UNIVERSITY OF CAMBRIDGE

Algebraic Techniques for Random Covering Graphs

Shashwat Silas
St John's College

Submitted to the University of Cambridge in partial fulfilment of the requirements for the degree of Master of Philosophy in Advanced Computer Science

June 2016

Abstract. This thesis is initiated by a problem posed by Alon Amit and Nathan Linial in their paper [**AL**, **2002**]. They introduce the currently highly studied model of random covering graphs (also known as random *lifts* of graphs), and their main theorem is that asymptotically almost surely, a random n-covering of a simple connected graph G with minimum degree δ is δ-connected. They ask whether this probability can be estimated as a function of n and suggest a possible generalization of their work to iterated random coverings.

We develop new algebraic techniques which provide a solution to their question, prove new results about the edge expansion of random covering graphs, and about δ-connectivity of families where δ is not a fixed constant. We use wreath products of groups to describe iterated random coverings and extend all our results to them. We show the existence of homotopy invariants in general models of random covering graphs and use them to show a connection between random covering graphs and random regular graphs. As an intermediate step to our results, we prove a general version of Babai's theorem about the probability of generating the symmetric group using two random generators, and prove results towards a further generalization of this theorem to wreath products of symmetric groups.

Acknowledgements. I would like to thank my supervisor, Dr. Thomas Sauerwald for his guidance through this project and for constantly encouraging me to follow my interests. As with Thomas, I have previously also been extremely fortunate to have the most supportive teachers nurturing my interest in Computer Science and Mathematics, and none of this would be possible without the effort invested in my education by Professors Paul Valiant and Michael Rosen at Brown.

I owe deep gratitude to St John's College for providing me an idyllic home during my time at Cambridge and for supporting my studies through a Benefactor's Scholarship for Research.

Many thanks to my friends Alexander Makelov and Luke Kweku Abraham. Alex, for reading early drafts of this work and being available for discussion through busy times, and Kweku, for the most thorough and informative editing.

The Cambridge Computer Lab has been a wonderful place to study. I always felt welcomed and heard. Thanks to everyone involved in the administration of the MPhil for their many efforts to create such an environment. I hope to be back some day.

Finally, thanks to Mom for always taking care of me.

"There's never enough time to do all the nothing you want."

—Calvin and Hobbes

Contents

List of Illustrations

CHAPTER 0

Introduction

Randomization is surprisingly often a good way out of a sticky situation. Consider the following permutation packet routing problem. Suppose n is even. Given the n-hypercube, which has the vertices $\{0,1\}^n$ and edges between any two vertices which differ at exactly one coordinate: we place one packet at each vertex, and we would like to permute the packets given the restrictions that in a single time step, any edge can carry only one packet and any packet can cross only one edge. The obvious solution is to use bit-fixing. Given a packet $(a_1,\ldots,a_n)$ whose destination is $(b_1,\ldots,b_n)$: for each i, check if $a_i = b_i$, and if not, simply take the edge that connects $(b_1,\ldots,b_{i-1},a_i,a_{i+1},\ldots,a_n)$ to $(b_1,\ldots,b_{i-1},b_i,a_{i+1},\ldots,a_n)$. We can clog up this network in the following way: represent the initial locations of the packets as ab for each $a,b \in \{0,1\}^{\frac{n}{2}}$ and consider the permutation which sends each packet from ab to ba. Now each packet will need to cross an address of the form aa to get to its destination. There are $2^{\frac{n}{2}}$ packets with address aa for $a \in \{0,1\}^{\frac{n}{2}}$, each with exactly n edges leaving it, implying the that the routing will take $\Omega\left(\frac{2^{\frac{n}{2}}}{n}\right)$ time steps. Interestingly, a different approach works well. Choose a random permutation of the packets, and first send each packet to its destination in the random permutation. From these random locations send each packet to its desired location. Even though it seems like we are doing more work in these two routing steps, careful analysis of this randomized algorithm shows that its expected runtime is $O(n)$, an improvement from exponential to linear time. The takeaway is that randomization is a powerful, and justly important, tool in computer science, and that random mathematical objects, like random permutations, are very handy!

Graphs are one of the most versatile and pervasive abstractions in science. They not only model computer and social networks, but are important everywhere from combinatorics and algorithms to biology and chemistry. Since randomization and graphs are both important in computer science, it is unsurprising that the theory of 'random graphs' has proved useful as well. Pioneered by Paul Erdós and Béla Bollabás, there are several notions of random graphs. As we know: random anything tends to have many nice properties.

The study of properties of random graphs has current importance as it is intertwined with one of the most powerful ideas in recent computer science theory: *expander graphs.* Expander graphs have the paradoxical qualities of being sparse yet well-connected, and they have played a central role in recent advances in complexity theory, approximation algorithms and cryptography. An excellent and quick introduction to expanders may be found in [**Tre**, **2014**]. One way to understand the magic of expander graphs is that they mimic the nice properties of random graphs but they can be constructed without randomness. In fact, such an explicit construction of expander graphs was an important problem in mathematics and computer science until it was solved by Grigory Margulis in [**Mar**, **1973**]. Even now, the construction of 'optimal' expander graphs, called Ramanujan graphs, is an important open problem in computer science. Very recently, [**MSS**, **2015**] and [**HPS**, **2016**] have made important advances towards a solution by proving existence results for such graphs using a construction known as *covering graphs*. Covering graphs also have applications to the Unique Games conjecture [**AKK**, **2008**]. We will study a random model for these covering graphs proposed by [**AL**, **2002**].

Even though important graphs, like the Internet or Facebook, can have large and complicated global structures, graphs inherently model local relationships. Covering graphs formalize a notion of local similarity amongst graphs which are globally very different. Somewhat imprecisely, a large graph which is locally similar to a small graph is said to be a *cover* of the small graph which is called the *base*. The study of *random* covering graphs came to the forefront after the work of [**AL**, **2002**], which many others have expanded upon (cf. Chapter 2.2, page 25 for references). These results show that most random coverings of a graph not only preserve its good properties but have very nice behavior in general.

In this thesis we will follow a long line of work focusing on fundamental questions about random covering graphs. We will approach these questions using novel algebraic techniques. The study of random covering graphs has two main questions:

1. What are the properties of random covering graphs?
2. How do random covering graphs inherit structure from their base graph?

Much work has been done on the first question to understand the structural properties of random covering graphs *asymptotically almost surely*, i.e. properties which hold with probability tending to one as the size of the covering graph goes to infinity. In their highly influential paper [**AL**, **2002**], Amit and Linial ask whether their main theorem, an asymptotic statement about connectivity in random coverings graphs (Theorem 2.10), can be estimated as a function of the *degree* of the covering (cf. Chapter 1). In Chapter 5 we solve this problem (Theorem 5.11) and prove several new results as well.

For the second question, we turn to algebraic topology. We will discuss in Chapter 1 that covering graphs arise from the notion of covering spaces in topology. It is well known that covering spaces of homotopy equivalent topological spaces have many similarities. Fittingly, in Chapter 7 we will show that there are probabilistic similarities between the random covering graphs of any two homotopy equivalent graphs.

It is natural to use algebraic techniques to study random covering graphs; we will show in Chapter 2 that random covering graphs are constructed using random permutations, and after all, graphs are topological spaces. Our main idea is simple: through a simplification of the Amit-Linial model for random covering graphs we establish a natural relationship between a random covering graph and a randomly generated subgroup of the symmetric group on n elements, $\mathcal{S}_n$. We call this subgroup the walk-subgroup and use it to prove new results about both graphs and groups. In order to make this technique work, we needed to prove a general version of Babai's theorem about the probability of generating the symmetric group using two random generators, which is an interesting result in itself, and its proof is in Chapter 4 and Appendix A.

One testament to the robustness of our techniques is that we were able to naturally extend all our results to iterated random covering graphs (random coverings of random coverings of...), for the first time showing their similarities to random covering graphs and answering a question raised by [**Wit**, **2010**]. The main contribution of this work is methodological and we think that algebraic techniques similar to the ones in this thesis could be used widely in the study of random covering graphs.

After developing the necessary ideas, we will put our new results pertaining to random covering graphs into proper context in Chapter 2.2. We discuss the relevance of the results about groups and topological applications in Chapters 4 and 7 respectively. The contents of this thesis are as follows:

Chapter 1
We introduce topological covering spaces and covering graphs, and discuss their basic properties.

Chapter 2
We present the Amit-Linial model for random covering graphs and prove its equivalence to a simpler model. We situate our new results and techniques for random covering graphs.

Chapter 3
We provide a new generalization of the Amit-Linial model to *iterated* random coverings using wreath products of symmetric groups.

Chapter 4
We prove results in group theory which are needed for our theorems in the following chapters. The probability with which the subgroup generated by two random permutations is the whole symmetric group or the alternating group is studied in [**Dix**, **1969**] and [**Bab**, **1989**]. We make minor modifications to some of their theorems to do the same for the case of l random permutations where $l \geq 2$. We prove a crucial first step in further generalizing this result to wreath products of symmetric groups.

