{-s_{i_2}},$$

meaning

$$C_1(i_1)(-g+F_2(j)) = \zeta_p^{s_{i_2}-s_{i_1}} C_1(i_2)(-g+F_2(j)).$$

It follows that for every $x \in -g+T_2$, we have $C_1(i_1)(x) = \zeta_p^{s_{i_2}-s_{i_1}} C_1(i_2)(x)$. Since $g \in T_2$, we can take $x=0$, which implies $s_{i_1} = s_{i_2}$. $\square$

Lemma 3.3.2. *Suppose $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$, $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. Then the following hold.*

1. *If F_1 is a translated code of distance d_1 with image T_1 and C_2 is (d_2, F_2)-robust then*

$$|\{(i,j) \in [n_1]\times[n_2] : E'[F_1, F_2, C_1, C_2, \vec{s}] \neq 1\}| \geq \frac{d_1 d_2}{p\,|G|^2}.$$

2. *If F_2 is a translated code of distance d_1 with image T_2 and C_1 is $(d_2, F_1, \vec{s})$-robust then*

$$|\{(i,j) \in [n_1]\times[n_2] : E'[F_1, F_2, C_1, C_2, \vec{s}] \neq 1\}| \geq \frac{d_1 d_2}{|G|^2}.$$

3. *If F_2 is a translated code of distance d_1 with image T_2, and $\vec{s}$ is (d_2, F_1, T_2)-robust, then*

$$|\{(i,j) \in [n_1]\times[n_2] : E'[F_1, F_2, C_1, C_2, \vec{s}] \neq 1\}| \geq \frac{d_1 d_2}{|G|^2}.$$

Proof. 1. First, suppose that F_1 is a translated code of distance d_1 with image T_1 and C_2 is (d_2, F_2)-robust. Consider

$$X_1 = \left\{ g \in T_1 : |\{i \in [n_1] : F_1(i) = g\}| \geq \frac{d_1}{|G|} \right\}.$$

It is clear that $|\{i \in [n_1] : F_1(i) \notin X_1\}| < d_1$. Since F_1 is a translated code of distance d_1 with image T_1, this means $\langle X_1\rangle_1 = T_1$.

Enumerate the elements of X_1 as $A_1, \ldots, A_m$. By the pigeonhole principle, we know that there is some $B_k \in \langle -A_k + \langle F_2 \rangle_1 \rangle^*$ and $u_k \in \mathbb{Z}/p\mathbb{Z}$ for which

$$|S(A_k, B_k, u_k)| = |\{i \in [n_1] : F_1(i) = A_k, C_1(i) = B_k, s_i = u_k\}| \geq \frac{1}{p\,|\langle -A_k + \langle F_2 \rangle_1 \rangle|} \frac{d_1}{|G|} \geq \frac{d_1}{p\,|G|^2}.$$

Let $\tau_1 = \bigcup_{k=1}^{m} S(A_k, B_k, u_k)$. Denote

$$\sigma = \{j \in [n_2] : \exists i \in \tau_1 \text{ such that } E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1\}, \qquad \tau_2 = [n_2] \setminus \sigma.$$

This means that for each $i \in \tau_1$ and $j \in \tau_2$, we have $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) = 1$. Since $\langle X_1 \rangle_1 = \langle F_1 \rangle_1$, Lemma 3.3.1 implies that for $j_1, j_2 \in \tau_2$, if $F_2(j_1) = F_2(j_2)$ then $C_2(j_1) = C_2(j_2)$. Since C_2 is (d_2, F_2)-robust, it follows that $|\sigma| \geq d_2$.

For each $j \in \sigma$, there is at least one $i \in \tau_1$ for which $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1$. If $i \in S(A_k, B_k, u_k)$, then it follows that for every $i' \in S(A_k, B_k, u_k)$, $E'[F_1, F_2, C_1, C_2, \vec{s}](i', j) \neq 1$. The result follows.

2. Next, suppose that F_2 is a translated code of distance d_1 with image T_2 and C_1 is $(d_2, F_1, \vec{s})$-robust. Consider

$$X_2 = \left\{ h \in T_2 : |\{j \in [n_2] : F_2(j) = h\}| \geq \frac{d_1}{|G|} \right\}.$$

It is clear that $|\{j \in [n_2] : F_2(j) \notin X_2\}| < d_1$. Since F_2 is a translated code of distance d_1 with image T_2, this means $\langle X_2 \rangle_1 = T_2$.

Enumerate the elements of X_2 as $A_1, \ldots, A_m$. By the pigeonhole principle, we know that there is some $B_k \in \langle -A_k + \langle F_1 \rangle_1 \rangle^*$ for which

$$|S(A_k, B_k)| = |\{j \in [n_2] : F_2(j) = A_k, C_2(j) = B_k\}| \geq \frac{d_1}{|\langle -A_k + \langle F_1 \rangle_1 \rangle|\,|G|} \geq \frac{d_1}{|G|^2}.$$

Let $\tau_2 = \bigcup_{k=1}^m S(A_k, B_k)$. Denote

$$\sigma = \{i \in [n_1] : \exists j \in \tau_2 \text{ such that } E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1\}, \qquad \tau_1 = [n_1] \setminus \sigma.$$

This means that for each $i \in \tau_1$ and $j \in \tau_2$, we have $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) = 1$.

Since $\langle X_2 \rangle_1 = \langle F_2 \rangle_1$, Lemma 3.3.1 implies that for $i_1, i_2 \in \tau_1$, if $F_1(i_1) = F_1(i_2)$ and $s_{i_1} = s_{i_2}$ then $C_1(i_1) = C_1(i_2)$. Since C_1 is $(d_2, F_1, \vec{s})$-robust, it follows that $|\sigma| \geq d_2$.

For each $i \in \sigma$, there is at least one $j \in \tau_2$ for which $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1$. If $j \in S(A_k, B_k)$, then it follows that for every $j' \in S(A_k, B_k)$, $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j') \neq 1$. The result follows.

3. For the last part, suppose F_2 is a translated code of distance d_1 with image T_2 and $\vec{s}$ is (d_2, F_1, T_2)-robust. Consider

$$X_2 = \left\{ h \in T_2 : |\{j \in [n_2] : F_2(j) = h\}| \geq \frac{d_1}{|G|} \right\}.$$

It is clear that $|\{j \in [n_2] : F_2(j) \notin X_2\}| < d_1$. Since F_2 is a translated code of distance d_1 with image T_2, this means $\langle X_2 \rangle_1 = T_2$.

Enumerate the elements of X_2 as $A_1, \ldots, A_m$. For each $1 \leq k \leq m$, by the pigeonhole principle, we know that there is some $B_k \in \langle -A_k + \langle F_1 \rangle_1 \rangle^*$ for which

$$|S(A_k, B_k)| = |\{j \in [n_2] : F_2(j) = A_k, C_2(j) = B_k\}| \geq \frac{d_1}{|\langle -A_k + \langle F_1 \rangle_1 \rangle| \, |G|} \geq \frac{d_1}{|G|^2}.$$

Let $\tau_2 = \bigcup_{k=1}^m S(A_k, B_k)$. Denote

$$\sigma = \{i \in [n_1] : \exists j \in \tau_2 \text{ such that } E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1\}, \qquad \tau_1 = [n_1] \setminus \sigma.$$

This means that for each $i \in \tau_1$ and $j \in \tau_2$, we have $E'[F_1, F_2, C_1, C_2, \vec{s}](i, j) = 1$.

Lemma 3.3.1 tells us that for $i_1, i_2 \in \tau_1$, if $F_1(i_1) = F_1(i_2) \in T_2$, then $s_{i_1} = s_{i_2}$. Since $\vec{s}$ is (d_2, F_1, T_2)-robust, it follows that $|\sigma| \geq d_2$.

For each $i \in \sigma$, there is at least one $j \in \tau_2$ for which $E'[F_1, F_2, C_1, C_2, \vec{s}](i, j) \neq 1$. If $j \in S(A_k, B_k)$, then it follows that for every $j' \in S(A_k, B_k)$, $E'[F_1, F_2, C_1, C_2, \vec{s}](i, j') \neq 1$. The result follows. □

3.4 Special (C_1, C_2)

Consider $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], G)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. In this section, our goal is to count the number of (C_1, C_2), with $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2 \rangle_1, F_1)$ and $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1 \rangle_1, F_2)$, that are $(F_1, F_2, \vec{s})$-special.

We will show the following.

Proposition 3.4.1. *Consider $F_1 \in \mathrm{Hom}([n_1], G)$ and $F_2 \in \mathrm{Hom}([n_2], G)$. Then the following hold.*

1. *The number of triples $(\vec{s}, C_1, C_2)$, with $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$, $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2 \rangle_1, F_1)$ and $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1 \rangle_1, F_2)$, such that (C_1, C_2) is $(F_1, F_2, \vec{s})$-special is at most*

$$p^{|G|} \times |G|^{(p+1)|G|} \times p^{\left|\{i \in [n_1] : F_1(i) \notin \langle F_2 \rangle_1\}\right|}.$$

2. *If $\mathrm{set}(F_1) = \mathrm{set}(F_2) = T$ for some $T \trianglelefteq_{tr} G$, then the number of $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2 \rangle_1, F_1)$ and $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1 \rangle_1, F_2)$, such that (C_1, C_2) is $(F_1, F_2, \vec{s})$-special is exactly*

$$= \begin{cases} |\Delta^2 \mathcal{G}(T)| \times |T| & \text{if } \vec{s} = 0, \\ 0 & \text{if } \vec{s} \neq 0. \end{cases}$$

3.4.1 Upper bound

Lemma 3.3.1 tells us that if (C_1, C_2) is $(F_1, F_2, \vec{s})$-special, then the map C_1 factors through

$$C_1 : [n_1] \xrightarrow{(F_1,s)} G \times (\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\beta_1} \bigcup_{g \in \langle F_1 \rangle_1} \langle -g + \langle F_2 \rangle_1 \rangle^* \,,$$

for some β_1 and the map C_2 factors through

$$C_2 : [n_2] \xrightarrow{F_2} G \xrightarrow{\beta_2} \bigcup_{h \in \langle F_2 \rangle_1} \langle -h + \langle F_1 \rangle_1 \rangle^* \,,$$

for some β_2.

Given $F \in \mathrm{Hom}([n], G)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$, we denote

$$\mathrm{set}(F, \vec{s}) = \{(F(e_i), s_i) : i \in [n]\} \subseteq G \times (\mathbb{Z}/p\mathbb{Z}).$$

We will denote the projections as $\pi_1 : G \times (\mathbb{Z}/p\mathbb{Z}) \to G$ and $\pi_2 : G \times (\mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$.

Given subsets $Y_1 \subseteq G \times (\mathbb{Z}/p\mathbb{Z})$ and $X_2 \subseteq G$, let $X_1 = \pi_1(Y_1)$. We denote by $\mathcal{D}(Y_1, X_2)$, the set of pairs of functions (β_1, β_2) such that the following hold:

1. β_1 maps Y_1 to $\bigcup_{g \in X_1} \langle -g + X_2 \rangle^*$ and for every $(g, s) \in Y_1$, $\beta_1(g, s) \in \langle -g + X_2 \rangle^*$;

2. β_2 maps X_2 to $\bigcup_{h \in X_2} \langle -h + X_1 \rangle^*$ and for every $h \in X_2$, $\beta_2(h) \in \langle -h + X_1 \rangle^*$;

3. For every $(g, s) \in Y_1$ and $h \in X_2$ we have

$$\beta_1(g, s)(-g + h)\beta_2(h)(-h + g)\zeta_p^s = 1.$$

Clearly,

$$|\mathcal{D}(Y_1, X_2)| \leq |G|^{(p+1)|G|}.$$

Lemma 3.4.2. *Consider $F_1 \in \mathrm{Hom}(\mathbb{Z}_p^{n_1}, G)$, $F_2 \in \mathrm{Hom}(\mathbb{Z}_p^{n_2}, G)$ and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. For $C_1 \in \mathcal{C}^*(\langle F_2 \rangle_1, F_1)$, $C_2 \in \mathcal{C}^*(\langle F_1 \rangle_1, F_2)$, the pair (C_1, C_2) is $(F_1, F_2, \vec{s})$-special if and only if there is $(\beta_1, \beta_2) \in \mathcal{D}(\mathrm{set}(F_1, \vec{s}), \mathrm{set}(F_2))$ such that $C_1(i) = \beta_1(F_1(i), s_i)$ and $C_2(j) = \beta_2(F_2(j))$.*

Therefore, the number of pairs (C_1, C_2) that are $(F_1, F_2, \vec{s})$-special is $|\mathcal{D}(\mathrm{set}(F_1, \vec{s}), \mathrm{set}(F_2))|$.

Proof. Denote $Y_1 = \mathrm{set}(F_1, \vec{s})$, $X_1 = \mathrm{set}(F_1)$ and $X_2 = \mathrm{set}(F_2)$. If (C_1, C_2) is $(F_1, F_2, \vec{s})$-special, then by Lemma 3.3.1, we can construct following functions

- $\beta_1 : Y_1 \to \bigcup_{g \in X_1} \langle -g + \langle X_2 \rangle_1 \rangle^*$. For $(g, s) \in Y_1$, choose $i \in [n_1]$ such that $F_1(i) = g$, $s_i = s$, and define $\beta_1(g, s) = C_1(i) \in \langle -g + \langle X_2 \rangle_1 \rangle^*$. By Lemma 3.3.1, this is well defined.

- $\beta_2 : X_2 \to \bigcup_{h \in X_2} \langle -h + \langle X_1 \rangle_1 \rangle^*$. For $h \in X_2$, choose $j \in [n_2]$ such that $F_2(j) = h$, and define $\beta_2(h) = C_2(j) \in \langle -h + \langle X_1 \rangle_1 \rangle^*$. By Lemma 3.3.1, this is well defined.

Since (C_1, C_2) is $(F_1, F_2, \vec{s})$-special, we see that for each $(g, s) \in Y_1$ and $h \in X_2$, we have

$$\beta_1(g, s)(-g + h)\beta_2(h)(-h + g)\zeta_p^s = 1.$$

Therefore, $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$.