Chapter 5
We define the walk-subgroup of a covering graph. We show a simple application of the walk-subgroup by using it to calculate the probability of connectivity in random coverings. We improve a result of [**AL**, **2006**] showing a lower bound on the edge expansion of random coverings. We provide a lower bound on the probability that

a random n-covering of a simple connected graph G with minimum degree δ is δ-connected. We also show that even allowing for all simple connected graphs with minimum degree growing slowly enough as a function of n and the number of vertices in the base graph, random coverings remain asymptotically almost surely δ-connected.

Chapter 6

We extend all the results for random coverings to iterated random coverings.

Chapter 7

We show the existence of homotopy invariants in random covering graphs, i.e. properties whose probability only depends on the homotopy type of the base graph. We extend some of our results to a highly studied model of random regular graphs.

Chapter 8

We offer some thoughts on the new techniques and mention some future applications.

Background

The main background we assume for the proofs is basic graph theory and some group theory. The material in Chapters 1 and 7 requires familiarity with algebraic topology which may be found in Hatcher's textbook [**Hat**, **2002**], while Chapter 4-6 require some knowledge of (transitive/primitive etc.) permutation groups which can be found in the text by Dummit and Foote [**DF**, **1984**]. The work pertaining to new results is self-contained, and written to be of interest to a wide audience of computer scientists and mathematicians.

CHAPTER 1

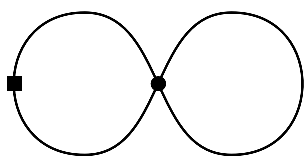
Covering Spaces and Covering Graphs

Covering graphs are a special case of covering spaces from topology. In this thesis we will often view covering graphs as combinatorial objects which are completely described by finite permutation groups. This perspective is ideal for many applications. However, the heart of the theory of covering graphs lies in topology, and in Chapter 7 we will need to view them as topological spaces in order to obtain some of our most elegant results. With this is mind, we will postpone the combinatorial description of covering graphs to the next chapter and introduce them by analogy to topological covering spaces. A complete treatment of covering spaces may be found in [**Hat**, **2002**]. We will need the following notions:

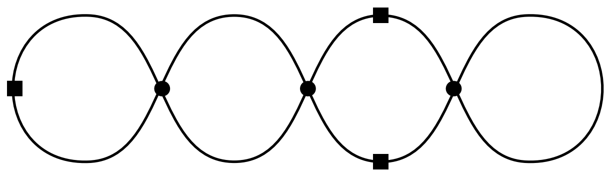
DEFINITION 1.1 (Graph Homomorphism). *We write $\underline{V(G)}$ for the vertices and $\underline{E(G)}$ for the edges of a graph G. For two graphs G and H, a graph homomorphism from $G \to H$ is a pair of maps $\varphi_V : V(G) \to V(H)$ and $\varphi_E : E(G) \to E(H)$, such that if $e \in E(G)$ connects $v, u \in V(G)$, then $\varphi_E(e)$ connects $\varphi_V(v), \varphi_V(u) \in V(H)$.*

DEFINITION 1.2 (Covering Space). *A covering space of X is a space $\tilde{X}$ together with a surjective continuous map $\pi : \tilde{X} \to X$ such that any point $x \in X$ belongs to an open neighborhood U for which $\pi^{-1}(U) = \bigcup_i U_i$, where $U_i \cap U_j = \emptyset$ if $i \neq j$ and the U_i are homeomorphic to U for all i.*

Instead of referring to $\tilde{X}$ as a covering space of X, it is also common to refer to X as the base space for $\tilde{X}$. The neighborhood U in the definition is called an *evenly-covered* neighborhood, and the U_i form the *sheets* of the *fiber* of U in $\tilde{X}$. The map π may be called a *covering map* or *covering projection.* In a sense, covering spaces are locally homeomorphic stacks of their base space. They capture the relationship between a sheet of paper and a book.



(a)



(b)

FIGURE 1.1. 1(b) is a two sheeted covering space of 1(a). The fibers of the two marked points of 1(a) has been illustrated in 1(a).

We define covering graphs analogously,

DEFINITION 1.3 (Covering Graph). *A covering graph of G is a graph $\tilde{G}$ together with a graph homomorphism $(\pi_V : V(\tilde{G}) \to G, \pi_E : E(\tilde{G}) \to G)$ where π_E is surjective. Moreover, given any $v, u \in V(G)$: for every point $v' \in \pi_V^{-1}(v)$, there is a bijection between set of edges connecting v' to a point in $\pi_V^{-1}(u)$ and the set of edges connecting v to u.*

The preimage of any vertex or edge in the base graph is called its *fiber*. Another way to thing about this definition is the following: if an edge connects v to u in the base graph, the fiber of the that edge defines a perfect matching between the fibers of v and u in the covering graph. This will become clear from the proof of Proposition 1.5.

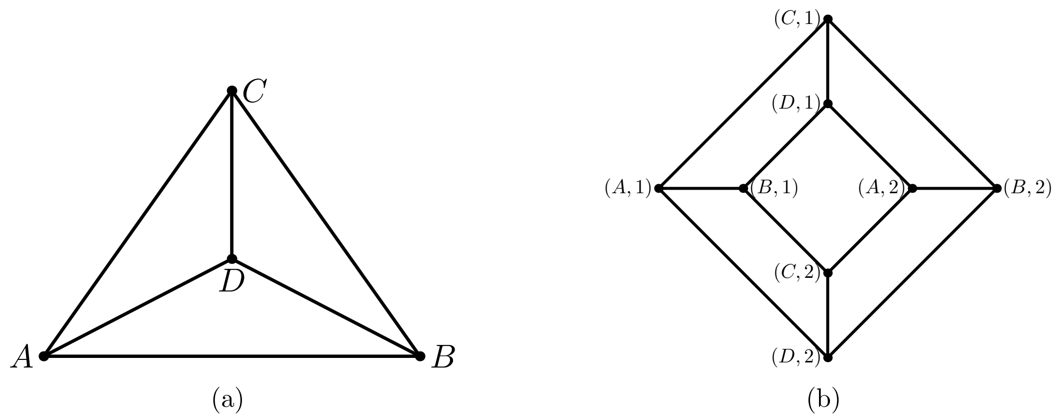


FIGURE 1.2. 2(b) is a two sheeted (or degree two) cover of 2(a). The fiber of each vertex has two points which are further indexed by the set $\{1, 2\}$.

Now we mention some basic properties of covering spaces and prove their analogs for covering graphs.

PROPOSITION 1.4 (Degree of a Covering Space). *Let $\tilde{X}$ be a covering space of some path-connected space X. Then the number of sheets in the fiber of any evenly-covered set of X is equal.* □

PROPOSITION 1.5 (Degree of a Covering Graph). *Let $\tilde{G}$ be a covering graph of a connected graph G. Then the number of points in the fiber of any vertex or edge is equal.*

PROOF. Take $e \in E(G)$ which connects $v, u \in V(G)$. Let F_v, F_u and F_e be the fibers of v, u and e respectively. For any point in $v' \in F_v$, the edges incident to it in $\tilde{G}$ are in bijection with the edges incident to v in G, so there is only one edge incident to v' with image e under the covering projection. Moreover, by the definition of covering this bijection is adjacency preserving which tells us that every edge in F_e is incident to a vertex in F_v. Together, these two observations show a bijection between F_v and F_e. Similarly, we may construct a bijection between F_e and F_u. We may reapply this argument along all paths G, and since G is connected, the proposition follows. □

One of the most useful properties of covering spaces is the following *homotopy lifting property*. Its analog for covering graphs will be a central ingredient in many of the proofs to come.

PROPOSITION 1.6. *Given a covering space $\pi : \tilde{X} \to X$, a homotopy $\varphi_t : Y \to X$ with $t \in [0,1]$, and a map $\tilde{\varphi}_0 : Y \to \tilde{X}$ such that $\pi(\tilde{\varphi}_0) = \varphi_0$, there exists a unique homotopy $\tilde{\varphi}_t : Y \to \tilde{X}$ of $\tilde{\varphi}_0$ such that $\pi(\tilde{\varphi}_t) = \varphi_t$. In particular, if we take Y to be a single point, then we see that any path p starting at $x \in X$ gives us unique paths starting at each point of $\pi^{-1}(x)$, each of whose image under π is p.* □

Colloquially, we say that any path starting at $x \in X$ *lifts* to a unique path starting at each point of $\pi^{-1}(x)$ in $\tilde{X}$.