Conversely, given $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$, we can construct C_1 and C_2 as $C_1(i) = \beta_1(F_1(i), s_i)$

and $C_2(j) = \beta_2(F_2(j))$. For $i \in [n_1]$, $j \in [n_2]$, we see that

$$\begin{aligned} E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) &= C_1(i)(-F_1(i) + F_2(j))C_2(j)(-F_2(j) + F_1(i))\zeta_p^{s_i} \\ &= \beta_1(F_1(i), s_i)(-F_1(i) + F_2(j))\beta_2(F_2(j))(-F_2(j) + F_1(i))\zeta_p^{s_i} = 1. \end{aligned}$$

Therefore, (C_1, C_2) is $(F_1, F_2, \vec{s})$-special. □

Lemma 3.4.3. *Suppose that we have non-empty subsets $Y_1 \subseteq G \times (\mathbb{Z}/p\mathbb{Z})$ and $X_2 \subseteq G$. If $(g, s), (g, s') \in Y_1$, then for every $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$ and every $x \in -g + \langle X_2 \rangle_1$, we have*

$$\beta_1(g, s')(x) = \zeta_p^{s-s'}\beta_1(g, s)(x).$$

Proof. For each $h \in X_2$, we have

$$\beta_1(g, s)(-g + h) = \left(\zeta_p^{s}\beta_2(h)(-h + g)\right)^{-1},$$

$$\beta_1(g, s')(-g + h) = \left(\zeta_p^{s'}\beta_2(h)(-h + g)\right)^{-1}.$$

This means that for each $x \in -g + X_2$, we have

$$\beta_1(g, s')(x) = \zeta_p^{s-s'}\beta_1(g, s)(x).$$

It follows that the same would hold for every x in $\langle -g + X_2 \rangle_1 = -g + \langle X_2 \rangle_1$. □

Lemma 3.4.4. *Suppose that we have non-empty subsets $Y_1 \subseteq G \times (\mathbb{Z}/p\mathbb{Z})$ and $X_2 \subseteq G$. Let $X_1 = \pi_1(Y_1)$. Then the following hold.*

1. *If there is some $g \in X_1 \cap \langle X_2 \rangle_1$, for which there are (at least) two different (g, s) and (g, s') in Y_1, then $\mathcal{D}(Y_1, X_2) = \emptyset$.*

2. If there is some $g \in X_1 \cap X_2$ with $(g, s) \in Y_1$ and $s \neq 0$, then $\mathcal{D}(Y_1, X_2) = \emptyset$.

Proof. First, suppose that there is some $g \in X_1 \cap \langle X_2 \rangle_1$ for which there are (at least) two different (g, s) and (g, s') in Y_1. Assume for the sake of contradiction that $\mathcal{D}(Y_1, X_2)$ is not empty, consider $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$. By Lemma 3.4.3, we know that for every $x \in -g + \langle X_2 \rangle_1$, we have

$$\beta_1(g, s')(x) = \zeta_p^{s-s'} \beta_1(g, s)(x).$$

Since $g \in \langle X_2 \rangle_1$, we know that $0 \in -g + \langle X_2 \rangle_1$. Taking $x = 0$, we see that $1 = \zeta_p^{s-s'}$. This contradicts the fact that $s \neq s'$. We conclude that $\mathcal{D}(Y_1, X_2)$ is empty.

Next, suppose that there is some $g \in X_1 \cap X_2$ with $(g, s) \in Y_1$ and $s \neq 0$. Assume for the sake of contradiction that $\mathcal{D}(Y_1, X_2) \neq \emptyset$. Consider $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$. Since $(g, s) \in Y_1$ and $g \in X_2$, we have

$$\beta_1(g, s)(-g + g)\beta_2(g)(-g + g)\zeta_p^s = 1.$$

This means $\zeta_p^s = 1$, which contradicts $s \neq 0$. Therefore, $\mathcal{D}(Y_1, X_2) = \emptyset$. □

We are now ready to prove the first part of Proposition 3.4.1.

Proof of part (1) of Proposition 3.4.1. First we count the number of $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$ for which $\mathcal{D}(\mathrm{set}(F_1, \vec{s}), \mathrm{set}(F_2))$ is non-empty. By the first part of Lemma 3.4.4, if $\mathcal{D}(\mathrm{set}(F_1, \vec{s}), \mathrm{set}(F_2)) \neq \emptyset$, then there is a function $\lambda : \mathrm{set}(F_1) \cap \langle F_2 \rangle_1 \to \mathbb{Z}/p\mathbb{Z}$ such that for each $i \in [n_1]$, if $F_1(i) \in \langle F_2 \rangle_1$, then $s_i = \lambda(F_1(i))$.

The number of choices for λ is at most

$$p^{\left|\mathrm{set}(F_1) \cap \langle F_2 \rangle_1\right|} \leq p^{|G|}.$$

Once we fix λ, then the number of choices for $\vec{s}$ is

$$p^{\left|\{i\in[n_1]:F_1(i)\notin\langle F_2\rangle_1\}\right|}.$$

Once we choose $\vec{s}$, then the number of (C_1, C_2) that are $(F_1, F_2, \vec{s})$-special is

$$|\mathcal{D}(\mathrm{set}(F_1, \vec{s}), \mathrm{set}(F_2))| \leq |G|^{(p+1)|G|}.$$

The result follows. $\square$

3.4.2 Exact count for $\mathrm{set}(F_1) = \mathrm{set}(F_2) = T$

Given a translated subgroup $T \trianglelefteq_{\mathrm{tr}} G$, we denote by $D(T,T)$, the set of pairs of functions (β_1, β_2) such that the following hold:

1. β_1 maps T to $\mathcal{G}(T)^*$;

2. β_2 maps T to $\mathcal{G}(T)^*$;

3. For every $g, h \in T$, we have

$$\beta_1(g)(-g+h)\beta_2(h)(-h+g) = 1.$$

Clearly,

$$|D(T,T)| \leq |G|^{2|G|}.$$

Proof of part (2) of Proposition 3.4.1. If $\vec{s} \neq 0$, then the second part of Lemma 3.4.4 implies that

$$|\mathcal{D}(\mathrm{set}(F_1,\vec{s}),T)| = 0.$$

On the other hand, if $\vec{s}=0$, then $\mathrm{set}(F_1,\vec{s}) = T\times\{0\}$. In this case it is clear that

$$|\mathcal{D}(\mathrm{set}(F_1,\vec{s}),T)| = |D(T,T)|\,.$$

Therefore, we will be done if we show that $|D(T,T)| = |\Delta^2\mathcal{G}(T)|\times|T|$.

Let $\mathcal{G}(T) = H$. We will denote the class of $x\otimes y$ in $\Delta^2 H$ by $x\wedge y$. We can see that $|D(T,T)| = |D(H,H)|$, due to the following bijection. Fix $g_0\in T$.

- If $(\beta_1,\beta_2)\in D(T,T)$, then we can define $\alpha_1 : H\to H^*$ and $\alpha_2 : H\to H^*$ as $\alpha_1(x) = \beta_1(g_0+x)$, $\alpha_2(x)=\beta_2(g_0+x)$. It is clear that $(\alpha_1,\alpha_2)\in D(H,H)$.

- If $(\alpha_1,\alpha_2)\in D(H,H)$, then we can define $\beta_1 : T\to H^*$ and $\beta_2 : T\to H^*$ as $\beta_1(g) = \alpha_1(-g_0+g)$, $\beta_2(g)=\alpha_2(-g_0+g)$. It is clear that $(\beta_1,\beta_2)\in D(T,T)$.

Therefore, it is enough to compute the size of $D(H,H)$, that is, the number of maps $\alpha_1 : H\to H^*$ and $\alpha_2 : H\to H^*$ such that for every $x,y\in H$, we have

$$\alpha_1(x)(-x+y)\alpha_2(y)(-y+x) = 1.$$

This is equivalent to saying that for every $y,z\in H$,

$$\alpha_2(y)(z) = \alpha_1(z+y)(z). \tag{3.5}$$

So α_2 is determined by α_1. We want to count how many $\alpha_1 : H\to H^*$ satisfy the condition that the $\alpha_2(y)$ obtained from (3.5) are characters. We are counting the $\alpha_1 : H\to H^*$, such that for every $y, z_1, z_2 \in H$

$$\alpha_1(y+z_1)(z_1)\alpha_1(y+z_2)(z_2) = \alpha_1(y+z_1+z_2)(z_1+z_2). \tag{3.6}$$

Let A be the set of all such α_1.

Consider the map $f : H^* \times (\Delta^2(H))^* \to A$ defined as follows. For $\theta \in H^*$, $\iota \in (\Delta^2(H))^*$ and $x, y \in H$, we define

$$f(\theta,\iota)(x)(y) = \theta(y)\iota(x \wedge y).$$

Note that $f(\theta,\iota)(x)$ is a character since

$$\begin{aligned} f(\theta,\iota)(x)(y_1+y_2) &= \theta(y_1+y_2)\iota(x \wedge (y_1+y_2)) \\ &= \theta(y_1)\theta(y_2)\iota(x \wedge y_1)\iota(x \wedge y_2) \\ &= f(\theta,\iota)(x)(y_1)f(\theta,\iota)(x)(y_2). \end{aligned}$$

Moreover, $f(\theta,\iota) \in A$ since

$$\begin{aligned} &\frac{f(\theta,\iota)(y+z_1+z_2)(z_1+z_2)}{f(\theta,\iota)(y+z_1)(z_1)f(\theta,\iota)(y+z_2)(z_2)} \\ &= \frac{\theta(z_1+z_2)\iota((y+z_1+z_2) \wedge (z_1+z_2))}{\theta(z_1)\iota((y+z_1) \wedge z_1)\theta(z_2)\iota((y+z_2) \wedge z_2)} \\ &= \iota\Big((y+z_1+z_2) \wedge (z_1+z_2) - (y+z_1) \wedge z_1 - (y+z_2) \wedge z_2\Big) \\ &= \iota\Big(z_1 \wedge z_2 + z_2 \wedge z_1\Big) = \iota(0) = 1. \end{aligned}$$

Next, we will show that the map f is injective. Suppose $f(\theta_1,\iota_1) = f(\theta_2,\iota_2)$. Then

$$\theta_1(y) = f(\theta_1,\iota_1)(0)(y) = f(\theta_2,\iota_2)(0)(y) = \theta_2(y).$$

This means that $\theta_1 = \theta_2$. Therefore it follows that $\iota_1 = \iota_2$.

It remains to show that the map $f : H^* \times (\Delta^2(H))^* \to A$ is surjective. Consider $\alpha_1 \in A$. Take $\theta = \alpha_1(0) \in H^*$ and define $\lambda \in (\Delta^2(H))^*$ by

$$\lambda(x \wedge y) = \alpha_1(x)(y)\alpha_1(0)(-y).$$

In order for this to be a valid definition, we need to check that $\lambda((x_1 + x_2) \wedge y) = \lambda(x_1 \wedge y)\lambda(x_2 \wedge y)$, $\lambda(x \wedge (y_1 + y_2)) = \lambda(x \wedge y_1)\lambda(x \wedge y_2)$ and $\lambda(x \wedge y)\lambda(y \wedge x) = 1$.

First, we check that $\lambda(x \wedge (y_1 + y_2)) = \lambda(x \wedge y_1)\lambda(x \wedge y_2)$.

$$\begin{aligned}
&\frac{\lambda(x \wedge (y_1 + y_2))}{\lambda(x \wedge y_1)\lambda(x \wedge y_2)} \\
&= \alpha_1(x)(y_1 + y_2)\alpha_1(0)(-y_1 - y_2) \times \alpha_1(x)(-y_1)\alpha_1(0)(y_1) \times \alpha_1(x)(-y_2)\alpha_1(0)(y_2) \\
&= 1.
\end{aligned}$$

Next, we check that $\lambda(x \wedge y)\lambda(y \wedge x) = 1$. Note that

$$\begin{aligned}
\lambda(x \wedge y)\lambda(y \wedge x) &= \alpha_1(x)(y)\alpha_1(0)(-y) \times \alpha_1(y)(x)\alpha_1(0)(-x) \\
&= \alpha_1(x)(y)\alpha_1(y)(x)\alpha_1(0)(-x - y).
\end{aligned}$$

Now (3.6), tells us that

$$\begin{aligned}
\alpha_1(0)(-x - y) &= \alpha_1((x + y) - x - y)(-x - y) \\
&= \alpha_1((x + y) - x)(-x)\alpha_1((x + y) - y)(-y) \\
&= \alpha_1(y)(-x)\alpha_1(x)(-y).
\end{aligned}$$

It follows that $\lambda(x \wedge y)\lambda(y \wedge x) = 1$.

Finally, we show that $\lambda((x_1+x_2)\wedge y) = \lambda(x_1\wedge y)\lambda(x_2\wedge y)$. Notice that

$$\lambda((x_1+x_2)\wedge y) = \frac{1}{\lambda(y\wedge(x_1+x_2))} = \frac{1}{\lambda(y\wedge x_1)\lambda(y\wedge x_2)} = \lambda(x_1\wedge y)\lambda(x_2\wedge y).$$

We have thus shown that λ is well defined. This shows that f is surjective and hence bijective. $\square$

3.5 Non special (C_1, C_2)

In this section we consider the case when F_1 and F_2 are codes and (C_1, C_2) is not $(F_1, F_2, \vec{s})$-special. Our goal is to show that at least linearly many coefficients $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j)$ are $\neq 1$.

Lemma 3.5.1. *Suppose $F_1 \in \mathrm{Hom}([n_1], G)$ is a translated code with distance δn_1 and image T_1, $F_2 \in \mathrm{Hom}([n_2], G)$ is a translated code with distance δn_2 and image T_2 and $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$. For $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)$, if (C_1, C_2) is not $(F_1, F_2, \vec{s})$-special, then there are at least δn_2 pairs $(i,j) \in [n_1]\times[n_2]$ for which $E'[F_1, F_2, C_1, C_2, \vec{s}] \neq 1$.*

Proof. Denote $X_2 = \mathrm{set}(F_2)$, so $\langle X_2\rangle_1 = T_2$. Assume for the sake of contradiction that there are some $C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)$, $C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)$ for which

$$1 \leq |\{(i,j) \in [n_1]\times[n_2] : E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1\}| < \delta n_2.$$

Denote

$$\sigma = \{i \in [n_1] : \exists j \in [n_2], E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \neq 1\},$$

so $1 \leq |\sigma| < \delta n_2 \leq \delta n_1$. Let $Y_1 = \{(F_1(i), s_i) : i \in [n_1]\setminus\sigma\}$ and $X_1 = \pi_1(Y_1)$. Since F_1 is a translated code of distance δn_1 with image T_1, it follows that $\langle X_1\rangle_1 = T_1$.

Denote $\tau = [n_1] \setminus \sigma$, let F_τ be the restriction of F_1 to τ and F_σ be the restriction of F_1 to σ. Also let C_τ be the restriction of C_1 to τ and C_σ be the restriction of C_1 to σ. If we restrict ourselves to $\tau \times [n_2]$ then (C_τ, C_2) is $(F_\tau, F_2, \vec{s})$-special on these indices. Therefore, by Lemma 3.4.2 there is $(\beta_1, \beta_2) \in \mathcal{D}(Y_1, X_2)$ such that $C_\tau(i) = \beta_1(F_\tau(i), s_i)$ and $C_2(j) = \beta_2(F_2(j))$.

Fix some $i_0 \in \sigma$. Consider the set

$$A = \left\{h \in X_2 : C_\sigma(i_0)(-F_\sigma(i_0) + h)\beta_2(h)(-h + F_\sigma(i_0))\zeta_p^{s_{i_0}} = 1\right\}.$$

By the definition of σ, we know that $A \subsetneq X_2$.

We know that $F_\sigma(i_0) \in T_1 = \langle X_1 \rangle_1$. Say $F_\sigma(i_0) = \sum_t a_t g_t$ for $g_t \in X_1$ and $\sum a_t = 1$. Recall that $X_1 = \pi_1(Y_1)$, so for each t, pick some $(g_t, s_t) \in Y_1$.

We claim that $\langle A \rangle_1 \cap X_2 = A$. Assume for the sake of contradiction that there is some $h \in \langle A \rangle_1 \cap X_2$, which is not in A. Since $h \in \langle A \rangle_1$, $h = \sum_k b_k h_k$ for $h_k \in A$ and $\sum b_k = 1$.