PROPOSITION 1.7 (Walk Lifting Property of Covering Graphs). *Let $\tilde{G} \to G$ be a n-degree covering graph with respect to the covering projection (π_V, π_E). Given a walk $W = w_1, \ldots, w_n$, where the $w_i \in E(G)$, which starts at the vertex v in G and a point $v' \in \pi_V^{-1}(v)$, there is a unique walk $w'_1, \ldots, w'_n$ starting at v' such that its image under the projection map is $w_1, \ldots, w_n$. In particular, W lifts to n edge disjoint walks in the covering graph, each starting at a point in $\pi_V^{-1}(v)$.*

PROOF. Once we specify $v' \in \pi_v^{-1}(v)$, by definition of the covering there is only one w'_1 in the fiber of w_1 starting at v' such that $\pi_E(w'_1) = w_1$, and it connects v' to a point in the fiber of its end point in G. The same argument can be applied for the rest of the walk. This gives us n walks which are lifts of W, one starting at each point in $\pi_V^{-1}(v)$. These walks are edge disjoint for the following reason: if there e connects x to y in the base graph, then in the covering graph, the edges in the fiber of e form a perfect matching between the fibers of x and y, so lifts of e cannot take two distinct points in the fiber of x to the same point in the fiber of y. □

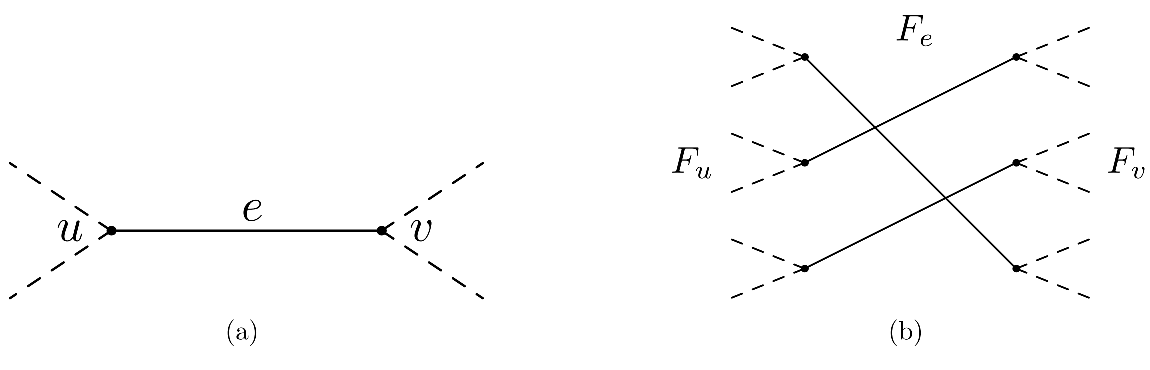


FIGURE 1.3. 3(b) illustrates the fibers of the vertices and edges of 3(a) in a degree 3 covering graph. In particular, notice that two edges in the fiber of e cannot collide in the fiber of v, which results in the edge disjoint walk lifting property.

Note that $\tilde{G}$ has at most as many *closed* walks as G, because a closed walk starting at $v' \in \pi_v^{-1}(v)$ in $\tilde{G}$ projects to a closed walk in G starting at v. In fact, a covering projection $p : \tilde{X} \to X$ induces an injective homomorphism of fundamental groups $p_* : \pi_1(\tilde{X}) \to \pi_1(X)$. There is a beautiful topological theory of covering graphs that can be developed from here. One may describe the automorphism groups of covering graphs, their fundamental groups, and even prove several results about free groups more elegantly than through other techniques. For example, it is possible to prove that a subgroup of a free group is free with only a little more work than what we have presented. However, we will move on to the combinatorial view of covering graphs in pursuit of our main theorems, before coming back to topology in Chapter 7. We mention one last fact which holds for coverings spaces and covering graphs, which will be useful for our discussion of iterated random coverings:

PROPOSITION 1.8. *The composition of finite degree covering projections is a covering projection. The degree of the composition of finite degree covering projections is multiplicative.* □

In accordance with the language of covering spaces, we will use *covering* to refer to entire covering graphs and *lift* to refer to an element in the preimage of a vertex, edge or walk under the covering projection.

CHAPTER 2

Random Covering Graphs

1. A Modified Amit-Linial Model

In this section we will discuss the model of random labeled n-coverings of graphs introduced by [**AL**, **2002**] and also develop an equivalent and more convenient model of random labeled n-coverings which will be the standard for the remainder of thesis. This simplified model has been mentioned by [**AL**, **2002**], but we develop it carefully as we use it extensively in our work. Before doing so, we must make a connection between covering graphs and groups by realizing them as the derived graphs of *voltage assignments*.

DEFINITION 2.1 (Voltage Assignment). *Given a graph G = (V,E) and a permutation group $\mathcal{G}$ (we denote the domain of the permutation action by S), a voltage assignment of G to $\mathcal{G}$ is a map $\varphi : E(G) \to \mathcal{G}$.*

A voltage assignment can be used to construct a derived graph in the following way,

DEFINITION 2.2. *Given a graph G with oriented edges and a voltage assignment $\varphi : G \to \mathcal{G}$, the derived graph of (G, φ), which we denote G^φ, has the vertex set $\{v\} \times S$ for all $v \in G$. The vertices (v, s_1) and (u, s_2) in G^φ are connected if and only if v is connected to u in G (say by edge e), and $\varphi(e)(s_1) = s_2$. The edge orientations are removed from the resultant graph.*

DEFINITION 2.3 (Section). *Every vertex in such a derived graph is labeled by a vertex of the base graph and an element of S. All vertices labeled by the same element of S are collectively referred to as a section of the derived graph.*

LEMMA 2.4. *Given a graph G and a voltage assignment $\varphi : G \to \mathcal{G}$, let G^φ be its derived graph. Then G^φ is a covering graph of G.*

PROOF. We need a pair of maps $\pi_V : V(G^\varphi) \to V(G)$ and $\pi_E : E(G^\varphi) \to E(G)$ which together define a covering projection. Define $\pi_V : (v, s) \mapsto v$ for all $v \in V(G)$ and $s \in S$. Let π_E be the map which sends an edge connecting (v, s_1) to (u, s_2) to an edge connecting v to u, for each $v, u \in V(G)$ and $s_1, s_2 \in S$. To see that (π_V, π_E) together define a graph homomorphism, notice that if e connects (v, s_1) to (u, s_2) then by definition $\pi_E(e)$ connects $\pi_V(v)$ to $\pi_V(u)$. This is clearly a surjective graph homomorphism. Finally, since $\mathcal{G}$ is a permutation group acting on S, we see that there is a bijection between the edges connecting v to u in G, and the edges connecting (v, s) to some (u, s') in G^φ for each $s \in S$ and each $u, v \in V(G)$, so that (π_V, π_E) is indeed a covering projection. □

We now present a result of [**GT**, **1987**], which shows that every n-degree covering graph of G can be obtained as the derived graph of a voltage assignment where we take $\mathcal{G} = \mathcal{S}_n$, the symmetric group on n elements acting canonically on the set $\{1, \ldots, n\}$.

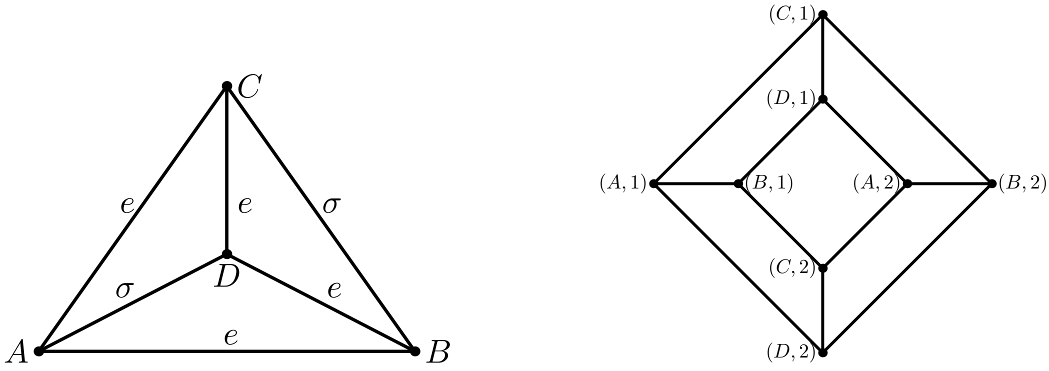
THEOREM 2.5 (Gross-Tucker). *Let H be an n-degree covering graph of G. Then there is a voltage assignment $\varphi : E(G) \to \mathcal{S}_n$ such that G^φ is isomorphic to H. In fact, given a spanning tree T of G, we may even impose the condition $\varphi(e) = id$ for any subset of edges of T.*

PROOF. Choose a spanning tree T of G and pick a root vertex in this tree, v. We assign orientations to every edge of G in the following way: assign a positive orientation to every edge in T and an arbitrary orientation to every other edge. Then we assign orientations to the edges of H so that the covering projection $(\pi_V : V(H) \to V(G), \pi_E : E(H) \to E(G))$ is direction preserving (these orientations will not be of importance once the derived graph is constructed, and can be forgotten at that point).

The preimage of $v \in V(G)$ denoted by $\pi_V^{-1}(v)$, has n points. Label them $(v, 1), \ldots, (v, n)$ arbitrarily. Choose an edge e of T in G which starts at v and terminates at some vertex, call it u. Since (π_V, π_E) is a covering projection, $\pi_E^{-1}(e)$ must consist of n edges of H with each originating at a distinct vertex (v, i). Label them so that (e, i) originates from (v, i). Label the vertices in $\pi_V^{-1}(u)$ as $(u, 1), \ldots, (u, n)$ in any arbitrary way. The n edges in $\pi_E^{-1}(e)$ define a bijection between $(v, 1), \ldots, (v, n)$ and $(u, 1), \ldots, (u, n)$. This bijection, call it σ, can be viewed as an element of $\mathcal{S}_n$, and we define $\varphi(e) = \sigma$. We continue this procedure until all edges of T have been assigned voltages from $\mathcal{S}_n$, keeping in mind to always select the next vertex of T so that its initial point is the end point of a path in which every edge has already been assigned a voltage. Since we are completely free to choose the labeling of each fiber, we may choose it so that the voltage assigned to any subset of edges of T is the identity permutation, by for example, labeling the end point of (e, i) as (u, i) for each i.

Now we need to assign voltages to all the edges not in T. Suppose f is such an edge which connects s to t. By definition $\pi_E^{-1}(f)$ can be viewed as a matching between $\pi_V^{-1}(s)$ and $\pi_V^{-1}(t)$. Since $\pi_V^{-1}(s)$ and $\pi_V^{-1}(t)$ have already been labeled in the assignment of voltages to T, this matching can be viewed as permutation τ according to the labels. Define $\varphi(f) = \tau$. Repeat this process till the voltage assignment is completely defined. Removing the orientations from the edges of the derived graph G^φ yields a graph isomorphic H by construction. $\square$

We can now revisit the example of covering graphs we saw in Figure 1.2.



(a) (b)

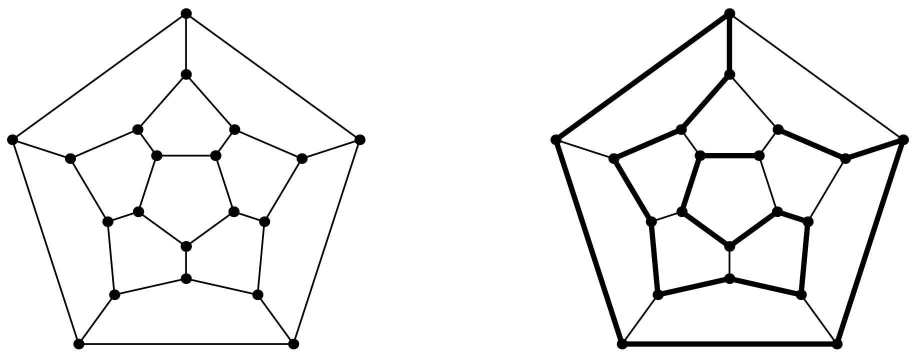
Figure 2.1. If e is the identity element of $\mathcal{S}_2$ and σ the transposition, then 1(b) is the derived graph of the voltage assignment shown in 1(a).

We may now define the model of random labeled n-coverings, $L_n(G)$, introduced by [**AL**, **2002**].

Definition 2.6 ($L_n(G)$). *Given a graph G with unoriented edges, a labeled n-covering is the derived graph of G and a voltage assignment with voltages in $\mathcal{S}_n$ (we assign an arbitrary orientation to the edges of G for purposes of construction, but these are removed in the derived graph). We use $\underline{L_n(G)}$ to refer to the set of all labeled n-coverings, as well the uniform distribution on this set. A graph in $L_n(G)$ is called a random labeled n-covering of G. Put another way, a random labeled n-covering of G is the derived graph of G, together with a random voltage assignment in $\mathcal{S}_n$: which independently assigns every edge of G a randomly chosen permutation from $\mathcal{S}_n$.*

We clarify that this is a random model for *labeled* covering graphs in the following sense: G is assumed to have a fixed labeling, and every point in the fiber of a vertex of G inherits a label from its initial point, and each fiber is further indexed by the set $\{1, \ldots, n\}$. Random graph models are usually defined for labeled graphs. By the Gross-Tucker theorem $L_n(G)$ contains a labeled graph isomorphic to every n-degree covering of G. Since each graph in $L_n(G)$ is the derived graph of a voltage assignment of the edges of G to elements of $\mathcal{S}_n$, clearly the number of graphs in $L_n(G)$ is just the number of possible voltage assignments, which is $(n!)^{|E(G)|}$. We define an alternate model for random labeled n-coverings of G.

Definition 2.7 ($L_n^T(G)$). *Given a graph G with unoriented edges, a subset S of $E(G)$ which does not contain a cycle, and an ordering of the edges of G, we extend S to a spanning tree T using Kruskal's algorithm and orient all edges of T to be positive. We use $\underline{L_n^T(G)}$ to refer to a subset of all labeled n-coverings given by restricting to voltage assignments which send the every edge of T to the identity permutation, as well the uniform distribution on this subset. In this model, a random labeled n-covering can be thought of as the derived graph produced by arbitrarily orienting the edges of $G - T$ and* *making a random voltage assignment in $\mathcal{S}_n$ to these edges, whereas the edges of T are always assigned the identity permutation.*



(a) (b)

FIGURE 2.2. If thin edges are assigned random permutations and thick edges are assigned the identity permutation, then the derived graph of the assignment in 2(a) is in $L_n(G)$ and the that of 2(b) is in $L_n^T(G)$.

Again by the Gross-Tucker theorem we see that $L_n^T(G)$ contains a labeled graph isomorphic to every n-degree covering of G. The number of graphs in $L_n^T(G)$ is $(n!)^{|E(G)|-|T|}$ since we restrict the possible voltage assignments.

DEFINITION 2.8. *A graphical property is a property of graphs which does not depend on the labeling of a graph, only its structure. Formally, if G has the graphical property $\mathcal{P}$, then any G' isomorphic to G also has property $\mathcal{P}$. In particular, a set $\mathcal{C}$ of all graphs with graphical property $\mathcal{P}$ is a union of complete isomorphism classes of graphs.*

THEOREM 2.9 (Equivalence of $L_n(G)$ and $L_n^T(G)$). *The probability that a graph in $L_n(G)$ has property $\mathcal{P}$ is the same as the probability that a graph in $L_n^T(G)$ has the graphical property $\mathcal{P}$.*

PROOF. Let $\mathcal{M}_n(G)$ be the set of all n-degree covering graphs of G. We already know that both $L_n(G)$ and $L_n^T(G)$ contain labeled graphs isomorphic to each graph in $\mathcal{M}_n(G)$ (and indeed, each graph in $L_n(G)$ and $L_n^T(G)$ is isomorphic to some graph in $\mathcal{M}_n(G)$). Given H in $\mathcal{M}_n(G)$, we follow the proof of the Gross-Tucker theorem which contains a way to construct the derived graph (recall that these are labeled graphs) of a voltage assignment in the symmetric group which is isomorphic to H. We then count the number of redundant labeled graphs produced by this construction in two cases: first if we require the derived graph to be in $L_n(G)$, and second when we require the derived graph to be in $L_n^T(G)$.

In the construction of graphs in $L_n(G)$ isomorphic to H, we have complete freedom to label the vertices of T as we like. This can be seen through the proof of the Gross-Tucker theorem combined with the fact that $L_n(G)$ contains the derived graph of any possible voltage assignment. Obviously changing the labeling of the fibers of a covering graph does not change its isomorphism class. This shows us that by simply changing the labeling of the fibers, we may produce $(n!)^{|V(G)|}$ distinct labeled graphs isomorphic to H in $L_n(G)$. We call this set of graphs the canonical family of H in $L_n(G)$. Note that if H' in $\mathcal{M}_n(G)$ is distinct from H as a covering graph of G (indeed, H' may even be isomorphic to H as a covering of G), then their canonical families in $L_n(G)$ are disjoint since they are sets of labeled graphs. To clarify this point, suppose that there is a graph K in the intersection of their canonical families. This means that adding additional labels to the fibers of H and H' can create the same graph K, so obviously H and H' must be identical to begin with.

However, in the construction of graphs in $L_n^T(G)$ isomorphic to H, we do not have complete freedom to label the vertices of T. This is because $L_n^T(G)$ only contains graphs of voltage assignments which send edges of T to the identity permutation. Indeed, any vertex which is the end point of an edge in T has its labeling completely determined by its initial point. This results in only $(n!)^{|V(G)|-|T|}$ distinct labeled graphs in the canonical family of H in $L_n^T(G)$. The same argument as the previous case shows that canonical families of distinct graphs are disjoint. Now let $\mathcal{C}$ be the subset of graphs in $\mathcal{M}_n(G)$ which have the graphical property $\mathcal{P}$. Any graph in $L_n(G)$ $[L_n^T(G)]$ which has property $\mathcal{P}$ must be in the canonical family of some graph of $\mathcal{C}$ in $L_n(G)$ $[L_n^T(G)]$ because $\mathcal{C}$ is a complete set of graphs in $\mathcal{M}_n(G)$ which have property $\mathcal{P}$. Finally, since canonical families contain graphs of the same isomorphism type we get

$$\text{Prob(A graph in } L_n(G) \text{ has property } \mathcal{P}) = \frac{|\mathcal{C}|(n!)^{|V(G)|}}{(n!)^{|E(G)|}}$$

and similarly

$$\text{Prob(A graph in } L_n^T(G) \text{ has property } \mathcal{P}) = \frac{|\mathcal{C}|(n!)^{|V(G)|-|T|}}{(n!)^{|E(G)|-|T|}} = \frac{|\mathcal{C}|(n!)^{|V(G)|}}{(n!)^{|E(G)|}}$$

from which the theorem follows. □

From this point on we will use the notation $L_n(G)$ to refer to the random model of n-degree coverings even if every edge in an acyclic set of edges of G is assumed to have the identity permutation associated to it. We adopt this convention since we are only concerned with probabilities of graphical properties.