Now,

$$\begin{aligned}
C_\sigma(i_0)(-F_\sigma(i_0)+h) &= C_\sigma(i_0)\left(\sum_k b_k(-F_\sigma(i_0)+h_k)\right) \\
&= \prod_k C_\sigma(i_0)(-F_\sigma(i_0)+h_k)^{b_k} \\
&= \prod_k \left(\beta_2(h_k)(-h_k+F_\sigma(i_0))\zeta_p^{s_{i_0}}\right)^{-b_k} \\
&= \zeta_p^{-s_{i_0}} \prod_k \left(\beta_2(h_k)\left(\sum_t a_t(-h_k+g_t)\right)\right)^{-b_k} \\
&= \zeta_p^{-s_{i_0}} \prod_k \prod_t \left(\beta_2(h_k)(-h_k+g_t)\right)^{-b_k a_t} \\
&= \zeta_p^{-s_{i_0}} \prod_k \prod_t \left(\beta_1(g_t,s_t)(-g_t+h_k)\zeta_p^{s_t}\right)^{b_k a_t} \\
&= \zeta_p^{-s_{i_0}} \prod_t \left(\beta_1(g_t,s_t)\left(\sum_k b_k(-g_t+h_k)\right)\zeta_p^{s_t \sum_k b_k}\right)^{a_t} \\
&= \zeta_p^{-s_{i_0}} \prod_t \left(\beta_1(g_t,s_t)(-g_t+h)\zeta_p^{s_t}\right)^{a_t} \\
&= \zeta_p^{-s_{i_0}} \prod_t \left(\beta_2(h)(-h+g_t)\right)^{-a_t} \\
&= \zeta_p^{-s_{i_0}} \left(\beta_2(h)\left(\sum_t a_t(-h+g_t)\right)\right)^{-1} \\
&= \zeta_p^{-s_{i_0}} \left(\beta_2(h)(-h+F_\sigma(i_0))\right)^{-1}.
\end{aligned}$$

This contradicts the fact that $h \notin A$. We conclude that $\langle A \rangle_1 \cap X_2 = A$. Since $A \subsetneq X_2$, this means that $X_2 \not\subseteq \langle A \rangle_1$ and hence $\langle A \rangle_1 \neq T_2$.

Now consider

$$\sigma_2 = \{j \in [n_2] : F_2(j) \in X_2 \setminus A\}.$$

Notice that $\langle F_2(j) : j \in [n_2] \setminus \sigma_2 \rangle_1 = \langle A \rangle_1 \neq T_2$. Since F_2 is a translated code of distance δn_2 with image T_2, this implies $|\sigma_2| \geq \delta n_2$. For every $j \in \sigma_2$, $E'[F_1, F_2, C_1, C_2, \vec{s}](i_0, j) \neq 1$.

This contradicts the choice of (C_1, C_2). $\square$

3.6 Computing moments

In this section, we will prove Proposition 3.2.11, which will complete the proof of Conjecture 3.1.3 for odd p.

3.6.1 Estimation for codes

We start with the case where F_1 and F_2 are both codes. We combine the results from Section 3.3, Section 3.4 and Section 3.5 to bound the probability

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}].$$

Proposition 3.6.1. *Let p be a prime, $0 < \alpha \leq 1$, $\alpha n_1 \leq n_2 \leq n_1$, G be a finite abelian p-group and $\delta > 0$. Then there is $K > 0$, such that for sufficiently large n_1, for every pair of translated subgroups $T_1, T_2 \trianglelefteq_{tr} G$. Suppose*

- *$F_1 \in \mathrm{Hom}([n_1], G)$ is a translated code of distance δn_1 with image T_1;*
- *$F_2 \in \mathrm{Hom}([n_2], G)$ is a translated code of distance δn_2 with image T_2;*
- *$\vec{t} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}$, $F_1' \in \mathcal{C}_{n_1}(T_2, F_1)$ and $F_2' \in \mathcal{C}_{n_2}(T_1, F_2)$;*
- *For every $i \in [n_1]$ if $F_1(i) \notin T_2$, then $\chi_{T_2, F_1(i)}(F_1'(i)) = \zeta_p^{t_i}$.*

Then we have

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}] \leq \frac{K}{\left|\mathcal{C}^*_{n_1}(T_2, F_1)\right| \left|\mathcal{C}^*_{n_2}(T_1, F_2)\right| p^{n_1}} p^{|\{i \in [n_1] : F_1(i) \notin T_1 \cap T_2\}|}.$$

On the other hand, if there is some $i \in [n_1]$ for which $F_1(i) \notin T_2$ and $\chi_{T_2, F_1(i)}(F_1'(i)) \neq \zeta_p^{t_i}$,

then

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}] = 0.$$

Proof. Lemma 3.2.13 tells us that if there is some $i \in [n_1]$ for which $F_1(i) \notin T_2$ and $\chi_{T_2,F_1(i)}(F_1'(i)) \neq \zeta_p^{t_i}$, then

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}] = 0.$$

Now assume that $F_1(i) \notin T_2 \implies \chi_{T_2,F_1(i)}(F_1'(i)) = \zeta_p^{t_i}$. Equation (3.4) implies that

$$\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2') \text{ and } \eta(L_{n_1,n_2}) = \vec{t}] \\
&\leq \frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|} \frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|} \frac{1}{p^{n_1}} \sum_{C_1 \in \mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)} \sum_{C_2 \in \mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)} \sum_{\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}} \\
&\qquad \prod_{i=1}^{n_1} \prod_{j=1}^{n_2} \left| \mathbb{E}\left[\left(E'[F_1, F_2, C_1, C_2, \vec{s}](i,j) \right)^{a_{ij}} \right] \right|.
\end{aligned}$$

First, we compute the contribution of $(C_1, C_2, \vec{s})$ for which (C_1, C_2) is $(F_1, F_2, \vec{s})$-special. By Proposition 3.4.1, the number of triples $(C_1, C_2, \vec{s})$ for which (C_1, C_2) is $(F_1, F_2, \vec{s})$-special is at most

$$p^{|G|} \times |G|^{(p+1)|G|} \times p^{|\{i \in [n_1] : F_1(i) \notin T_2\}|}.$$

Thus, their combined contribution is at most

$$\frac{p^{|G|} \times |G|^{(p+1)|G|}}{\left|\mathcal{C}^*_{n_1}(T_2, F_1)\right| \left|\mathcal{C}^*_{n_2}(T_1, F_2)\right| p^{|\{i \in [n_1] : F_1(i) \in T_2\}|}}.$$

Next, we compute the contribution of triples $(C_1, C_2, \vec{s})$ for which (C_1, C_2) is not $(F_1, F_2, \vec{s})$-

special. We divide these into several cases based on a constant $\gamma > 0$ that we will pick later.

1. We compute the contribution of $(C_1, C_2, \vec{s})$ for which C_1 is $(\gamma n_1, F_1, \vec{s})$-robust. Lemma 3.3.2 tells us that for such $(\vec{s}, C_1, C_2)$, at least $\frac{\delta\gamma\alpha n_1^2}{|G|^2}$ of the coefficients $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j)$ are not 1. By Lemma 3.2.15, for each such coefficient

$$\left|\mathbb{E}\left[\left(E'[F_1, F_2, C_1, C_2, \vec{s}](i,j)\right)^{a_{ij}}\right]\right| \le \exp\left(-\frac{\epsilon}{|G|^2}\right).$$

The number of $(\vec{s}, C_1, C_2)$ is at most $p^{n_1}\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right|$. Therefore, the combined contribution of such triples is at most

$$\frac{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right| p^{n_1}}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1, F_1)\right|\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1, F_2)\right| p^{n_1}}\left(\exp\left(-\frac{\epsilon}{|G|^2}\right)\right)^{\frac{\delta\gamma\alpha n_1^2}{|G|^2}} = \exp\left(-\frac{\epsilon\delta\gamma\alpha n_1^2}{|G|^4}\right).$$

2. Next, we compute the contribution of $(\vec{s}, C_1, C_2)$ for which C_2 is $(\gamma n_2, F_2)$-robust. Lemma 3.3.2 tells us that for such $(\vec{s}, C_1, C_2)$, at least $\frac{\delta\gamma\alpha n_1^2}{p|G|^2}$ of the coefficients $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j)$ are not 1. Similarly to above, the combined contribution of such triples is at most

$$\exp\left(-\frac{\epsilon\delta\gamma\alpha n_1^2}{p\,|G|^4}\right).$$

3. Next, we compute the contribution of $(\vec{s}, C_1, C_2)$ for which $\vec{s}$ is $(\gamma n_1, F_1, T_2)$-robust. Lemma 3.3.2 tells us that for such $(\vec{s}, C_1, C_2)$, at least $\frac{\delta\gamma\alpha n_1^2}{|G|^2}$ of the coefficients $E'[F_1, F_2, C_1, C_2, \vec{s}](i,j)$ are not 1. Similarly to above, the combined contribution of such triples is at most

$$\exp\left(-\frac{\epsilon\delta\gamma\alpha n_1^2}{|G|^4}\right).$$

4. Finally, we compute the contribution of $(\vec{s}, C_1, C_2)$ for which (C_1, C_2) is not $(F_1, F_2, \vec{s})$-

special, C_1 is not $(\gamma n_1, F_1, \vec{s})$-robust, C_2 is not $(\gamma n_2, F_2)$-robust and $\vec{s}$ is not $(\gamma n_1, F_1, T_2)$-robust. Lemma 3.5.1 tells us that in this case there will be at least $\delta\alpha n_1$ many coefficients that are not 1.

Lemma 3.9.6 tells us that the number of $\vec{s}$ that are not $(\gamma n_1, F_1, T_2)$-robust is at most $p^{|G|}(4p)^{n_1\sqrt{\gamma}}p^{|\{i\in[n_1]:F_1(i)\notin T_2\}|}$. Lemma 3.9.5 tells us that the number of $C_1 \in \mathcal{C}^*_{n_1}(T, F_1)$ that are not $(\gamma n_1, F_1, \vec{s})$-robust is at most $|G|^{p|G|}(4|G|)^{n_1\sqrt{\gamma}}$. Lemma 3.9.4 tells us that the number of $C_2 \in \mathcal{C}^*_{n_2}(T, F_2)$ that are not $(\gamma n_2, F_2)$-robust is at most $|G|^{|G|}(4|G|)^{n_2\sqrt{\gamma}}$. Therefore, the combined contribution of such triples is at most

$$\frac{1}{\left|\mathcal{C}^*_{n_1}(T_2, F_1)\right| \left|\mathcal{C}^*_{n_2}(T_1, F_2)\right|} \frac{1}{p^{|\{i\in[n_1]:F_1(i)\in T_2\}|}} \left(p^{|G|}|G|^{(p+1)|G|}\right)\left(\left(64p|G|^2\right)^{\sqrt{\gamma}} \exp\left(-\frac{\epsilon\delta\alpha}{|G|^2}\right)\right)^{n_1}.$$

We choose a sufficiently small γ to ensure that

$$\left(64p|G|^2\right)^{\sqrt{\gamma}} \exp\left(-\frac{\epsilon\delta\alpha}{|G|^2}\right) < 1.$$

We fix such a γ and denote $c = -\log\left(\left(64p|G|^2\right)^{\sqrt{\gamma}} \exp\left(-\frac{\epsilon\delta\alpha}{|G|^2}\right)\right) > 0$. For sufficiently large values of n_1, we will have

$$p|G|^2 \exp\left(-\frac{\epsilon\delta\gamma\alpha n_1}{p|G|^4}\right) < \exp(-c).$$

Therefore, for sufficiently large values of n_1, the combined contribution of triples $(C_1, C_2, \vec{s})$ coming from (1), (2), (3) and (4) is at most

$$\frac{1}{\left|\mathcal{C}^*_{n_1}(T_2, F_1)\right| \left|\mathcal{C}^*_{n_2}(T_1, F_2)\right|} \frac{1}{p^{|\{i\in[n_1]:F_1(i)\in T_2\}|}} \left(3 + p^{|G|}|G|^{(p+1)|G|}\right) \exp(-cn_1).$$

We conclude that

$$\begin{aligned}&\mathbb{P}[(F_1,F_2)\circ L_{n_1,n_2}=(F_1',F_2') \text{ and } \eta(L_{n_1,n_2})=\vec{t}]\\&\le \frac{1}{\left|\mathcal{C}^*_{n_1}(T_2,F_1)\right|\left|\mathcal{C}^*_{n_2}(T_1,F_2)\right|}\frac{1}{p^{|\{i\in[n_1]:F_1(i)\in T_2\}|}}\left(p^{|G|}\left|G\right|^{(p+1)|G|}+\left(3+p^{|G|}\left|G\right|^{(p+1)|G|}\right)\exp(-cn_1)\right).\end{aligned}$$

The first part of the result follows by choosing $K=3+2\times p^{|G|}\left|G\right|^{(p+1)|G|}$. □

3.6.2 Main term

In this subsection, we fix a translated subgroup $T\trianglelefteq_{\mathrm{tr}} G$ and consider F_1 and F_2 that are translated codes with the same image T. Note that $\langle F_1\rangle_1=\langle F_2\rangle_1=T$ implies $\mathcal{C}^*_{n_1}(T,F_1)=\mathrm{Hom}([n_1],\mathcal{G}(T)^*)$ and $\mathcal{C}^*_{n_2}(T,F_2)=\mathrm{Hom}([n_2],\mathcal{G}(T)^*)$.

Proposition 3.6.2. *Let p be a prime, $0<\alpha\le 1$, $\alpha n_1\le n_2\le n_1$, G be a finite abelian p-group and $\delta>0$. Then there are $c>0$ and $K_1>0$, such that for sufficiently large n_1, for every translated subgroup $T\trianglelefteq_{tr} G$, if $F_1\in\mathrm{Hom}([n_1],G)$ is a translated code of distance δn_1 with image T, $F_2\in\mathrm{Hom}([n_2],G)$ is a translated code of distance δn_2 with image T such that $\mathrm{set}(F_1)=\mathrm{set}(F_2)=T$ and $\vec{t}\in(\mathbb{Z}/p\mathbb{Z})^{n_1}$, then we have*

$$\left|\mathbb{P}[(F_1,F_2)\circ L_{n_1,n_2}=0,\eta(L_{n_1,n_2})=\vec{t}]-\frac{|\Delta^2(\mathcal{G}(T))|}{\left|T\right|^{n_1+n_2-1}p^{n_1}}\right|\le\frac{K_1\exp(-cn_1)}{\left|T\right|^{n_1+n_2}p^{n_1}}.$$

Proof. The proof of Proposition 3.6.1 tells us that

$$\begin{aligned}&\mathbb{P}[(F_1,F_2)\circ L_{n_1,n_2}=0,\eta(L_{n_1,n_2})=\vec{t}]\\&=\frac{1}{\left|T\right|^{n_1+n_2}}\frac{1}{p^{n_1}}\sum_{\substack{C_1\in\mathcal{C}^*_{n_1}(T,F_1)\\C_2\in\mathcal{C}^*_{n_2}(t,F_2)\\\vec{s}\in(\mathbb{Z}/p\mathbb{Z})^{n_1}\\(C_1,C_2)\text{ is }(F_1,F_2,\vec{s})-\text{special}}}\zeta_p^{-\vec{s}\cdot\vec{t}}+\text{error term},\end{aligned}$$

with

$$|\text{error term}| \le \frac{1}{|T|^{n_1+n_2}} \frac{1}{p^{n_1}} \left(3 + p^{|G|} \, |G|^{(p+1)|G|}\right) \exp(-cn_1).$$

We are given that $\operatorname{set}(F_1) = \operatorname{set}(F_2) = T$. We compute the contribution of $(C_1, C_2, \vec{s})$ for which (C_1, C_2) is $(F_1, F_2, \vec{s})$-special. Proposition 3.4.1 tells us that if $\vec{s} \neq 0$, then there are no pairs (C_1, C_2) that are $(F_1, F_2, \vec{s})$-special. On the other hand, for $\vec{s} = 0$, the number of pairs (C_1, C_2) that are $(F_1, F_2, \vec{s})$-special is $|\Delta^2 \mathcal{G}(T)| \times |T|$. The result follows. □

Corollary 3.6.3. *Let p be a prime, $0 < \alpha \le 1$, $\rho, \delta > 0$ and G be a finite abelian p-group. Consider a translated subgroup $T \trianglelefteq_{tr} G$. We have*

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(T,T)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)} \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)|.$$

Proof. Note that

$$\begin{aligned}
&\left| \left(\sum_{F_1 \in \mathcal{S}_{n,\delta}(T,T)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)} \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \right) - \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)| \right| \\
&\le \sum_{F_1 \in \mathcal{S}_{n,\delta}(T,T)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)} \sum_{\vec{t} \in \mathcal{E}_{n,\rho}} \left| \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] - \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right| \\
&\quad + \left| |\mathcal{S}_{n,\delta}(T,T)| \times \left|\mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)\right| \times |\mathcal{E}_{n,\rho}| \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^{n_1}} - \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)| \right|.
\end{aligned}$$

For the second term note that

$$\begin{aligned}
&\left| |\mathcal{S}_{n,\delta}(T,T)| \times \left|\mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)\right| \times |\mathcal{E}_{n,\rho}| \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n_1+n_2-1} p^{n_1}} - \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)| \right| \\
&= \left|\Delta^2 \mathcal{G}(T)\right| \times |\mathcal{G}(T)| \left| \frac{|\mathcal{S}_{n,\delta}(T,T)| \times \left|\mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)\right| \times |\mathcal{E}_{n,\rho}|}{|T|^{n+\lceil \alpha n \rceil} p^n} - 1 \right|.
\end{aligned}$$

By Lemma 3.9.3 and Lemma 3.9.7, this goes to 0 as $n \to \infty$.