2. Summary and Context of New Results

Random coverings of graphs have been extensively studied. Work on expansion properties, connectivity, independence numbers, chromatic numbers, hamiltonicity and perfect matchings can be found in [**AL**, **2002**], [**Fri**, **2003**], [**AL**, **2006**], [**BL**, **2006**], [**LR**, **2005**], [**LWW**, **2015**] and [**ALM**, **2002**] amongst many others. Here, we will situate this thesis by providing the context for our new results.

2.1. Connectivity Properties. It is well known that random coverings of connected graphs which are not trees are asymptotically almost surely (a.a.s.) connected. In fact, a much stronger notion of connectivity holds in the following way:

THEOREM 2.10 ([**AL**, **2002**]). *Let G be a simple connected graph with minimum degree $\delta \geq 3$. Then with probability $1 - o_n(1)$, a random n-covering of G is δ-connected.*

They ask whether this probability can be estimated as a function of n, and this question has also been raised by [**Wit**, **2010**]. We first compute the probability of connectivity, and then show an explicit lower bound on the probability of δ-connectivity. So far the literature on δ-connectivity in random covering graphs has been restricted to fixed δ unlike that of other random models of graphs. The result of [**AL**, **2002**] ties together well with the case of $G_{n,d}$ (the model of random d-regular graphs on n vertices with the usual assumption that dn is even) where it is a classical result of [**Bol**, **1981**] that as $n \to \infty$, for fixed $d \geq 3$, $H \in G_{n,d}$ is almost surely d-connected. However, it is also known due to [**Luc**, **1992**] that $H \in G_{n,d}$ is a.a.s. d-connected even if we only assume $3 \leq d(n) \leq n^{.02}$. That is to say, we may allow d be grow slowly as a function of n. We prove an analog of this result for random coverings of graphs, providing a more robust description of their connectivity.

2.2. Edge Expansion. The edge expansion (cf. Chapter 5.3) of random coverings can be lower bounded as a function of the base graph in the following way,

THEOREM 2.11 ([**AL**, **2006**]). *Let G be a connected graph with $|E| > |V|$. Then there is a positive constant $\xi_0(G)$, such that a.a.s. a random covering of G has expansion $\xi_0(G)$.*

We improve this result by calculating the probability and mildly raising the lower bound. The study of expansion properties of random coverings has a vast literature, with much of it relying on spectral graph theory and the *trace method* introduced by [**Fri**, **2003**]. The author demonstrates that covering graphs cannot have better expansion than their base graph because they inherit every eigenvalue of their base graph, but showed that a.a.s. the new eigenvalues are bounded by $D^{1/2}\rho^{1/2} + o(1)$, where D is the largest eigenvalue of the base graph and ρ the spectral radius of its universal cover. This bound has been improved several times since then, and in fact, Friedman's conjecture states that the bound should be $\rho + o(1)$. These results use the trace method along with the analysis of word maps and fixed points of permutations. It is possible that our method of studying covering graphs through permutation groups yields new results in this direction.

2.3. 'Relative' Random Graphs. In [**FKS**, **1989**] it is shown that random regular graphs are a.a.s. good expanders (specifically, ν-weakly Ramanujan). [**Fri**, **2003**] showed a 'relative' version of this result for random covering graphs which proves that random covering graphs are a.a.s. '*weakly*-relative expanders'. That is to say, their expansion is only slightly worse than perfect, relative to the expansion properties of the starting point in the random construction. For example, a.a.s. a random covering of a Ramanujan graph is *weakly*-Ramanujan. We extend this notion of random coverings as 'relative' random regular graphs in two ways. First, we show that a relative version of Luczak's theorem for d-connectivity in random regular graphs for $3 \leq d \leq n^{.02}$ holds for random coverings. It is relative in the sense that we must account for the size of the base graph as well as the degree of the covering. Second, we show the existence of homotopy invariants in random covering graphs in the following sense: the probability that random covering graphs have certain properties depends only on the homotopy type of the base graph. These results in particular extend the current understanding of how random coverings inherit structure from their base graph.

2.4. Iterated Random Coverings. [**AL**, **2002**] and [**Wit**, **2010**] mention the possibility of extending the known results for random coverings to iterated random coverings. Iterated coverings have been constructed and studied by [**Mak**, **2015**], however, no *random* model for iterated coverings has been published yet. We develop such a model and extend all our results to it, which for the first time shows that iterated random coverings have similar structural properties to random coverings.

CHAPTER 3

Iterated Random Covering Graphs

Notice that if $G_k \to G_{k-1} \to \cdots \to G_1 \to G$ is a sequence of covering maps of degree $n_k, \ldots n_1$ respectively, then G_k is an $n_k n_{k-1} \ldots n_1$ cover of G. However a random covering of degree n_2 of a random covering of degree n_1 of G is not a *random* covering of G. That is to say it is distributed differently than a covering produced by a random voltage assignment of elements of $\mathcal{S}_{n_1 n_2}$ to edges of G. In particular one may notice that most random coverings of degree $n_1 n_2$ have probability zero in the iterated construction. In order to extend the model for random covering graphs to iterated random covering graphs, we must first develop wreath products of groups. We will show that iterated random coverings are the derived graphs of random voltage assignments in wreath products of symmetric groups.

1. Semidirect Products and Wreath Products

We describe iterated wreath products in two ways. The first is purely algebraic and the second relies on an intuitive interpretation of wreath products as automorphism groups of rooted trees. The following two sections follow the work of [**Mak**, **2015**]. Given a group $\mathcal{H}$ and a surjective group homomorphism $\beta : \mathcal{K} \to \mathcal{H}$, we call $\mathcal{K}$ an *extension* of $\mathcal{H}$ by $\ker(\beta) \cong \mathcal{G}$. Put another way, all extensions of $\mathcal{H}$ by $\mathcal{G}$ are the possibilities for $\mathcal{K}$ in the following short exact sequence of groups

$$1 \to \mathcal{G} \xrightarrow{\alpha} \mathcal{K} \xrightarrow{\beta} \mathcal{H} \to 1$$

For example, we may take $\mathcal{K} = \mathcal{G} \times \mathcal{H}$ along with the maps $\alpha(x, 1) = (x, 1)$ and $\beta(1, y) = (1, y)$, which gives us the familiar direct product as an extension. An extension is said to be *split* if there is a homomorphism $\gamma : \mathcal{H} \to \mathcal{K}$ such that $\beta \circ \gamma = id_{\mathcal{H}}$. In the case when $\gamma(\mathcal{H})$ is a normal subgroup of $\mathcal{K}$, the only possibility for $\mathcal{K}$ is the direct product $\mathcal{G} \times \mathcal{H}$. However, if we drop the assumption that $\gamma(\mathcal{H})$ is a normal subgroup we generate more possibilities for extensions of $\mathcal{H}$ by $\mathcal{G}$, these are denoted by $\mathcal{G} \rtimes \mathcal{H}$, a *semidirect product* of $\mathcal{H}$ and $\mathcal{G}$.

Definition 3.1. *Given a group $\mathcal{G}$ and a group $\mathcal{H}$, along with a homomorphism $\varphi : \mathcal{H} \to Aut(\mathcal{G})$, we define the* <u>*semidirect product $\mathcal{G} \rtimes_\varphi \mathcal{H}$*</u> *to be the set $\mathcal{G} \times \mathcal{H}$ with the group operation*

$$(g_1, h_1) \cdot (g_2, h_2) = (\varphi_{h_2}(g_1) g_2, h_1 h_2)$$

and the identity $(1_{\mathcal{G}}, 1_{\mathcal{H}})$. *In particular we see that semidirect products of* $\mathcal{G}$ *and* $\mathcal{H}$ *are in a one to one correspondence with the possibilities for* φ.

DEFINITION 3.2. *Given two permutation groups* $\mathcal{G}$ *and* $\mathcal{H}$ *with permutation actions on sets* T *and* S *respectively, the* wreath product of $\mathcal{G}$ and $\mathcal{H}$, *denoted* $\mathcal{G} \wr \mathcal{H}$, *is the semi-direct product* $\mathcal{G}^{|S|} \rtimes \mathcal{H}$, *where the action of* $h \in \mathcal{H}$ *on* $\mathcal{G}^{|S|}$ *is defined to be* $\varphi_h(g_1, g_2, \ldots, g_{|S|}) = \varphi(g_{h(1)}, g_{h(2)}, \ldots, g_{h(|S|)})$.

Define the natural (and faithful) action of $\mathcal{G} \wr \mathcal{H}$ on the set $T \times S$ in the following way: given $(\mu, \pi) \in \mathcal{G} \wr \mathcal{H}$ where $\mu \in \mathcal{G}^{|S|}$ and $\pi \in \mathcal{H}$ and $(t, s) \in T \times S$, $(\mu, \pi)(t, s) = (\pi(t), \mu_t(s))$. Details that this is indeed a faithful action can be checked easily.