Next, Proposition 3.6.2 tells us that

$$\begin{aligned}
&\sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T,T) \\ \mathrm{set}(F_1)=T}} \sum_{\substack{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T) \\ \mathrm{set}(F_2)=T}} \sum_{\vec{t} \in \mathcal{E}_{n,\rho}} \left| \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] - \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right| \\
&\leq |\mathcal{S}_{n,\delta}(T,T)| \times \left|\mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T)\right| \times |\mathcal{E}_{n,\rho}| \times \frac{K_1 \exp(-c(n + \lceil \alpha n \rceil))}{|T|^{n+\lceil \alpha n \rceil} p^n} \\
&\leq K_1 \exp(-c(n)).
\end{aligned}$$

Finally, consider subsets $X_1, X_2 \subseteq T$. Proposition 3.6.1 tells us that

$$\begin{aligned}
&\sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T,T) \\ \mathrm{set}(F_1)=X_1}} \sum_{\substack{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T) \\ \mathrm{set}(F_2)=X_2}} \sum_{\vec{t} \in \mathcal{E}_{n,\rho}} \left| \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] - \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right| \\
&\leq \sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T,T) \\ \mathrm{set}(F_1)=X_1}} \sum_{\substack{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T) \\ \mathrm{set}(F_2)=X_2}} \sum_{\vec{t} \in \mathcal{E}_{n,\rho}} \left(\mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] + \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right) \\
&\leq \sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T,T) \\ \mathrm{set}(F_1)=X_1}} \sum_{\substack{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T,T) \\ \mathrm{set}(F_2)=X_2}} \sum_{\vec{t} \in \mathcal{E}_{n,\rho}} \left(\frac{K}{|T|^{n+\lceil \alpha n \rceil} p^n} + \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right) \\
&\leq \left(\frac{K}{|T|^{n+\lceil \alpha n \rceil} p^n} + \frac{|\Delta^2 \mathcal{G}(T)|}{|T|^{n+\lceil \alpha n \rceil - 1} p^n} \right) \times |X_1|^n \times |X_2|^{\lceil \alpha n \rceil} \times p^n \\
&= \left(K + \left|\Delta^2 \mathcal{G}(T)\right| \times |T|\right) \times \left(\frac{|X_1|}{|T|} \right)^n \times \left(\frac{|X_2|}{|T|} \right)^{\lceil \alpha n \rceil}.
\end{aligned}$$

If $X_1 \subsetneq T$ or $X_2 \subsetneq T$, then this limit will be 0. The result follows. □

3.6.3 Error term, Type 1

In this subsection, we fix chains of translated subgroups $T_1 \trianglelefteq_{\mathrm{tr}} S_1 \trianglelefteq_{\mathrm{tr}} G$ and $T_2 \trianglelefteq_{\mathrm{tr}} S_2 \trianglelefteq_{\mathrm{tr}} G$ such that T_1, T_2, S_1 and S_2 are not all the same and $|T_1| \leq |T_2|$.

Lemma 3.6.4. *Let p be a prime, $0 < \alpha \leq 1$, $\alpha n_1 \leq n_2 \leq n_1$, G be a finite abelian p-group and $\delta > 0$. Then is a constant $K > 0$, such that for sufficiently large n_1, if*

1. *$F_1 \in \operatorname{Hom}([n_1], G)$ is a translated code of distance δn_1 with image T_1;*

2. *$F_2 \in \operatorname{Hom}([n_2], G)$ is a translated code of distance δn_2 with image T_2;*

3. *$F_1' \in \mathcal{C}_{n_1}(T_2, F_1)$ and $F_2' \in \mathcal{C}_{n_2}(T_1, F_2)$,*

then we have

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2')] \leq \frac{K}{|\mathcal{C}_{n_1}(T_2, F_1)| \times |\mathcal{C}_{n_2}(T_1, F_2)|}.$$

Proof. Note that

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2')] = \sum_{\vec{t} \in (\mathbb{Z}/p\mathbb{Z})^{n_1}} \mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}].$$

Let $A_1 = \{i \in [n_1] : F_1(i) \in T_2\}$ and $A_2 = \{i \in [n_1] : F_1(i) \in T_1 \setminus T_2\}$. Proposition 3.6.1 tells us that if there is some $i \in A_2$ for which $\chi_{T_2, F_1(i)}(F_1'(i)) \neq \zeta_p^{t_i}$, then

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}] = 0.$$

Let B be the set of vectors in $(\mathbb{Z}/p\mathbb{Z})^{n_1}$ for which each $i \in A_2$, we have $\chi_{T_2, F_1(i)}(F_1'(i)) = \zeta_p^{t_i}$. Clearly $|B| = p^{|A_1|}$.

Moreover, Proposition 3.6.1 tells us that for each $\vec{t} \in B$,

$$\mathbb{P}[(F_1, F_2) \circ L_{n_1,n_2} = (F_1', F_2'), \eta(L_{n_1,n_2}) = \vec{t}] \leq \frac{K}{\left|\mathcal{C}^*_{n_1}(T_2, F_1)\right| \left|\mathcal{C}^*_{n_2}(T_1, F_2)\right| p^{A_1}}.$$

The result follows. $\square$

Proposition 3.6.5. *Let p be a prime, $0 < \alpha \leq 1$, $\rho > 0$, G be a finite abelian p-group. Suppose we have chains of translated subgroups $T_1 \trianglelefteq_{tr} S_1 \trianglelefteq_{tr} G$ and $T_2 \trianglelefteq_{tr} S_2 \trianglelefteq_{tr} G$. If*

1. *T_1, T_2, S_1, S_2 are not all the same;*

2. *$|T_1| \leq |T_2|$,*

then for sufficiently small $\delta > 0$, we have

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T_2,S_2)} \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 0.$$

Proof. We will show that

$$\lim_{n\to\infty} \sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T_2,S_2)} \mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0] = 0,$$

this will clearly imply the result.

Denote $D_1 = [S_1 : T_1]$ and $D_2 = [S_2 : T_2]$. Further, denote

$$e_1 = \begin{cases} 1 - \epsilon & \text{if } D_1 > 1 \text{ and } T_2 \subseteq T_1 \\ 1 & \text{otherwise} \end{cases}, \qquad e_2 = \begin{cases} 1 - \epsilon & \text{if } D_2 > 1 \text{ and } T_1 \subseteq T_2 \\ 1 & \text{otherwise} \end{cases}.$$

Consider $F_1 \in \mathcal{S}_{n,\delta}(T_1, S_1)$ and $F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T_2, S_2)$. Denote

$$\sigma_1 = \{i \in [n] : F_1(i) \notin T_1\}, \qquad \tau_1 = [n] \setminus \sigma_1,$$
$$\sigma_2 = \{j \in [\lceil \alpha n \rceil] : F_2(j) \notin T_2\}, \qquad \tau_2 = [\lceil \alpha n \rceil] \setminus \sigma_2.$$

We know that $|\sigma_1| < \delta \log_p(D_1) n$ and $|\sigma_2| < \delta \log_p(D_2) \lceil \alpha n \rceil$. Moreover, if $D_1 > 1$, then $\sigma_1 \neq \emptyset$ and if $D_2 > 1$, then $\sigma_2 \neq \emptyset$. Let F_{τ_1} be the restriction of F_1 to τ_1, F_{σ_1} be the restriction of F_1 to σ_1, F_{τ_2} be the restriction of F_2 to τ_2 and F_{σ_2} be the restriction of F_2

to σ_2. We know that $F_{\tau_1} : \tau_1 \to T_1$ is a translated code of distance δn with image T_1 and $F_{\tau_2} : \tau_2 \to T_2$ is a translated code of distance $\delta\alpha n$ with image T_2.

If $Z_1 \subseteq [n]$ and $Z_2 \subseteq [\lceil \alpha n \rceil]$, then we denote:

- A_{Z_1,Z_2} is $|Z_1| \times |Z_2|$ matrix whose entries are a_{ij} for $i \in Z_1$ and $j \in Z_2$.
- B_{Z_1,Z_2} is $|Z_1| \times |Z_1|$ diagonal matrix, whose diagonal entries are $-\sum_{j \in Z_2} a_{ij}$ for $i \in Z_1$.
- C_{Z_1,Z_2} is a $|Z_2| \times |Z_2|$ diagonal matrix, whose diagonal entries are $-\sum_{i \in Z_1} a_{ij}$ for $j \in Z_2$.

Therefore, $L_n^{(\alpha)}$ has the block structure

$$L_n^{(\alpha)} = \begin{bmatrix} B_{\tau_1,\tau_2} + B_{\tau_1,\sigma_2} & 0 & A_{\tau_1,\tau_2} & A_{\tau_1,\sigma_2} \\ 0 & B_{\sigma_1,\tau_2} + B_{\sigma_1,\sigma_2} & A_{\sigma_1,\tau_2} & A_{\sigma_1,\sigma_2} \\ A^T_{\tau_1,\tau_2} & A^T_{\sigma_1,\tau_2} & C_{\tau_1,\tau_2} + C_{\sigma_1,\tau_2} & 0 \\ A^T_{\tau_1,\sigma_2} & A^T_{\sigma_1,\sigma_2} & 0 & C_{\tau_1,\sigma_2} + C_{\sigma_1,\sigma_2} \end{bmatrix}.$$

Denote the restriction of F_1 to τ_1 as F_{τ_1} and the restriction to σ_1 as F_{σ_1}. Similarly denote the restriction of F_2 to τ_2 as F_{τ_2} and the restriction to σ_2 as F_{σ_2}. We construct the matrix $L_n^{(\alpha)}(\tau_1, \tau_2)$ as

$$L_n^{(\alpha)}(\tau_1, \tau_2) = \begin{bmatrix} B_{\tau_1,\tau_2} & A_{\tau_1,\tau_2} \\ A^T_{\tau_1,\tau_2} & C_{\tau_1,\tau_2} \end{bmatrix}.$$

Note that if $(F_1, F_2) \circ L_n^{(\alpha)} = 0$, then

$$(F_{\tau_1}, F_{\tau_2}) \circ (L_n^{(\alpha)}(\tau_1, \tau_2)) = (-F_{\tau_1} \circ B_{\tau_1,\sigma_2} - F_{\sigma_2} \circ A^T_{\tau_1,\sigma_2}, -F_{\sigma_1} \circ A_{\sigma_1,\tau_2} - F_{\tau_2} \circ C_{\sigma_1,\tau_2}).$$

We denote

$$F_1' = -F_{\tau_1} \circ B_{\tau_1,\sigma_2} - F_{\sigma_2} \circ A^T_{\tau_1,\sigma_2} \in \mathrm{Hom}(\tau_1, G),$$
$$F_2' = -F_{\sigma_1} \circ A_{\sigma_1,\tau_2} - F_{\tau_2} \circ C_{\sigma_1,\tau_2} \in \mathrm{Hom}(\tau_2, G).$$

The important thing to note here is that F_1', F_2' and $L_n^{(\alpha)}(\tau_1, \tau_2)$ are independent. Therefore, by Lemma 3.6.4

$$\mathbb{P}\Big[(F_{\tau_1}, F_{\tau_2})(L_n^{(\alpha)}(\tau_1, \tau_2)) = (F_1', F_2') \mid F_1' \in \mathcal{C}_{\tau_1}(T_2, F_{\tau_1}), F_2' \in \mathcal{C}_{\tau_2}(T_1, F_{\tau_2})\Big]$$
$$\leq \frac{K}{|\mathcal{C}_{\tau_1}(T_2, F_{\tau_1})| \times |\mathcal{C}_{\tau_2}(T_1, F_{\tau_2})|}.$$

Next, we bound the probability that $F_1' \in \mathcal{C}_{\tau_1}(T_2, F_{\tau_1})$ and $F_2' \in \mathcal{C}_{\tau_2}(T_1, F_{\tau_2})$.

- Consider the case when $e_2 = 1 - \epsilon$, that is $D_2 > 1$ and $T_1 \subseteq T_2$. For $i \in \tau_1$,

  $$F_1'(i) = \sum_{j \in \sigma_2} a_{ij}(F_{\sigma_2}(j) - F_{\tau_1}(i)).$$

  By the definition of τ_1 and σ_2, we know that $F_{\sigma_2}(j) \notin T_2$ and $F_{\tau_1}(i) \in T_1 \subseteq T_2$. This means that $\langle -F_{\tau_1}(i) + T_2 \rangle = \mathcal{G}(T_2)$ and $-F_{\tau_1}(i) + F_{\sigma_2}(j) \notin \mathcal{G}(T_2)$. Since $\sigma_2 \neq \emptyset$ and a_{ij} are ϵ-balanced, the probability of $F_1'(i) \in \mathcal{G}(T_2)$ is at most $1 - \epsilon$.

- Similarly in the case when $e_1 = 1 - \epsilon$, the probability of $F_2'(j) \in \langle -F_{\tau_2}(j) + T_1 \rangle$ is at most $1 - \epsilon$.

- Each of these conditions are independent and hence

  $$\mathbb{P}\Big[F_1' \in \mathcal{C}_{\tau_1}(T_2, F_{\tau_1}) \text{ and } F_2' \in \mathcal{C}_{\tau_2}(T_1, F_{\tau_2})\Big] \leq e_1^{|\tau_1|} e_2^{|\tau_2|}.$$

We conclude that

$$\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0]\le e_1^{|\tau_1|}e_2^{|\tau_2|}\times\frac{K}{|\mathcal{C}_{\tau_1}(T_2,F_{\tau_1})|\times|\mathcal{C}_{\tau_2}(T_1,F_{\tau_2})|}.$$

Next, we sum over different F_1 and F_2 corresponding to a fixed choice of τ_1, τ_2

$$\begin{aligned}
&\sum_{\substack{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)\\F_1(\tau_1)\subseteq T_1}}\sum_{\substack{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)\\F_2(\tau_2)\subseteq T_2}}\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0,\eta(L_n^{(\alpha)})\in\mathcal{E}_{n,\rho}]\\
&\le\sum_{\substack{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)\\F_1(\tau_1)\subseteq T_1}}\sum_{\substack{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)\\F_2(\tau_2)\subseteq T_2}}\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0]\\
&\le Ke_1^{|\tau_1|}e_2^{|\tau_2|}\sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)}\sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)}\prod_{i\in\tau_1}\frac{1}{|\langle -F_1(i)+T_2\rangle|}\prod_{j\in\tau_2}\frac{1}{|\langle -F_2(j)+T_1\rangle|}\\
&\le Ke_1^{|\tau_1|}e_2^{|\tau_2|}\,|G|^{|\sigma_1|+|\sigma_2|}\left(\sum_{g\in T_1}\frac{1}{|\langle -g+T_2\rangle|}\right)^{|\tau_1|}\left(\sum_{h\in T_2}\frac{1}{|\langle -h+T_1\rangle|}\right)^{|\tau_2|}.
\end{aligned}$$

Note that $\sum_{g\in T_1}\frac{1}{|\langle -g+T_2\rangle|}\ge\frac{1}{|G|}$ and $\sum_{h\in T_2}\frac{1}{|\langle -h+T_1\rangle|}\ge\frac{1}{|G|}$. Therefore,

$$\begin{aligned}
&\sum_{\substack{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)\\F_1(\tau_1)\subseteq T_1}}\sum_{\substack{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)\\F_2(\tau_2)\subseteq T_2}}\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0,\eta(L_n^{(\alpha)})\in\mathcal{E}_{n,\rho}]\\
&\le K\left(\frac{|G|^2}{1-\epsilon}\right)^{|\sigma_1|}\left(\frac{|G|^2}{1-\epsilon}\right)^{|\sigma_2|}e_1^ne_2^{\alpha n}\left(\sum_{g\in T_1}\frac{1}{|\langle -g+T_2\rangle|}\right)^{n}\left(\sum_{h\in T_2}\frac{1}{|\langle -h+T_1\rangle|}\right)^{\alpha n}\\
&\le K\left(\left(\left(\frac{|G|^2}{1-\epsilon}\right)^{\log_p(D_1)+\alpha\log_p(D_2)}\right)^{\delta}e_1e_2^{\alpha}\left(\sum_{g\in T_1}\frac{1}{|\langle -g+T_2\rangle|}\right)\left(\sum_{h\in T_2}\frac{1}{|\langle -h+T_1\rangle|}\right)^{\alpha}\right)^{n}.
\end{aligned}$$

Moreover, the number of choices for σ_1 is at most

$$\sum_{k\le\log_p(D_1)\delta n}\binom{n}{k}\le\exp\left(2\sqrt{\log_p(D_1)\delta n}\right),$$

and the number of choices for σ_2 is at most

$$\sum_{k \le \log_p(D_2)\delta\alpha n} \binom{\alpha n}{k} \le \exp\left(2\sqrt{\log_p(D_2)\delta}\alpha n\right).$$

We conclude that

$$\begin{aligned}&\sum_{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)} \sum_{F_2 \in \mathcal{S}_{\lceil \alpha n \rceil,\delta}(T_2,S_2)} \mathbb{P}[(F_1,F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] \\ &\le K\left(\left(\left(\frac{|G|^2}{1-\epsilon}\right)^{2\log_p(|G|)} \exp\left(4\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}} e_1 e_2^\alpha \left(\sum_{g \in T_1} \frac{1}{|\langle -g + T_2 \rangle|}\right)\left(\sum_{h \in T_2} \frac{1}{|\langle -h + T_1 \rangle|}\right)^\alpha\right)^n.\end{aligned}$$

We know that $e_1 \le 1$ and $e_2 \le 1$. Since $|T_1| \le |T_2|$, we see that

$$\begin{aligned}\left(\sum_{g \in T_1} \frac{1}{|\langle -g + T_2 \rangle|}\right)\left(\sum_{h \in T_2} \frac{1}{|\langle -h + T_1 \rangle|}\right)^\alpha &\le \left(\sum_{g \in T_1} \frac{1}{|T_2|}\right)\left(\sum_{h \in T_2} \frac{1}{|T_1|}\right)^\alpha \\ &= \frac{|T_1|}{|T_2|}\left(\frac{|T_2|}{|T_1|}\right)^\alpha \le 1.\end{aligned} \tag{3.7}$$

This means that

$$e_1 e_2^\alpha \left(\sum_{g \in T_1} \frac{1}{|\langle -g + T_2 \rangle|}\right)\left(\sum_{h \in T_2} \frac{1}{|\langle -h + T_1 \rangle|}\right)^\alpha \le 1. \tag{3.8}$$

If the inequality in (3.7) was strict, then the inequality in (3.8) will also be strict. On the other hand, if equality holds in (3.7), then for every $T_1 \subseteq T_2$ and $T_2 \subseteq T_1$, hence $T_1 = T_2$. This would mean that either $T_1 \subsetneq S_1$ or $T_2 \subsetneq S_2$. Thus, either $e_1 < 1$ or $e_2 < 1$. In either case, the inequality in (3.8) is strict.

Therefore, we can pick a sufficiently small δ to ensure

$$\left(\left(\frac{|G|^2}{1-\epsilon}\right)^{2\log_p(|G|)} \exp\left(4\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}} e_1 e_2^{\alpha} \left(\sum_{g\in T_1} \frac{1}{|\langle -g+T_2\rangle|}\right)\left(\sum_{h\in T_2} \frac{1}{|\langle -h+T_1\rangle|}\right)^{\alpha} < 1.$$

This completes the proof. □

3.6.4 Error term, Type 2

In this subsection, we fix chains of translated subgroups $T_1 \trianglelefteq_{\mathrm{tr}} S_1 \trianglelefteq_{\mathrm{tr}} G$ and $T_2 \trianglelefteq_{\mathrm{tr}} S_2 \trianglelefteq_{\mathrm{tr}} G$ such that $|T_1| > |T_2|$. This is the first time that we will use the assumption that a_{ij} are identically distributed.

Given $g \in G$ and $F_2 \in \mathcal{S}_{\lceil \alpha n\rceil,\delta}(T_2, S_2)$, let $\sigma_2 = \{j \in [n_2] : F_2(j) \notin T_2\}$. We denote

$$\nu_{F_2}(g) = \mathbb{P}\left[\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \in \langle -g+T_2\rangle\right].$$

For $g \in G \setminus T_2$ and $l \in \mathbb{Z}/p\mathbb{Z}$, we denote

$$\begin{aligned}&\nu_{F_2}(g,l)\\ &= \mathbb{P}\left[\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \in \langle -g+T_2\rangle \text{ and } \chi_{T_2,g}\Big(-\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j))\Big)\zeta_p^{\sum_{j\in\sigma_2} a_{1j}} = \zeta_p^l\right].\end{aligned}$$

Lemma 3.6.6. *Consider $F_2 \in \mathcal{S}_{\lceil \alpha n\rceil,\delta}(T_2, S_2)$ and $l \in \mathbb{Z}/p\mathbb{Z}$. If $l \neq 0$, then*

$$\sum_{g\in T_1\cap T_2} \frac{\nu_{F_2}(g)}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p\nu_{F_2}(g,l)}{|\langle -g+T_2\rangle|} \le 1.$$

Proof. For each $h \in T_2$, let $b_h \in \mathbb{Z}_p$ be a Haar-uniform random variable such that the b_h and

a_{ij} are independent. Note that

$$\sum_{g\in T_1}\mathbb{P}\left[\sum_{h\in T_2} b_h(-g+h)+\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j))=0 \mid \sum_{h\in T_2} b_h+\sum_{j\in\sigma_2} a_{1j}\equiv l \pmod p\right]$$
$$=\sum_{g\in T_1}\mathbb{P}\left[\sum_{h\in T_2} b_h(h)+\sum_{j\in\sigma_2} a_{1j}(-F_2(j))=lg \mid \sum_{h\in T_2} b_h+\sum_{j\in\sigma_2} a_{1j}\equiv l \pmod p\right]\leq 1.$$

Also note that

$$\sum_{g\in T_1}\mathbb{P}\left[\sum_{h\in T_2} b_h(-g+h)+\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j))=0 \mid \sum_{h\in T_2} b_h+\sum_{j\in\sigma_2} a_{1j}\equiv l \pmod p\right]$$
$$=\sum_{g\in T_1}\mathbb{P}\left[\sum_{h\in T_2} b_h(-g+h)=-\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \mid \sum_{h\in T_2} b_h\equiv l-\sum_{j\in\sigma_2} a_{1j} \pmod p\right]$$

We break into cases based on $g\in T_1\cap T_2$ or $g\in T_1\setminus T_2$.

1. Case 1: $g\in T_1\cap T_2$. If $\sum_{h\in T_2} b_h\equiv k \pmod p$, then $\sum_{h\in T_2} b_h(-g+h)$ is a uniformly random element of $\langle -g+T_2\rangle=\mathcal{G}(T_2)$. Therefore,

$$\mathbb{P}\left[\sum_{h\in T_2} b_h(-g+h)=-\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \mid \sum_{h\in T_2} b_h\equiv l-\sum_{j\in\sigma_2} a_{1j} \pmod p\right]$$
$$=\frac{1}{|T_2|}\mathbb{P}\left[\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j))\in\mathcal{G}(T_2)\right]=\frac{1}{|T_2|}\nu_{F_2}(g).$$

2. Case 2: $g\in T_1\setminus T_2$. If $\sum_{h\in T_2} b_h\equiv k \pmod p$, then $\sum_{h\in T_2} b_h(-g+h)$ is a uniformly random element of

$$\left\{x\in\langle -g+T_2\rangle : \chi_{T_2,g}(x)=\zeta_p^k\right\}.$$

The size of this set is $\frac{|\langle -g+T_2\rangle|}{p}$. Therefore,

$$\mathbb{P}\left[\sum_{h\in T_2} b_h(-g+h) = -\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \mid \sum_{h\in T_2} b_h \equiv l - \sum_{j\in\sigma_2} a_{1j} \pmod p\right]$$
$$= \frac{p}{|\langle -g+T_2\rangle|}\mathbb{P}\left[\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j)) \in \langle -g+T_2\rangle\,, \chi_{T_2,g}\Big(-\sum_{j\in\sigma_2} a_{1j}(-g+F_2(j))\Big) = \zeta_p^{l-\sum_{j\in\sigma_2} a_{1j}}\right]$$
$$= \frac{p}{|\langle -g+T_2\rangle|}\nu_{F_2}(g,l).$$

The result follows. □

Proposition 3.6.7. *Let p be a prime, $\frac{1}{p} < \alpha \le 1$, $0 < \rho < \alpha - \frac{1}{p}$, G be a finite abelian p-group. Suppose we have chains of translated subgroups $T_1 \trianglelefteq_{tr} S_1 \trianglelefteq_{tr} G$ and $T_2 \trianglelefteq_{tr} S_2 \trianglelefteq_{tr} G$. If $|T_1| > |T_2|$, then for sufficiently small $\delta > 0$, we have*

$$\lim_{n\to\infty} \sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 0.$$

Proof. Let D_1, D_2, σ_1, σ_2, τ_1, τ_2 be as in the proof of Proposition 3.6.5. Define F_{τ_1}, F_{τ_2}, block matrix $L_{n_1,n_2}(\tau_1,\tau_2)$ and $F_1' \in \mathrm{Hom}(\tau_1, G)$, $F_2' \in \mathrm{Hom}(\tau_2, G)$ in the same way as in the proof of Proposition 3.6.5. Recall that F_1', F_2' and $L_n^{(\alpha)}(\tau_1,\tau_2)$ are independent. Also recall that if $(F_1,F_2)\circ L_n^{(\alpha)} = 0$, then $(F_{\tau_1},F_{\tau_2})\circ L_n^{(\alpha)}(\tau_1,\tau_2) = (F_1',F_2')$.

Pick $\vec{t} \in \mathcal{E}_{n,\rho}$. Let $\vec{u} \in (\mathbb{Z}/p\mathbb{Z})^{\tau_1}$ be the vector whose entries are $u_i = t_i - \sum_{j\in\sigma_2} a_{ij}$ for $i \in \tau_1$. This is a random vector, but it is independent of $L_n^{(\alpha)}(\tau_1,\tau_2)$. Note that

$$\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] \le \mathbb{P}[(F_{\tau_1},F_{\tau_2})\circ(L_n^{(\alpha)}(\tau_1,\tau_2)) = (F_1',F_2'), \eta(L_n^{(\alpha)}(\tau_1,\tau_2)) = \vec{u}].$$

This probability is zero unless the following conditions hold.

1. For each $i \in \tau_1$, $F_1'(i) \in \langle -F_1(i) + T_2\rangle$.

2. For each $j \in \tau_2$, $F_2'(j) \in \langle -F_2(j) + T_1 \rangle$.

3. For each $i \in \tau_1$, if $F_{\tau_1}(i) \notin T_2$, then $\chi_{T_2,F_1(i)}(F_1'(i)) = \zeta_p^{u_i}$.

Note that

$$F_1'(i) = -\sum_{j\in\sigma_2} a_{ij}(-F_1(i) + F_2(j)).$$

Since all a_{ij} are independent and identically distributed, the probability for conditions (1), (3) to hold is

$$\prod_{\substack{i\in\tau_1\\ F_1(i)\in T_2}} \nu_{F_2}(F_1(i)) \prod_{\substack{i\in\tau_1\\ F_1(i)\notin T_2}} \nu_{F_2}(F_1(i), t_i).$$

The probability for condition (2) to hold is at most 1. Proposition 3.6.1 tells us that

$$\begin{aligned}
&\mathbb{P}[(F_{\tau_1}, F_{\tau_2}) \circ (L_n^{(\alpha)}(\tau_1, \tau_2)) = (F_1' F_2'), \eta(L_n^{(\alpha)}(\tau_1, \tau_2)) = \vec{u}] \\
&= \mathbb{P}[(F_{\tau_1}, F_{\tau_2}) \circ (L_n^{(\alpha)}(\tau_1, \tau_2)) = (F_1', F_2'), \eta(L_n^{(\alpha)}(\tau_1, \tau_2)) = \vec{u} \mid (1), (2), (3)] \times \mathbb{P}[(1), (2), (3)] \\
&\le \frac{K}{\left|\mathcal{C}^*_{|\tau_1|}(T_2, F_{\tau_1})\right| \left|\mathcal{C}^*_{|\tau_2|}(T_1, F_{\tau_2})\right| p^{|\tau_1|}} p^{|\{i\in\tau_1 : F_1(i)\notin T_2\}|} \prod_{\substack{i\in\tau_1\\ F_1(i)\in T_2}} \nu_{F_2}(F_1(i)) \prod_{\substack{i\in\tau_1\\ F_1(i)\notin T_2}} \nu_{F_2}(F_1(i), t_i) \\
&= \frac{K}{p^{|\tau_1|}} \prod_{\substack{i\in\tau_1\\ F_1(i)\in T_2}} \frac{\nu_{F_2}(F_1(i))}{|\langle -F_1(i) + T_2 \rangle|} \prod_{\substack{i\in\tau_1\\ F_1(i)\notin T_2}} \frac{p\nu_{F_2}(F_1(i), t_i)}{|\langle -F_1(i) + T_2 \rangle|} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j) + T_1 \rangle|}.
\end{aligned}$$