The wreath product of more than two groups is similar, although notationally more involved. Let $\mathcal{G}_k, \ldots, \mathcal{G}_1$ be permutation groups with actions defined on sets $N_k, \ldots, N_1$ respectively. The iterated wreath product $\mathcal{G}_k \wr \cdots \wr \mathcal{G}_1$ is the semidirect product $\mathcal{G}_k^{\prod_{i=i}^{k-1} |N_i|} \rtimes \mathcal{G}_{k-1}^{\prod_{i=1}^{k-2} |N_i|} \rtimes \cdots \rtimes \mathcal{G}_2^{N_1} \rtimes \mathcal{G}_k$. The action of $(g_i, \ldots, g_1) \in \mathcal{G}_i \wr \cdots \wr \mathcal{G}_1$ (note that $g_j \in \mathcal{G}_j^{\prod_{i=1}^{j-1} |N_i|}$) on $\mathcal{G}_{i+1}^{\prod_{j=1}^{i} |N_j|}$ is described as follows: similar to the wreath product of two groups, $\mathcal{G}_i \wr \cdots \wr \mathcal{G}_1$ acts on $N_i \times \cdots \times N_1$ by $(g_i, \ldots, g_1)(n_i, \ldots, n_1) = (g_{i_{(n_{i-1}, \ldots, n_1)}}(n_1), \ldots, g_1(n_1))$. This in turn, defines the action of $(g_i, \ldots, g_1)$ on $\mathcal{G}_{i+1}^{\prod_{j=1}^{i} |N_j|}$ the same way as Definition 3.2 by simply noting that indexing set of the domain of the action changes from S to $N_i \times \cdots \times N_1$.

2. Wreath Products Through Rooted Trees

We will closely follow the excellent exposition of wreath products through rooted trees and their relation to covering graphs found in [**Mak**, **2015**].

DEFINITION 3.3. *Define* $T_{S_1, \ldots, S_n}$ *to be the rooted tree on* n *levels such that every node which is* $i < n$ *levels away from the root has children labeled by the set* S_{i+1}. *In particular, the root has* $|S_1|$ *children and there are a total of* $\prod_{i=1}^{n} |S_i|$ *leaves.*

Note that we can describe a vertex which is i levels away from the root by an element of $S_1 \times \cdots \times S_i$, with $(s_1, \ldots, s_i) \in S_1 \times \cdots \times S_i$ representing the s_ith child of the s_{i-1}th child of the ... s_1th child of the root. In particular every leaf can be described by an element in $S_1 \times \cdots \times S_n$. By convention we refer to the root as $()$. Any automorphism of such a tree must send every level of the tree bijectively to itself, but it must also preserve the parent-child relationship amongst nodes, meaning that we can only permute children of a common parent amongst themselves. Therefore, any automorphism of $T_{S_1, \ldots, S_n}$ can be described by assigning to each vertex $(s_1, \ldots, s_i)$ (note that this is at distance i from the root) an element $\pi_{s_1, \ldots, s_i}$ of the symmetric group on $|S_{i+1}|$ elements, according to which its children are permuted. The automorphism can be defined as

$$\varphi(s_1, \ldots, s_i) = (\pi_{()}(s_1), \ldots, \pi_{s_1, \ldots, s_{i-1}}(s_i))$$

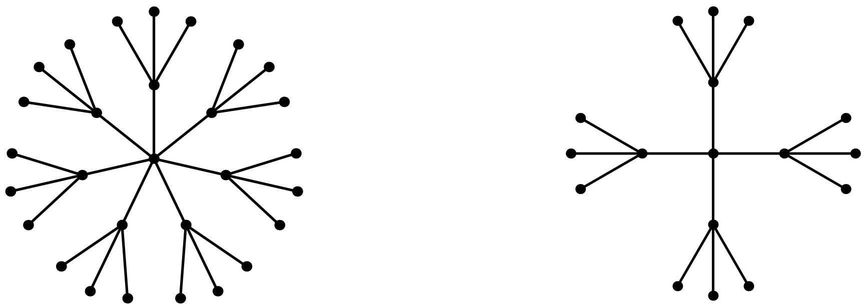


FIGURE 3.1. The automorphism group of 1(a) is $\mathcal{S}_3 \wr \mathcal{S}_7$ and the automorphism group of 1(b) is $\mathcal{S}_3 \wr \mathcal{S}_4$

For our applications, we will not be usually be working with the entire automorphism group of $T_{S_1,\ldots,S_n}$, but rather automorphism groups in which children of $(s_1, \ldots, s_i)$ will be permuted under the action of $\mathcal{G}_{i+1}$, a subgroup of the symmetric group on $|S_{i+1}|$ elements. In our treatment of covering graphs, these $\mathcal{G}_i$ will be subgroups of symmetric groups generated by random permutations.

LEMMA 3.4. *The automorphism group of $T_{S_1,\ldots,S_n}$ generated by the action of $\mathcal{G}_{i+1}$ on $(s_1, \ldots, s_i)$ is $\mathcal{G}_n \wr \cdots \wr \mathcal{G}_1$. It is a permutation group on on the set of leaves, which may be indexed by $S_1 \times \cdots \times S_n$.*

PROOF. The proof may be found in Appendix B. $\square$

PROPOSITION 3.5. *Suppose we have a sequence of covering graphs $G_n \to \cdots \to G_1 \to G$ where each G_i is obtained from its predecessor by a voltage assignment to a group of permutations $\mathcal{H}_i$ acting on a set S_i. Note that the degree of G_i as a cover of its predecessor is $|S_i|$. Then G_n is the derived graph of a voltage assignment of G to elements of $\mathcal{H}_n \wr \cdots \wr \mathcal{H}_1$ where the domain of their action is $S_1 \times \cdots \times S_n$. Conversely, any covering of graphs $G_n \to G$ which is the derived graph of a voltage assignment of $\mathcal{H}_n \wr \cdots \wr \mathcal{H}_1$ (with the action defined on on $S_1 \times \cdots \times S_n$) is an iterated covering as described above.*

PROOF. The proof may be found in Appendix B. $\square$

3. The Model: $L_{n_k \ldots n_1}(G)$

We may now construct random labeled iterated $(n_k, \ldots, n_1)$-coverings of graphs.

COROLLARY 3.6 (Gross-Tucker Theorem for Iterated Coverings). *Suppose we have a sequence of covering graphs $G_k \to \cdots \to G_1 \to G$ of degrees $n_k, \ldots, n_1$ respectively. Then G_k is the derived graph of a voltage assignment of G to elements of $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ (acting on $N_1 \times \cdots \times N_k$). Furthermore, given a spanning tree T of G we may even impose the condition that any fixed subset of edges in T is assigned the trivial voltage. Conversely,* *any covering of graphs $G_n \to G$ which is the derived graph of a voltage assignment from $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ (acting on $N_1 \times \cdots \times N_k$) is an iterated covering as described above.*

PROOF. This proof follows immediately from the original Gross-Tucker theorem combined with Proposition 3.5 where the $\mathcal{H}_i$ are taken to be $\mathcal{S}_{n_i}$. $\square$

DEFINITION 3.7 ($L_{n_k\ldots n_1}(G)$). *Given a graph G with unoriented edges, a labeled iterated $(n_k, \ldots, n_1)$-covering is the derived graph of G and a voltage assignment with voltages in $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$. We use $\underline{L_{n_k\ldots n_1}(G)}$ to refer the set of all labeled iterated $(n_k, \ldots, n_1)$-coverings and also the uniform distribution on this set. A graph in $L_{n_k\ldots n_1}(G)$ is called a random labeled iterated $(n_k, \ldots, n_1)$-covering. It is useful to think of a random labeled n-coverings as the derived graph of G, and a random voltage assingment in $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$: which assigns a permutation from $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ independently and uniformly at random to each edge of G.*

Note that a random graph in $L_{n_2 n_1}(G)$ is a random graph in $L_{n_2}(H)$ for some H in $L_{n_1}(G)$. Also, by the Gross-Tucker theorem for iterated coverings, we know that $L_{n_k\ldots n_1}(G)$ contains a labeled graph isomorphic to any iterated $(n_k, \ldots, n_1)$-cover of G. We now define a more convenient yet equivalent model of random labeled iterated $(n_k, \ldots, n_1)$-coverings.

DEFINITION 3.8 ($L^T_{n_k\ldots n_1}(G)$). *Given a graph G with unoriented edges, a subset S of $E(G)$ which does not contain a cycle, and an ordering of the edges of G, we first extend S to a spanning tree T using Kruskal's algorithm and then orient all edges of T to be positive. We use $\underline{L^T_{n_k\ldots n_1}(G)}$ to refer to a subset of all labeled iterated $(n_k, \ldots, n_1)$-coverings given by restricting to voltage assignments which send T to the identity element, as well as the uniform distribution on this subset. In this model, a random labeled $(n_k, \ldots, n_1)$-covering can be thought of as the derived graph produced by arbitrarily orienting the edges of $G - T$ and making a random voltage assignment from $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ to these edges,whereas edges in T are assigned the identity element.*

By the Gross-Tucker theorem for iterated coverings, we know that $L^T_{n_k\ldots n_1}(G)$ contains a labeled graph isomorphic to any iterated $(n_k, \ldots, n_1)$-cover of G.

THEOREM 3.9 (Equivalence of $L_{n_k\ldots n_1}(G)$ and $L^T_{n_k\ldots n_1}(G)$). *The probability that a graph in $L_{n_k\ldots n_1}(G)$ has graphical property $\mathcal{P}$ is the same as the probability that a graph in $L^T_{n_k\ldots n_1}(G)$ has the graphical property $\mathcal{P}$.*

PROOF. This is essentially the same as the proof of Theorem 2.9 after the following observation: the number possible of labelings of the fiber of a vertex changes from $|\mathcal{S}_n| = n!$ to $|\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}|$. This allows us to observe at the appropriate stage in the proof

$$\text{Prob(A graph in } L_{n_k\ldots n_1}(G) \text{ has property } \mathcal{P}) = \frac{|\mathcal{C}|(|\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}|)^{|V(G)|}}{(|\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}|)^{|E(G)|}}$$

and similarly

$$\text{Prob(A graph in } L^T_{n_k \dots n_1}(G) \text{ has property } \mathcal{P}) = \frac{|\mathcal{C}|(|\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}|)^{|V(G)|-|T|}}{(|\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}|)^{|E(G)|-|T|}}$$

from which we get the theorem. □

Similar to our convention for $L_n(G)$ and $L^T_n(G)$, from this point we will use the notation $L_{n_k \dots n_1}(G)$ to refer to the random model of $(n_k, \dots, n_1)$-degree coverings even if a every edge in an acyclic set of edges of G is assumed to have the identity permutation associated to it.

CHAPTER 4

Group Theoretic Preliminaries

"Tout vient à point à qui sait attendre."

In Chapter 5 we will establish a natural relationship between random covering graphs and randomly generated subgroups of $\mathcal{S}_n$ on which we base most of our results. In this chapter we will prove results about randomly generated subgroups of $\mathcal{S}_n$ which are necessary for our main theorems. Any prerequisites for this chapter, such as definitions of transitive or primitive group actions or facts about $\mathcal{S}_n$ can be found in an accessible format in the textbook by Dummit and Foote [**DF**, **1984**].

1. The Generalized Dixon-Babai Theorem

Given two random elements σ, τ of $\mathcal{S}_n$, it is natural to ask what subgroup of $\mathcal{S}_n$ they generate. It is easy to see that if σ, τ are both even permutations, they can only generate even permutations, and therefore cannot generate any subgroup of $\mathcal{S}_n$ bigger than $\mathcal{A}_n$. This happens with probability $\frac{1}{4}$. So we cannot hope to say that two random elements a.a.s. generate the whole of $\mathcal{S}_n$. However, aside from this complication the best possible result is indeed true. [**Dix**, **1969**] showed that the probability that two random elements of $\mathcal{S}_n$ generate $\mathcal{S}_n$ or $\mathcal{A}_n$ is at least $1 - \frac{2}{\log(\log(n))^2}$, which goes to one as n increases. This result was achieved through elementary methods. In fact, [**Bab**, **1989**] used the classification of finite simple groups to improve this result.

PROPOSITION 4.1 (Babai). *The probability that two random elements of $\mathcal{S}_n$ generate $\mathcal{S}_n$ or $\mathcal{A}_n$ is $1 - \frac{1}{n} + O(\frac{1}{n^2})$.* □

[**Dix**, **2005**] gives a succint summary of Babai's proof: it begins by appealing to two results of [**Dix**, **1969**]. The first shows that the probability that two random elements of $\mathcal{S}_n$ generate a transitive subgroup of $\mathcal{S}_n$ is $1 - \frac{1}{n} + O(\frac{1}{n^2})$. The second shows that the probability that this group is imprimitive is $\leq n2^{\frac{-n}{4}}$. Babai complements these results with the following observation which relies on the classification of finite simple groups: the probability that these elements generate a primitive subgroup different from $\mathcal{S}_n$ or $\mathcal{A}_n$ is $O\left(\frac{n^{\sqrt{n}}}{n!}\right)$. It follows that the probability that two random elements of $\mathcal{S}_n$ generate a transitive subgroup of $\mathcal{S}_n$ which is not $\mathcal{S}_n$ or $\mathcal{A}_n$ is $O\left(n2^{\frac{-n}{4}} + \frac{n^{\sqrt{n}}}{n!}\right)$, which goes to zero faster than n^{-k} for every $k > 0$. This implies Babai's theorem.

For our purposes we need a generalization of this result to $l > 2$ random elements. Such a generalization is indeed attainable by simple modifications of arguments used by both [**Bab**, **1989**] and [**Dix**, **1969**]. [**Dix**, **2005**] in particular mentions the generalization but does not prove it. So we shall prove the following theorem,

THEOREM 4.2 (Dixon-Babai). *The probability that l random elements of $\mathcal{S}_n$ generate $\mathcal{S}_n$ or $\mathcal{A}_n$ is* $1 - \frac{1}{n^{l-1}} + O(\frac{1}{n^l})$.

We begin as they did, with the following generalization of a result due to [**Dix**, **1969**], using a technique of [**Bab**, **1989**].

LEMMA 4.3. *The probability that l independently chosen random permutations from $\mathcal{S}_n$ fail to generate a transitive subgroup is bounded by*

$$\sum_{1 \le r \le n/2} \binom{n}{r}^{1-l} \le \frac{1}{n^{l-1}} + O(n^{-l})$$

PROOF. Let S be the set $\{1, 2, \ldots, n\}$. Given l random permutations, let $\mathcal{G}$ be the subgroup of $\mathcal{S}_n$ they generate. For any subset $A \subseteq S$, let $I(A)$ be the event that A is invariant under $\mathcal{G}$. Suppose $|A| = r$, then by independence we have

$$Prob(I(A)) = \binom{n}{r}^{-l}$$

Now suppose that $\mathcal{G}$ is not a transitive group. Then it must be that $I(A)$ holds for some A where $1 \le |A| \le n/2$ (since $I(A) = I(S \setminus A)$), and by union bound we know that this probability is less than

$$\sum_{1 \le r \le n/2} \binom{n}{r}^{1-l} \le \frac{1}{n^{l-1}} + O\left(\frac{1}{n^l}\right)$$

Note that this result is tight because probability that l random permutations have at least a fixed point is easily seen to be $\frac{1}{n^{l-1}} + O\left(\frac{1}{n^l}\right)$. ☐

We may conclude that the probability that l random elements of $\mathcal{S}_n$ generate a transitive subgroup of $\mathcal{S}_n$ is $1 - \frac{1}{n^{l-1}} + O(\frac{1}{n^l})$. We make minor modifications to a proof of [**Dix**, **1969**] to show the following:

LEMMA 4.4. *The probability that l random elements generate a transitive but imprimitive subgroup of $\mathcal{S}_n$ is less than* $n2^{\frac{-n(l-1)}{4}}$.

PROOF. Suppose a l-tuple $(x_1, \ldots, x_l)$ of elements of $\mathcal{S}_n$ generates a transitive but imprimitive subgroup. We denote the blocks of imprimitivity associated with this subgroup $\Gamma_1, \ldots, \Gamma_m$ where $m \neq 1, n$. We know that each Γ_i must have the same order d, and that together they form a partition of $\{1, \ldots, n\}$. Also note that any element of $\langle x_1, \ldots, x_l \rangle$ must permute the blocks of imprimitivity amongst themselves and if $\alpha \in \Gamma_i$, then $x_i(\alpha) \in x_i(\Gamma_i)$. This means that once we specify the transitive action of $\langle x_1, \ldots, x_l \rangle$ on the Γ_i there are at most $(d!)^m$ possibilities for each x_i. Let $t_m(l)$ be the proportion of l-tuples of elements in $\mathcal{S}_m$ which generate a transitive subgroup of $\mathcal{S}_m$. Then the number of l-tuples of elements in $\mathcal{S}_n$ which generate an imprimitive subgroup of $\mathcal{S}_n$ with blocks $\Gamma_1, \ldots, \Gamma_m$ is bounded by $(m!)^l t_m(l)(d!)^{lm}$.

The set $\{1, \ldots, n\}$ may be partitioned m blocks of d elements in $\frac{n!}{(d!)^m m!}$ ways. Let i_n be the proportion of l-tuples of elements in $\mathcal{S}_n$ which generate a transitive by imprimitive group. From the previous bound we know that

$$(n!)^l i_n \leq \sum_{(m,d) \text{ s.t. } md=n} \frac{(m!)^l t_m(l)(d!)^{lm} n!}{(d!)^m m!} \leq \sum_{(m,d) \text{ s.t. } md=n} n!(m!)^{l-1}(d!)^{m(l-1)}$$

where we used the fact that $t_m(l) \leq 1$. So we get that

$$i_n \leq \sum_{(m,d) \text{ s.t. } md=n} \left(\frac{m!(d!)^m}{n!} \right)^{l-1}$$

Now note that

$$\frac{m!(d!)^m}{n!} = \prod_{i=1}^{m} i \binom{id}{i}^{-1} = \prod_{i=1}^{m} \prod_{j=1}^{d-1} \left(\frac{d-j}{id-j} \right) \leq \prod_{i=1}^{m} i^{1-d} = (m!)^{1-d} \leq (2^{\frac{m}{2}})^{\frac{-d}{2}} = 2^{\frac{-n}{4}}$$

where we use that $m, d \geq 2$. Raising both sides to the power $l-1$ and combining the result with the previous equation gives us that

$$i_n \leq \sum_{(m,d) \text{ s.t. } md=n} 2^{\frac{-n(l-1)}{4}}$$

The lemma follows after noticing that picking m determines d, and there are certainly less than n choices for m. □

The final step in the proof of the Dixon-Babai theorem requires several facts from the classification of finite simple groups and was proved for $l = 2$ in [**Bab**, **1989**]. They state the general result and its proof follows from simple modifications of their arguments for the case $l = 2$. We give a proof of the following result in Appendix A.