Note that if $F_1(i) \in T_2$, then $|\langle -F_1(i) + T_2 \rangle| = |T_2|$. Therefore,

$$\begin{aligned}
&\mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}] \\
&\le \frac{K}{p^{|\tau_1|}} \prod_{\substack{i\in\tau_1\\ F_1(i)\in T_2}} \frac{\nu_{F_2}(F_1(i))}{|T_2|} \prod_{\substack{i\in\tau_1\\ F_1(i)\notin T_2}} \frac{p\nu_{F_2}(F_1(i), t_i)}{|\langle -F_1(i) + T_2 \rangle|} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j) + T_1 \rangle|}.
\end{aligned}$$

If we sum over different F_1 corresponding to the same τ_1, we see that

$$\begin{aligned}
&\sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)\\ F_1(\tau_1)\subseteq T_1}} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}]\\
&\le \frac{K}{p^{|\tau_1|}} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j)+T_1\rangle|} |S_1|^{|\sigma_1|} \prod_{i\in\tau_1} \left(\sum_{g\in T_1\cap T_2} \frac{\nu_{F_2}(g)}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p\nu_{F_2}(g,t_i)}{|\langle -g+T_2\rangle|} \right)\\
&= \frac{K}{p^n} (p\,|G|)^{|\sigma_1|} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j)+T_1\rangle|} \prod_{l\in\mathbb{Z}/p\mathbb{Z}} \left(\sum_{g\in T_1\cap T_2} \frac{\nu_{F_2}(g)}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p\nu_{F_2}(g,l)}{|\langle -g+T_2\rangle|} \right)^{|\{i\in\tau_1 : t_i = l\}|}.
\end{aligned}$$

By Lemma 3.6.6, we see that

$$\begin{aligned}
&\sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)\\ F_1(\tau_1)\subseteq T_1}} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}]\\
&\le \frac{K}{p^n} (p\,|G|)^{\log_p(D_1)\delta n} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j)+T_1\rangle|} \left(\sum_{g\in T_1\cap T_2} \frac{\nu_{F_2}(g)}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p\nu_{F_2}(g,0)}{|\langle -g+T_2\rangle|} \right)^{|\{i\in\tau_1 : t_i = 0\}|}.
\end{aligned}$$

If $g \notin T_2$, then $\langle -g+T_2\rangle \supsetneq \mathcal{G}(T_2)$, hence $|\langle -g+T_2\rangle| \ge p\times|T_2|$. This implies that

$$\sum_{g\in T_1\cap T_2} \frac{\nu_{F_2}(g)}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p\nu_{F_2}(g,0)}{|\langle -g+T_2\rangle|} \le \sum_{g\in T_1\cap T_2} \frac{1}{|T_2|} + \sum_{g\in T_1\setminus T_2} \frac{p}{p\,|T_2|} = \frac{|T_1|}{|T_2|}.$$

We see that

$$\begin{aligned}
&\sum_{\substack{F_1 \in \mathcal{S}_{n,\delta}(T_1,S_1)\\ F_1(\tau_1)\subseteq T_1}} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)} = 0, \eta(L_n^{(\alpha)}) = \vec{t}]\\
&\le \frac{K}{p^n} (p\,|G|)^{\log_p(D_1)\delta n} \prod_{j\in\tau_2} \frac{1}{|\langle -F_2(j)+T_1\rangle|} \left(\frac{|T_1|}{|T_2|}\right)^{|\{i\in\tau_1 : t_i = 0\}|}.
\end{aligned}$$

Since $|T_1| > |T_2|$ and $\vec{t}\in\mathcal{E}_{n,\rho}$, we know that

$$\left(\frac{|T_1|}{|T_2|}\right)^{|\{i\in\tau_1 : t_i = 0\}|} \le \left(\frac{|T_1|}{|T_2|}\right)^{|\{i\in[n_1] : t_i = 0\}|} \le \left(\frac{|T_1|}{|T_2|}\right)^{(\frac{1}{p}+\rho)n}.$$

The number of choices for τ_1 is at most

$$\sum_{k\leq \log_p(D_1)\delta n} \binom{n}{k} \leq \exp\left(2\sqrt{\log_p(D_1)\delta n}\right) \leq \exp\left(2\sqrt{\log_p(|G|)}\right)^{n\sqrt{\delta}}.$$

Therefore,

$$\sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0, \eta(L_n^{(\alpha)})=\vec{t}]$$
$$\leq \frac{K}{p^n}\left((p\,|G|)^{\log_p(D_1)}\exp\left(2\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_1|}{|T_2|}\right)^{(\frac{1}{p}+\rho)n}\prod_{j\in\tau_2}\frac{1}{|\langle -F_2(j)+T_1\rangle|}.$$

By summing over different the F_2 corresponding to the same τ_2, we see that

$$\sum_{\substack{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)\\ F_2(\tau_2)\subseteq T_2}}\sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0, \eta(L_n^{(\alpha)})=\vec{t}]$$
$$\leq \frac{K}{p^n}\left((p\,|G|)^{\log_p(D_1)}\exp\left(2\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_1|}{|T_2|}\right)^{(\frac{1}{p}+\rho)n}|S_2|^{|\sigma_2|}\left(\sum_{h\in T_2}\frac{1}{|\langle -h+T_1\rangle|}\right)^{|\tau_2|}$$
$$\leq \frac{K}{p^n}\left((p\,|G|^2)^{\log_p(|G|)}\exp\left(2\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_1|}{|T_2|}\right)^{(\frac{1}{p}+\rho)n}\left(\frac{|T_2|}{|T_1|}\right)^{|\tau_2|}.$$

Since $|T_2|<|T_1|$, we see that

$$\left(\frac{|T_2|}{|T_1|}\right)^{|\tau_2|} \leq \left(\frac{|T_2|}{|T_1|}\right)^{\alpha n(1-\delta\log_p(D_2))} \leq \left(\frac{|T_2|}{|T_1|}\right)^{\alpha n}|G|^{n\delta\log_p(|G|)}.$$

Therefore,

$$\sum_{\substack{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)\\ F_2(\tau_2)\subseteq T_2}}\sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0, \eta(L_n^{(\alpha)})=\vec{t}]$$
$$\leq \frac{K}{p^n}\left((p\,|G|^3)^{\log_p(|G|)}\exp\left(2\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_2|}{|T_1|}\right)^{(\alpha-\frac{1}{p}-\rho)n}.$$

The number of choices for τ_2 is at most

$$\sum_{k\leq \log_p(D_2)\delta\alpha n} \binom{\alpha n}{k} \leq \exp\left(2\sqrt{\log_p(D_2)\delta}\alpha n\right) \leq \exp\left(2\sqrt{\log_p(|G|)}\right)^{n\sqrt{\delta}}.$$

We conclude that

$$\sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)} \sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0, \eta(L_n^{(\alpha)})=\vec{t}]$$
$$\leq \frac{K}{p^n}\left((p\,|G|^3)^{\log_p(|G|)}\exp\left(4\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_2|}{|T_1|}\right)^{(\alpha-\frac{1}{p}-\rho)n}.$$

Since $|\mathcal{E}_{n,\rho}|\leq p^n$, we see that

$$\sum_{F_2\in\mathcal{S}_{\lceil\alpha n\rceil,\delta}(T_2,S_2)} \sum_{F_1\in\mathcal{S}_{n,\delta}(T_1,S_1)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0, \eta(L_n^{(\alpha)})\in\mathcal{E}_{n,\rho}]$$
$$\leq K\left((p\,|G|^3)^{\log_p(|G|)}\exp\left(4\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}n}\left(\frac{|T_2|}{|T_1|}\right)^{(\alpha-\frac{1}{p}-\rho)n}.$$

We know that $|T_2|<|T_1|$ and $\rho<\alpha-\frac{1}{p}$, so

$$\left(\frac{|T_2|}{|T_1|}\right)^{(\alpha-\frac{1}{p}-\rho)n}<1.$$

We can choose a sufficiently small $\delta>0$ to ensure that

$$\left((p\,|G|^3)^{\log_p(|G|)}\exp\left(4\sqrt{\log_p(|G|)}\right)\right)^{\sqrt{\delta}}\left(\frac{|T_2|}{|T_1|}\right)^{(\alpha-\frac{1}{p}-\rho)}<1.$$

The result follows. □

Proof of Proposition 3.2.11. This follows from Corollary 3.6.3, Proposition 3.6.5 and Proposition 3.6.7. □

3.7 Parity of 2-rank

In this section $p = 2$. We work with matrices over $\mathbb{F}_2$, and ranks of matrices are taken over $\mathbb{F}_2$. For a vector v, we write $\mathrm{Diag}(v)$ for the diagonal matrix whose diagonal entries are the entries of v, and we write $\mathbf{1}_m$ for the all-ones column vector of length m.

Reducing L_{n_1,n_2} modulo 2, the minus signs disappear, so if $A = (a_{ij}) \in \mathbb{M}_{n_1 \times n_2}(\mathbb{F}_2)$, then

$$\overline{L_{n_1,n_2}} = \begin{bmatrix} \mathrm{Diag}(A\mathbf{1}_{n_2}) & A \\ A^T & \mathrm{Diag}(A^T\mathbf{1}_{n_1}) \end{bmatrix}.$$

Our goal is to determine the parity of $\mathrm{rank}(\overline{L_{n_1,n_2}})$.

Lemma 3.7.1. *Let $B \in \mathbb{M}_k(\mathbb{F}_2)$ be symmetric, and let*

$$v = \begin{bmatrix} b_{11} \\ \vdots \\ b_{kk} \end{bmatrix} \in \mathbb{F}_2^k$$

be the vector of diagonal entries of B. Then $v \in \mathrm{Im}(B)$.

Proof. It suffices to show that for every $y \in \mathbb{F}_2^{1\times k}$, if $yB = 0$, then $yv = 0$. We have

$$yBy^T = \sum_{i=1}^{k} y_i^2 b_{ii} + \sum_{1\le i<j\le k} y_i y_j (b_{ij} + b_{ji}).$$

Over $\mathbb{F}_2$ we have $y_i^2 = y_i$ and $b_{ij} + b_{ji} = 0$, since B is symmetric. This means that

$$yBy^T = \sum_{i=1}^{k} y_i b_{ii} = yv.$$

Therefore, if $yB = 0$, then $yv = 0$. This completes the proof. □

Proposition 3.7.2. *Let $A = (a_{ij}) \in \mathbb{M}_{n_1 \times n_2}(\mathbb{F}_2)$, and let*

$$L(A) = \begin{bmatrix} \mathrm{Diag}(A\mathbf{1}_{n_2}) & A \\ A^T & \mathrm{Diag}(A^T\mathbf{1}_{n_1}) \end{bmatrix} \in \mathbb{M}_{n_1+n_2}(\mathbb{F}_2).$$

Then

$$\mathrm{rank}(L(A)) \equiv \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} a_{ij} \pmod 2.$$

Proof. We induct on the number of nonzero entries of A. If $A = 0$, then $L(A) = 0$, so the base case is clear.

Now assume $A \neq 0$, and choose (i_0, j_0) such that $a_{i_0 j_0} = 1$. Assume without loss of generality that $i_0 = 1$ and $j_0 = 1$. Let E_{11} be the matrix with 1 at the $(1,1)$ entry and zeros elsewhere. Set $A' = A + E_{11}$, so A' has one fewer nonzero entry than A. By the induction hypothesis,

$$\mathrm{rank}(L(A')) \equiv \sum_{i,j} a'_{ij} \equiv \sum_{i,j} a_{ij} + 1 \pmod 2.$$

It therefore suffices to prove that

$$\mathrm{rank}(L(A)) \equiv \mathrm{rank}(L(A')) + 1 \pmod 2.$$

We first remove a redundant row and column. Every row sum and every column sum of both $L(A)$ and $L(A')$ is zero. Hence, in each matrix, the (n_1+1)-th column is the sum of the other columns, so deleting that column does not change the column rank. After deleting that column, the (n_1+1)-th row is the sum of the remaining rows, so deleting that row does not change the rank. Let $\widetilde{L}(A)$ and $\widetilde{L}(A')$ denote the resulting principal submatrices. Then

$$\mathrm{rank}(L(A)) = \mathrm{rank}(\widetilde{L}(A)), \qquad \mathrm{rank}(L(A')) = \mathrm{rank}(\widetilde{L}(A')).$$

There is a scalar $d \in \mathbb{F}_2$ such that

$$\widetilde{L}(A') = \begin{bmatrix} d & \vec{x}^T \\ \vec{x} & K \end{bmatrix}, \qquad \widetilde{L}(A) = \begin{bmatrix} d+1 & \vec{x}^T \\ \vec{x} & K \end{bmatrix},$$

for some symmetric matrix K and some column vector $\vec{x}$.

We now describe K and $\vec{x}$ explicitly. Let B be the $(n_1 - 1) \times (n_2 - 1)$ matrix obtained from A by deleting row 1 and column 1. Let $\vec{u} \in \mathbb{F}_2^{n_2-1}$ be the first row of A with the first entry removed, turned into a column. Let $\vec{b} \in \mathbb{F}_2^{n_1-1}$ be the vector of row sums of A, ignoring the first row. Let $\vec{c} \in \mathbb{F}_2^{n_2-1}$ be the vector of column sums of A, ignoring the first column. Then

$$K = \begin{bmatrix} \mathrm{Diag}(\vec{b}) & B \\ B^T & \mathrm{Diag}(\vec{c}) \end{bmatrix}, \qquad \vec{x} = \begin{bmatrix} 0 \\ \vec{u} \end{bmatrix},$$

where the top zero vector has length $n_1 - 1$. Also note that $\mathbf{1}_{n_1-1}^T B + \vec{u}^T = \vec{c}^T$.

We will show that $\vec{x} \in \mathrm{Im}(K)$, assume for the moment that this is the case. Choose $\vec{z} \in \mathbb{F}_2^{n_1+n_2-2}$ such that $K\vec{z} = \vec{x}$. For $e \in \{0, 1\}$, we have

$$\begin{bmatrix} 1 & 0 \\ \vec{z} & I \end{bmatrix}^T \begin{bmatrix} d+e & \vec{x}^T \\ \vec{x} & K \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \vec{z} & I \end{bmatrix} = \begin{bmatrix} d+e+\vec{z}^T K \vec{z} & \vec{x}^T + \vec{z}^T K \\ \vec{x} + K\vec{z} & K \end{bmatrix}.$$

Since K is symmetric and we are working over $\mathbb{F}_2$, we have $\vec{x} + K\vec{z} = 0$ and $\vec{x}^T + \vec{z}^T K = 0$. Thus exactly one of $\widetilde{L}(A')$ and $\widetilde{L}(A)$ has rank $\mathrm{rank}(K)$, and the other has rank $\mathrm{rank}(K) + 1$. Therefore

$$\mathrm{rank}(\widetilde{L}(A')) \equiv \mathrm{rank}(\widetilde{L}(A)) + 1 \pmod 2.$$

This completes the induction step assuming $\vec{x} \in \mathrm{Im}(K)$.

Now, we want to show that $\vec{x} \in \mathrm{Im}(K)$. Equivalently, we want to find $\vec{y}_1 \in \mathbb{F}_2^{n_1-1}$ and $\vec{y}_2 \in \mathbb{F}_2^{n_2-1}$ such that

$$\mathrm{Diag}(\vec{b})\vec{y}_1 + B\vec{y}_2 = 0, \tag{3.9}$$

$$B^T\vec{y}_1 + \mathrm{Diag}(\vec{c})\vec{y}_2 = \vec{u}. \tag{3.10}$$

Let

$$I_0 = \{r \in \{1, \ldots, n_1 - 1\} : \vec{b}_r = 0\},$$

and let $W \subseteq \mathbb{F}_2^{n_2-1}$ be the span of the rows of B indexed by I_0. Note that (3.9) implies that $\vec{y}_2 \in W^\perp$. Here $W^\perp$ is defined in terms of the usual dot product on $\mathbb{F}_2^{n_2-1}$.

Define a linear map

$$T : W^\perp \to \mathbb{F}_2^{n_2-1}, \qquad T(\vec{y}) = B^T B\vec{y} + \mathrm{Diag}(\vec{c})\vec{y}.$$

Choose a basis $w_1, \ldots, w_k$ of $W^\perp$, and define $N \in \mathbb{M}_k(\mathbb{F}_2)$ by $N_{lm} := w_l^T T(w_m)$. Since

$$w_l^T T(w_m) = (Bw_l)^T(Bw_m) + w_l^T \mathrm{Diag}(\vec{c})w_m,$$

the matrix N is symmetric.

Next we compute its diagonal. Let $w \in W^\perp$. Since we are working over $\mathbb{F}_2$, we have

$$w^T T(w) = (Bw)^T(Bw) + w^T \mathrm{Diag}(\vec{c})w = \mathbf{1}_{n_1-1}^T Bw + \vec{c}^T w.$$

We have $\mathbf{1}_{n_1-1}^T B = (\vec{c}+\vec{u})^T$, so

$$w^T T(w) = (\vec{c}+\vec{u})^T w + \vec{c}^T w = \vec{u}^T w.$$

Therefore the diagonal vector of N is

$$\begin{bmatrix} \vec{u}^T w_1 \\ \vdots \\ \vec{u}^T w_k \end{bmatrix}.$$

By Lemma 3.7.1, this vector lies in $\mathrm{Im}(N)$. Thus there exists

$$q = \begin{bmatrix} q_1 \\ \vdots \\ q_k \end{bmatrix} \in \mathbb{F}_2^k, \qquad \text{such that} \qquad Nq = \begin{bmatrix} \vec{u}^T w_1 \\ \vdots \\ \vec{u}^T w_k \end{bmatrix}.$$

Choose

$$\vec{y}_2 = q_1 w_1 + \cdots + q_k w_k \in W^\perp.$$

Then for each l, $w_l^T T(\vec{y}_2) = \vec{u}^T w_l$, so

$$\vec{u} - T(\vec{y}_2) \in (W^\perp)^\perp = W.$$

Since W is spanned by the rows of B indexed by I_0, there exists a vector $\vec{g} \in \mathbb{F}_2^{n_1-1}$ supported on I_0 such that

$$B^T \vec{g} = \vec{u} - T(\vec{y}_2).$$

Choose $\vec{y}_1 = B\vec{y}_2 + \vec{g}$.

We verify (3.9) and (3.10). Since $\vec{y}_2 \in W^\perp$, the vector $B\vec{y}_2$ vanishes on I_0. Since we are working over $\mathbb{F}_2$, $\mathrm{Diag}(\vec{b})B\vec{y}_2 = B\vec{y}_2$. Also, $\mathrm{Diag}(\vec{b})\vec{g} = 0$ because $\vec{g}$ is supported on I_0. Therefore,

$$\mathrm{Diag}(\vec{b})\vec{y}_1 + B\vec{y}_2 = \mathrm{Diag}(\vec{b})(B\vec{y}_2 + \vec{g}) + B\vec{y}_2 = B\vec{y}_2 + B\vec{y}_2 = 0.$$

This proves (3.9). Also,

$$B^T\vec{y}_1 + \mathrm{Diag}(\vec{c})\vec{y}_2 = B^T(B\vec{y}_2 + \vec{g}) + \mathrm{Diag}(\vec{c})\vec{y}_2 = T(\vec{y}_2) + B^T\vec{g} = T(\vec{y}_2) + \vec{u} - T(\vec{y}_2) = \vec{u},$$

which proves (3.10). Hence $\vec{x} \in \mathrm{Im}(K)$. $\square$

Proposition 3.2.6. Suppose $p = 2$. For any $0 < \alpha \leq 1$,

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}\right] = \frac{1}{2}.$$

Proof. Note that

$$\mathrm{rank}(G(L_n^{(\alpha)})) = n + \lceil \alpha n \rceil - 1 - \mathrm{rank}\left(\overline{L_n^{(\alpha)}}\right).$$

Therefore,

$$\mathbb{P}\left[\mathrm{rank}(G(L_n^{(\alpha)})) \text{ is odd}\right] = \mathbb{P}\left[\mathrm{rank}\left(\overline{L_n^{(\alpha)}}\right) \equiv n + \lceil \alpha n \rceil \pmod 2\right].$$

By Proposition 3.7.2, this is

$$\mathbb{P}\left[\sum_{i=1}^{n}\sum_{j=1}^{\lceil \alpha n \rceil} a_{ij} \equiv n + \lceil \alpha n \rceil \pmod 2\right].$$

Since the a_{ij} are independent and ϵ-balanced, [24, Lemma 2.1] implies that

$$\left|\mathbb{P}\left[\sum_{i=1}^{n}\sum_{j=1}^{\lceil \alpha n\rceil} a_{ij} \equiv n+\lceil \alpha n\rceil+1 \pmod 2\right]-\frac{1}{2}\right| < \exp\Big(-\frac{\epsilon\alpha n^2}{2^2}\Big).$$

The result follows. $\square$

3.8 Raw moments sometimes diverge to infinity

We consider the special case of $L_n^{(\alpha)}$ when all a_{ij} are Haar-uniform and show that certain moments blow up to infinity.

Proposition 3.8.1. *Consider $0<\alpha<1$ and $m>\frac{2-\alpha}{1-\alpha}$. If all a_{ij} in $L_n^{(\alpha)}$ are Haar-uniform, then we have*

$$\lim_{n\to\infty}\mathbb{E}[\left|\mathrm{Hom}(G(L_n^{(\alpha)}),(\mathbb{Z}/p\mathbb{Z})^m)\right|]=\infty.$$

Proof. Denote $G=(\mathbb{Z}/p\mathbb{Z})^m$, $n_1=n$ and $n_2=\lceil \alpha n\rceil$. Recall that

$$\left|\mathrm{Hom}(G(L_n^{(\alpha)}),(\mathbb{Z}/p\mathbb{Z})^m)\right| = \frac{1}{p^m}\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}),(\mathbb{Z}/p\mathbb{Z})^m)\right|.$$

Moreover,

$$\mathbb{E}\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}),(\mathbb{Z}/p\mathbb{Z})^m)\right|\right] = \sum_{F_1\in\mathrm{Hom}([n_1],G)}\ \sum_{F_2\in\mathrm{Hom}([n_2],G)} \mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0].$$

It follows from (3.3) that

$$\begin{aligned}&\mathbb{P}[(F_1,F_2)\circ L_n^{(\alpha)}=0]\\ &=\frac{1}{\left|\mathcal{C}^*_{n_1}(\langle F_2\rangle_1,F_1)\right|}\frac{1}{\left|\mathcal{C}^*_{n_2}(\langle F_1\rangle_1,F_2)\right|}\sum_{C_1\in\mathcal{C}^*_{n_1}(\langle F_2\rangle_1,F_1)}\ \sum_{C_2\in\mathcal{C}^*_{n_2}(\langle F_1\rangle_1,F_2)}\prod_{i=1}^{n_1}\prod_{j=1}^{n_2}\mathbb{E}\left[E[F_1,F_2,C_1,C_2](i,j)^{a_{ij}}\right].\end{aligned}$$

Since all the a_{ij} are Haar-uniform, we know that the only (C_1, C_2) that will contribute are the ones for which all coefficients $E[F_1, F_2, C_1, C_2](i, j) = 1$. We call (C_1, C_2) as (F_1, F_2)-special if this condition holds.

Let T be a subgroup of G isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let $D(G, T)$ be the set of pairs of functions (β_1, β_2) such that the following hold:

1. β_1 maps G to $\bigcup_{g \in G} \langle -g + T \rangle^*$ and for every $g \in G$, $\beta_1(g) \in \langle -g + T \rangle^*$;

2. β_2 maps T to G^*;

3. For every $g \in G$ and $h \in T$, we have

$$\beta_1(g)(-g + h)\beta_2(h)(-h + g) = 1.$$

As a lower bound, we only sum over $F_1 \in \mathrm{Hom}([n_1], G)$, $F_2 \in \mathrm{Hom}([n_2], T)$ with $\mathrm{set}(F_1) = G$ and $\mathrm{set}(F_2) = T$. For such F_1, F_2, by an argument identical to Section 3.4, we see that the number of pairs (C_1, C_2) that are (F_1, F_2)-special is $|D(G, T)|$. Therefore,

$$\mathbb{P}[(F_1, F_2) \circ L_n^{(\alpha)} = 0] = \frac{|D(G, T)|}{\left|\mathcal{C}^*_{n_1}(T, F_1)\right| \times \left|\mathcal{C}^*_{n_2}(G, F_2)\right|}.$$

Note that

$$\left|\mathcal{C}^*_{n_2}(G, F_2)\right| = |G|^{n_2} = p^{mn_2}.$$

Moreover,

$$|\langle -g + T \rangle| = \begin{cases} p & \text{if } g \in T, \\ p^2 & \text{if } g \notin T, \end{cases}$$

so

$$\left|\mathcal{C}^*_{n_1}(T, F_1)\right| \le p^{2n_1}.$$

Finally, note that the number of $F_1 \in \mathrm{Hom}([n_1], G)$, with $\mathrm{set}(F_1) = G$ is $|G|^{n_1}(1 - o(1))$ and the number of $F_2 \in \mathrm{Hom}([n_1], T)$ with $\mathrm{set}(F_2) = T$ is $p^{n_2}(1 - o(1))$. Therefore,

$$\begin{aligned}\mathbb{E}\left[\left|\mathrm{Hom}(\mathrm{Coker}(L_n^{(\alpha)}), (\mathbb{Z}/p\mathbb{Z})^m))\right|\right] &\ge p^{mn}(1 - o(1)) \times p^{\alpha n}(1 - o(1)) \frac{|D(G, T)|}{p^{2n} p^{m\alpha n}} \\ &= (1 - o(1))\, |D(G, T)| \left(p^{m+\alpha-2-m\alpha}\right)^n.\end{aligned}$$

We know that $D(G, T) \ge 1$. By choice of α, we know that $m + \alpha - 2 - m\alpha > 0$, which completes the proof. □

3.9 Lemmas

Denote the binary entropy function as $H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. It is known that $\binom{a}{b} \le 2^{H(\frac{b}{a})a}$ and that $H(\alpha) \le 2\sqrt{\alpha}$. It follows that

$$\binom{a}{b} \le 2^{2\sqrt{ab}}.$$

Lemma 3.9.1. *For every integer $a \ge 1$ and every real number $0 < \delta \le 1$, we have*

$$\sum_{k=0}^{\lfloor \delta a \rfloor} \binom{a}{k} \le 2^{2\sqrt{\delta} a}.$$

Proof. First assume $0 < \delta \le \frac{1}{2}$. Using the standard entropy bound for the lower tail of binomial coefficients together with the estimate $H(\delta) \leq 2\sqrt{\delta}$, we get

$$\sum_{k=0}^{\lfloor \delta a \rfloor} \binom{a}{k} \leq 2^{H(\delta)a} \leq 2^{2\sqrt{\delta}a}.$$

For $\frac{1}{2} < \delta \leq 1$, we have the trivial bound $\sum_{k=0}^{\lfloor \delta a \rfloor} \binom{a}{k} \leq 2^a < 2^{2\sqrt{\delta}a}$. □

3.9.1 Counting codes and non-codes

We will obtain bounds on the sizes of $\mathcal{S}_{n,\delta}(S,T)$. We start with the case $T \subsetneq S$.

Lemma 3.9.2. *[23, Lemma 5.2] Given a chain of translated subgroups $T \trianglelefteq_{tr} S \trianglelefteq_{tr} G$, denote $D = [S : T] > 1$. Then we have*

$$|\mathcal{S}_{n,\delta}(S,T)| \leq 4^{n\sqrt{\delta \log_p(|G|)}} \, |T|^n \, D^{\delta \log_p(D) n}.$$

Proof. If $F \in \mathcal{S}_{n,\delta}(S,T)$, then there is $\sigma \subseteq [n]$ with $|\sigma| < \delta \log_p(D)n$ such that for $i \in [n] \setminus \sigma$ $F(i) \in T$ and for $i \in \sigma$ $F(i) \in S$. By enlarging σ, we can assume that $|\sigma| = \lceil \delta \log_p(D)n \rceil - 1$.

We have $\binom{n}{\lceil \delta \log_p(D)n \rceil - 1}$ choices for σ. Once σ is chosen, there are $|T|^{n-(\lceil \delta \log_p(D)n \rceil -1)} \, |S|^{\lceil \delta \log_p(D)n \rceil -1}$ choices for F. Therefore,

$$|\mathcal{S}_{n,\delta}(S,T)| \leq \binom{n}{\lceil \delta \log_p(D)n \rceil - 1} |T|^n \, D^{\lceil \delta \log_p(D)n \rceil -1} \leq 2^{2\sqrt{n\delta \log_p(D)n}} \, |T|^n \, D^{\delta \log_p(D)n}. \square$$

Given a group G, let K_G be the number of translated subgroups of G. We estimate the size of $\mathcal{S}_{n,\delta}(T,T)$.

Lemma 3.9.3. *Consider $0 < \delta < \frac{1}{9 \log_p(|G|)}$. There is a constant $c_{G,\delta} > 0$ (depending on G* *and δ), such that for each translated subgroup $T \trianglelefteq_{tr} G$*

$$|T|^n \left(1 - K_G \exp(-c_{G,\delta} n) - K_G 2^{-n}\right) \le |\mathcal{S}_{n,\delta}(T,T)| \le |T|^n .$$

Proof. The upper bound follows from the fact that

$$\mathcal{S}_{n,\delta}(T,T) \subseteq \mathrm{Hom}([n],T).$$

Moreover,

$$\mathrm{Hom}([n],T) \setminus \mathcal{S}_{n,\delta}(T,T) = \bigcup_{T' \trianglelefteq_{\mathrm{tr}} T} \mathcal{S}_{n,\delta}(T,T') \cup \mathrm{Hom}([n],T').$$

The number of T' is at most K_G, and

$$|\mathrm{Hom}([n],T')| = |T'|^n \le \frac{|T|^n}{2^n}.$$

Denote $[T : T'] = D > 1$. Then we know that

$$|\mathcal{S}_{n,\delta}(T,T')| \le 2^{2n\sqrt{\delta \log_p(|G|)}} |T|^n D^{-n+\delta \log_p(D) n} \le |T|^n \left(2^{2\sqrt{\delta \log_p(|G|)} - 1 + \delta \log_p(|G|)}\right)^n.$$

The bound on δ also ensures that $2\sqrt{\delta \log_p(|G|)} - 1 + \delta \log_p(|G|) < 0$. The result follows. □

3.9.2 Counting non-robust C

Lemma 3.9.4. *Given $0 < \gamma < 1$, $F \in \mathrm{Hom}([n],G)$ and a translated subgroup $T \trianglelefteq_{tr} G$, the number of $C \in \mathcal{C}_n^*(T,F)$ that are not $(\gamma n, F)$-robust is at most*

$$|G|^{|G|} (4|G|)^{n\sqrt{\gamma}} .$$

Proof. If $C \in \mathcal{C}_n^*(T,F)$ is not $(\gamma n, F)$-robust, then there is some $\sigma \subseteq [n]$ with $|\sigma| < \gamma n$

such that for $i_1, i_2 \in [n] \setminus \sigma$, $F(i_1) = F(i_2)$ implies $C(i_1) = C(i_2)$. This means there is some $\beta : G \to \bigcup_{g\in G} \langle -g + T\rangle^*$, such that for each $i \in [n]\setminus\sigma$ we have $C(i) = \beta(F(i))$. By enlarging σ, we can assume that $|\sigma| = \lceil \gamma n\rceil - 1$.

It follows that the number of choices for σ is $\binom{n}{\lceil\gamma n\rceil - 1}$. The number of choices for β is at most $|G|^{|G|}$. Once we choose σ and β, then $C(i)$ is determined for $i \in [n]\setminus\sigma$. For $i \in \sigma$, $C(i)$ has at most $|G|$ choices. Therefore, the number of $C \in \mathcal{C}_n^*(T, F)$ that are not $(\gamma n, F)$-robust is at most

$$\binom{n}{\lceil\gamma n\rceil - 1} |G|^{|G|} |G|^{\lceil\gamma n\rceil - 1} \leq 2^{2\sqrt{n(\gamma n)}} |G|^{|G|} |G|^{\gamma n} \leq |G|^{|G|} (4 |G|)^{n\sqrt{\gamma}}. \qquad \square$$

Lemma 3.9.5. *Given $0 < \gamma < 1$, $F \in \mathrm{Hom}([n], G)$, $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$ and a translated subgroup $T \trianglelefteq_{tr} G$, the number of $C \in \mathcal{C}_n^*(T, F)$ that are not $(\gamma n, F, \vec{s})$-robust is at most*

$$|G|^{p|G|} (4 |G|)^{n\sqrt{\gamma}}.$$

Proof. If $C \in \mathcal{C}_n^*(T, F)$ is not $(\gamma n, F, \vec{s})$-robust, then there is some $\sigma \subseteq [n]$ with $|\sigma| < \gamma n$ such that for $i_1, i_2 \in [n] \setminus \sigma$, $(F(i_1), s_{i_1}) = (F(i_2), s_{i_2})$ implies $C(i_1) = C(i_2)$. This means there is some $\beta : G \times (\mathbb{Z}/p\mathbb{Z}) \to \bigcup_{g\in G} \langle -g + T\rangle^*$, such that for each $i \in [n] \setminus \sigma$, we have $C(i) = \beta(F(i), s_i)$. By enlarging σ, we can assume that $|\sigma| = \lceil\gamma n\rceil - 1$.

It follows that the number of choices for σ is $\binom{n}{\lceil\gamma n\rceil - 1}$. The number of choices for β is at most $|G|^{p|G|}$. Once we choose σ and β, then $C(i)$ is determined for $i \in [n]\setminus\sigma$. For $i \in \sigma$, $C(i)$ has at most $|G|$ choices. Therefore, the number of $C \in \mathcal{C}_n^*(T, F)$ that are not $(\gamma n, F, \vec{s})$-robust is at most

$$\binom{n}{\lceil\gamma n\rceil - 1} |G|^{p|G|} |G|^{\lceil\gamma n\rceil - 1} \leq 2^{2\sqrt{n(\gamma n)}} |G|^{p|G|} |G|^{\gamma n} \leq |G|^{p|G|} (4 |G|)^{n\sqrt{\gamma}}. \qquad \square$$

Lemma 3.9.6. *Given $0 < \gamma < 1$, $F \in \mathrm{Hom}([n], G)$ and a translated subgroup $T \trianglelefteq_{tr} G$, the number of $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$ that are not $(\gamma n, F, T)$-robust is at most*

$$p^{|G|}\,(4p)^{n\sqrt{\gamma}}\,p^{|\{i\in[n]:F(i)\notin T\}|}.$$

Proof. If $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$ is not $(\gamma n, F, T)$-robust, then there is some $\sigma \subseteq [n]$ with $|\sigma| < \gamma n$ such that for $i_1, i_2 \in [n] \setminus \sigma$, $F(i_1) = F(i_2) \in T$ implies $s_{i_1} = s_{i_2}$. This means there is some $\lambda : T \to (\mathbb{Z}/p\mathbb{Z})$, such that for each $i \in [n] \setminus \sigma$, if $F(i) \in T$, then $s_i = \lambda(F(i))$. By enlarging σ, we can assume that $|\sigma| = \lceil \gamma n \rceil - 1$.

The number of choices for σ is $\binom{n}{\lceil \gamma n\rceil - 1}$. The number of choices for λ is at most $p^{|G|}$. Once we choose σ and λ, then s_i is determined for $i \in [n] \setminus \sigma$ with $F(i) \in T$. For other i, s_i has at most p choices. Therefore, the number of $\vec{s} \in (\mathbb{Z}/p\mathbb{Z})^n$ that are not $(\gamma n, F, T)$-robust is at most

$$\binom{n}{\lceil \gamma n\rceil - 1} p^{|G|} p^{|\{i\in[n]:F(i)\notin T\}|} p^{\lceil \gamma n\rceil - 1} \le 2^{2\sqrt{n(\gamma n)}} p^{|G|} p^{\gamma n} p^{|\{i\in[n]:F(i)\notin T\}|} \le p^{|G|}\,(4p)^{n\sqrt{\gamma}}\,p^{|\{i\in[n]:F(i)\notin T\}|}. \square$$

3.9.3 Size of $\mathcal{E}_{n,\rho}$

Lemma 3.9.7. *Given $\rho > 0$, we have*

$$\lim_{n\to\infty} \frac{|\mathcal{E}_{n,\rho}|}{p^n} = 1.$$

Proof. By Hoeffding's inequality, we see that

$$\left|1 - \frac{|\mathcal{E}_{n,\rho}|}{p^n}\right| \le \left|1 - \sum_{k:\left|k - \frac{1}{p}n\right| \le \rho n} \binom{n}{k} \frac{1}{p^k}\Big(1 - \frac{1}{p}\Big)^{n-k}\right| \le 2\exp\big(-2\rho^2 n\big).$$

The result follows. $\square$

Lemma 3.9.8. *Given $\rho > 0$, we have*

$$\lim_{n\to\infty} \mathbb{P}[\eta(L_n^{(\alpha)}) \in \mathcal{E}_{n,\rho}] = 1.$$

Proof. This follows from [22, Lemma 8.2]. □

Acknowledgments

We thank Nathan Kaplan for introducing me to this problem and for many helpful discussions about the problem. We acknowledge support from NSF Grant DMS 2154223.

Chapter 4

Further conjectures

In this chapter, we record two new conjectures.

4.1 The k-partite undirected graphs

Let $k \geq 2$ be an integer and $0 < v < 1$ a constant. For each $n \geq 1$, let $\Gamma_n^{(k)}(v)$ be a random undirected k-partite graph with vertex partition $V_1 \sqcup V_2 \sqcup \cdots \sqcup V_k$, with each $|V_i| = n$, where each edge between two distinct parts is included independently with probability v. Let $S_{\Gamma_n^{(k)}(v)}$ denote the sandpile group of $\Gamma_n^{(k)}(v)$.

We conjecture that, except in the bipartite 2-primary case, the limiting distribution of the Sylow p-subgroup of $S_{\Gamma_n^{(k)}(v)}$ should agree with the symmetric Cohen-Lenstra distribution. In the exceptional case $(k, p) = (2, 2)$, a different limiting distribution was conjectured by [10] and the results of Chapter 3 support this conjecture.

Conjecture 4.1.1. *Let p be a prime, $k \geq 2$ an integer and $0 < v < 1$. For every finite* *abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{P}\big[(S_{\Gamma_n^{(k)}(v)})_p \cong G\big] = \begin{cases} P_{\infty,p}^{\mathrm{Sym}}(G) & \text{if } k \neq 2 \text{ or } p \neq 2, \\ 2^{\mathrm{rank}(G)-1} P_{\infty,2}^{\mathrm{Sym}}(G) & \text{if } k = 2 \text{ and } p = 2. \end{cases}$$

In other words, the bipartite 2-primary case should remain the unique exceptional case among all undirected multipartite graphs.

4.2 A block random matrix model

We now describe a more general random matrix model that leads to many interesting limiting distributions.

Fix an integer $k \geq 1$ and a subset $S \subseteq [k] \times [k]$ such that $(i,i) \in S$ for each $1 \leq i \leq k$. For each $n \geq 1$, let $X_n \in \mathbb{M}_{kn}(\mathbb{Z}_p)$ be the random block matrix

$$X_n = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{bmatrix},$$

where each block $A_{ij} \in \mathbb{M}_n(\mathbb{Z}_p)$, and:

1. if $(i,j) \in S$, then the entries of A_{ij} are independent and ϵ-balanced;

2. if $(i,j) \notin S$, then $A_{ij} = 0$;

3. for different $(i,j) \in S$, the A_{ij} are mutually independent.

Definition 4.2.1. For a finite abelian p-group G, define $n_S(G)$ to be the number of k-tuples $(H_1, \ldots, H_k)$ such that

1. each $H_i \trianglelefteq G$;
2. $H_1 + \cdots + H_k = G$;
3. for each $(i, j) \in S$, we have $H_i \trianglelefteq H_j$.

The conjecture is that the limiting distribution of $\operatorname{Coker}(X_n)$ is governed by this subgroup-counting function.

Conjecture 4.2.2. *Let p be a prime, let $S \subseteq [k] \times [k]$ be a subset such that $(i, i) \in S$ for each $i \in [k]$. Then there exists a constant $C_{p,S} > 0$, such that for every finite abelian p-group G, we have*

$$\lim_{n\to\infty} \mathbb{P}\big[\operatorname{Coker}(X_n) \cong G\big] = C_{p,S} \frac{n_S(G)}{|\operatorname{Aut}(G)|}.$$

Moreover, for every finite abelian p-group G,

$$\lim_{n\to\infty} \mathbb{E}\big[|\operatorname{Sur}(\operatorname{Coker}(X_n), G)|\big] = n_S(G).$$

Let us briefly look at some special cases.

First, if $S = \{(i, i) : i \in [k]\}$, then

$$\operatorname{Coker}(X_n) = \operatorname{Coker}(A_{11}) \oplus \cdots \oplus \operatorname{Coker}(A_{kk}).$$

The limiting distribution of each $\operatorname{Coker}(A_{ii})$ is $P_{\infty,1}$. So the limiting distribution of $\operatorname{Coker}(X_n)$ would be the direct sum of k finite abelian p-groups each distributed according to $P_{\infty,1}$.

Next, if $S = [k] \times [k]$, then X_n is just an ϵ-balanced random matrix in $\mathbb{M}_{kn}(\mathbb{Z}_p)$. Moreover, in this case each $n_S(G) = 1$. So the limiting distribution is just $P_{\infty,1}$.

Finally, consider $S = \{(i,j) \in [k] \times [k] : i \leq j\}$. Then $n_S(G)$ counts the number of chains of subgroups of G of the form

$$H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_k = G.$$

This quantity is denoted as $n_k(G)$ by Nguyen and Van Peski in [16]. The limiting distribution of $\mathrm{Coker}(X_n)$ conjectured by us is the same distribution that Nguyen and Van Peski obtained as the limiting distribution of $\mathrm{Coker}(M_1 M_2 \ldots M_k)$, where $M_i \in \mathbb{M}_n(\mathbb{Z}_p)$ are independent, ϵ-balanced matrices.

Bibliography

[1] A. Bhargava, J. DePascale, and J. Koenig. The rank of the sandpile group of random directed bipartite graphs. *Annals of Combinatorics*, 27(4):979–992, 2023.

[2] M. Bhargava, D. M. Kane, H. W. Lenstra, B. Poonen, and E. Rains. Modeling the distribution of ranks, selmer groups, and shafarevich–tate groups of elliptic curves. *Cambridge Journal of Mathematics*, 3(3):275–321, 2015.

[3] G. Cheong and Y. Huang. The cokernel of a polynomial push-forward of a random integral matrix with concentrated residue. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 178, pages 229–257. Cambridge University Press, 2025.

[4] G. Cheong and N. Kaplan. Generalizations of results of Friedman and Washington on cokernels of random p-adic matrices. *Journal of Algebra*, 604:636–663, 2022.

[5] G. Cheong and M. Yu. The distribution of the cokernel of a polynomial evaluated at a random integral matrix. *arXiv preprint arXiv:2303.09125*, 2023.

[6] J. Clancy, N. Kaplan, T. Leake, S. Payne, and M. M. Wood. On a Cohen–Lenstra heuristic for jacobians of random graphs. *Journal of Algebraic Combinatorics*, 42(3):701–723, 2015.

[7] J. S. Ellenberg, A. Venkatesh, and C. Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *annals of Mathematics*, pages 729–786, 2016.

[8] E. Friedman and L. C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Théorie des nombres*, pages 227–239. de Gruyter Berlin, 1989.

[9] J. Fulman and N. Kaplan. Random partitions and Cohen–Lenstra heuristics. *Annals of Combinatorics*, 23(2):295–315, 2019.

[10] J. Fulman, N. Kaplan, D. Singhal, and O. Warnaar. Sandpile groups of random bipartite graphs and families of distributions with the same moments. Preprint, 2026.

[11] E. Hodges. The distribution of sandpile groups of random graphs with their pairings. *Transactions of the American Mathematical Society*, 377(12):8769–8815, 2024.

[12] S. Koplewitz. Sandpile groups and the coeulerian property for random directed graphs. *Advances in Applied Mathematics*, 90:145–159, 2017.

[13] J. Lee. Joint distribution of the cokernels of random p-adic matrices. In *Forum Mathematicum*, volume 35, pages 1005–1020. De Gruyter, 2023.

[14] M. Lipnowski, W. Sawin, and J. Tsimerman. Cohen-lenstra heuristics and bilinear pairings in the presence of roots of unity. *arXiv preprint arXiv:2007.12533*, 2020.

[15] A. Mészáros. The distribution of sandpile groups of random regular graphs. *Transactions of the American Mathematical Society*, 373(9):6529–6594, 2020.

[16] H. H. Nguyen and R. Van Peski. Universality for cokernels of random matrix products. *Advances in Mathematics*, 438:109451, 2024.

[17] H. H. Nguyen and M. M. Wood. Random integral matrices: universality of surjectivity and the cokernel. *Inventiones mathematicae*, 228(1):1–76, 2022.

[18] H. H. Nguyen and M. M. Wood. Local and global universality of random matrix cokernels. *Mathematische Annalen*, 391(4):5117–5210, 2025.

[19] W. Sawin and M. M. Wood. The moment problem for random objects in a category. *arXiv preprint arXiv:2210.06279*, 2022.

[20] J. Shen. Quantative universality for cokernels of matrices with symmetries. *arXiv preprint arXiv:2601.09704*, 2026.

[21] D. Singhal. Distribution of sandpile groups of random bipartite graphs. Preprint, 2026.

[22] D. Singhal. Distribution of sandpile groups of random directed bipartite graphs. Preprint, 2026.

[23] M. Wood. The distribution of sandpile groups of random graphs. *Journal of the American Mathematical Society*, 30(4):915–958, 2017.

[24] M. M. Wood. Random integral matrices and the Cohen-Lenstra heuristics. *American Journal of Mathematics*, 141(2):383–398, 2019.

[25] M. M. Wood. Probability theory for random groups arising in number theory. In *International Congress of Mathematicians*, pages 4476–4508. European Mathematical Society-EMS-Publishing House GmbH, 2023.