Lemma 4.5. *The probability that l random permutations generate a primitive group other than $\mathcal{A}_n$ or $\mathcal{S}_n$ is $O((\frac{n^{\sqrt{n}}}{n!})^{l-1})$.* □

Proof of Theorem 4.2. Putting Lemmas 4.4 and 4.5 together, we have that the probability that l random permutations generate a transitive subgroup of $\mathcal{S}_n$, but not $\mathcal{S}_n$ or $\mathcal{A}_n$ is $O\left(n 2^{\frac{-n(l-1)}{4}} + \left(\frac{n^{\sqrt{n}}}{n!} \right)^{l-1} \right)$ which goes to zero faster than n^{-k} for every $k > 0$, and the Dixon-Babai theorem follows from Lemma 4.3. □

In order to set up our applications of this theorem in the coming sections, we mention the following elementary result in group theory: $\mathcal{S}_n$ acts n-transitively on the set $\{1, \ldots, n\}$. That is, it acts transitively on the set $\{1, \ldots, n\}^n$. Such highly transitive actions of groups are rare, but it is also easy to show that $\mathcal{A}_n$ acts $(n-2)$-transitively on

$\{1, \dots, n\}$. Keeping this mind, the Dixon-Babai theorem can be reinterpreted as follows: the probability that l random permutations generate a subgroup of $\mathcal{S}_n$ which acts at least $(n-2)$-transitively on $\{1, \dots, n\}$ is $1 - \frac{1}{n^{l-1}} + O(\frac{1}{n^l})$.

2. Generating Transitive Subgroups of $\mathcal{S}_{n_1} \wr \cdots \wr \mathcal{S}_{n_k}$

From our development of the theory of iterated random coverings we will be able to make progress towards a similar theorem for wreath products of symmetric groups. In particular, we will be able to calculate the probability that l random elements in $\mathcal{S}_{n_1} \wr \cdots \wr \mathcal{S}_{n_k}$ produce a subgroup which acts transitively on $N_1 \times \cdots \times N_k$ (where N_i is $\{1, \dots, n_i\}$).

THEOREM 4.6. *The probability that l independently chosen permutations from $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ generate a subgroup of $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ which acts transitively on $N_k \times \cdots \times N_1$ is*

$$\left(1 - \frac{1}{n_1^{l-1}} + O\left(\frac{1}{n_1^l}\right)\right) \prod_{i=2}^{k} \left(1 - \frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)}} + O\left(\frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)+1}}\right)\right)$$

$\square$

This theorem will be apparent from Proposition 6.2. We conjecture that the following result will now be attainable.

CONJECTURE 4.7. *The probability that l independently chosen permutations from $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ generate $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ is*

$$\left(1 - \frac{1}{n_1^{l-1}} + O\left(\frac{1}{n_1^l}\right)\right) \prod_{i=2}^{k} \left(1 - \frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)}} + O\left(\frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)+1}}\right)\right)$$

Indeed, the proof may even follow from carefully applying known results from the classification of finite simple groups as in the work of [**Bab**, **1989**].

CHAPTER 5

Connectivity Properties of Random Covering Graphs

1. The Walk-Subgroup of a Covering Graph

DEFINITION 5.1. *Let H be a graph and $\mathcal{G}$ a group. To every edge of H associate an element of $\mathcal{G}$ through a voltage assignment $V : E(G) \to \mathcal{G}$. Given a walk $\{w_1, w_2, \ldots, w_n\}$ on H, consider the product $V(w_1)V(w_2)\ldots V(w_n)$ where if $w_i = w_j^{-1}$ then $V(w_i) = V(w_j)^{-1}$. The subset of $\mathcal{G}$ which can be produced by products which arise from walks is called the walk-subset of (H,V). In some special cases, this subset is a subgroup of $\mathcal{G}$, which we will call the walk-subgroup of (H,V).*

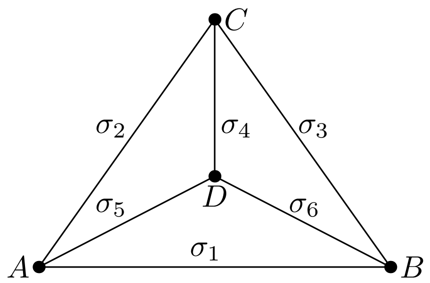


FIGURE 5.1. The element of the walk-subset corresponding to $\{AB, BC, CD\} = \sigma_1\sigma_3\sigma_4$, while the element corresponding to $\{AD, DC, CD, DB\} = \sigma_5\sigma_4\sigma_4^{-1}\sigma_6 = \sigma_5\sigma_6$.

Walk-subsets depend on the assignment $f : E(H) \to \mathcal{G}$ and the graph H. For example, if f assigns the identity element to every edge, then for every group $\mathcal{G}$ and graph H the walk-subgroup is trivial. To see the dependence on the structure of H, suppose that H is the line graph with group element g_i on edge i: the walk-subset consists of the $\binom{n}{2}$ elements $\Pi_{k\leq i\leq j} g_i$ where $1 \leq k, j \leq n$.

We have the following theorem about the structure of the walk-subsets for certain special assignments.

PROPOSITION 5.2. *Given a graph H and a spanning tree T, let l be the number of edges of H not in T. Now define f to be the assignment which sends every edge in T to the identity element, and any edge not in T to a distinct generator for the free group of l elements. In this case, the walk-subset, indeed walk-subgroup, is the free group on l elements.*

PROOF. This results from the following observation: there is a bijection between edges of H not in T and the fundamental cycles in H. By the definition of f, every fundamental cycle has only one non-trivial edge. To generate any element of the free group on l elements, simply consider the walk that starts in the fundamental cycle of the first required generator, does the requisite number of loops (raising this generator to the required power), and then traverses edges in T (which are all trivial) to the next required generator and so on. Finally, noting that fundamental cycles can be traversed in either direction regardless of the point of entry completes the proof. □

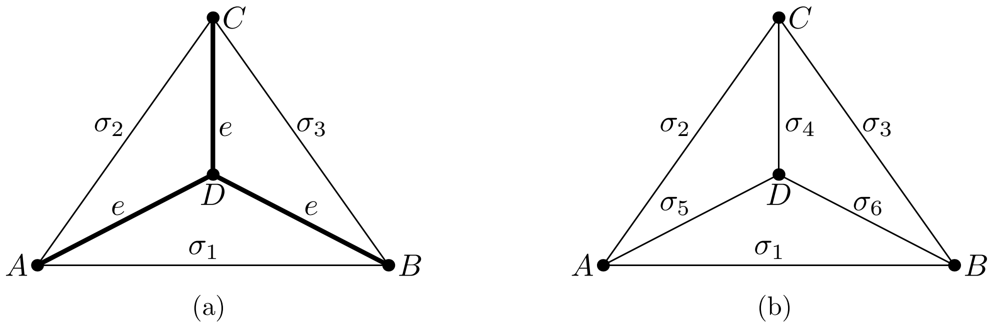


FIGURE 5.2. Let σ_i be elements of a group $\mathcal{G}$, and let e be the identity element. The walk-subgroup of 2(a) is the subgroup of $\mathcal{G}$ generated by σ_1, σ_2 and σ_3, whereas the walk-subset of 2(b) does not necessarily have a group structure.

COROLLARY 5.3. *Given a graph H and a spanning tree T, define f to be the assignment which sends every edge in T to the identity element, and any edge not in T to an element $g_i \in \mathcal{G}$. In this case the walk-subgroup is the subgroup generated by the g_i.* □

Since any $H \in L_n^T(G)$ (where T is a spanning tree of G) is the derived graph of a voltage assignment $V : E(G) \to \mathcal{S}_n$ which satisfies the conditions of Corollary 5.3, we sometimes refer to the walk-subgroup of (G, V) as the walk-subgroup of H. Also note that in case of random voltage assignments, the choice of T does not matter as the walk-subgroup is simply the entire subgroup generated by l random permutations, where l is the number of edges in G outside of T.

NOTE 5.4 (Associated Walk). *Every element σ in the walk-subgroup of a covering graph is the product of permutations assigned to edges along a (not necessarily unique) walk in the base graph. Such a walk is called an associated walk of σ.*

2. A Simple Application: Connectivity

As an example of the utility of the walk-subgroup of a covering graph, we will use it solve the connectivity problem in $L_n(G)$. By Proposition 2.9 we may choose a spanning tree T of G, and without loss of generality consider all voltages assigned to edges of T to be the identity permutation. These spanning tree edges are called flat edges.

THEOREM 5.5 (Connectivity). *Let G be a simple connected graph with $l-1$ more edges than vertices ($l \geq 1$). Then a random n-covering of G is connected with probability, $1 - \frac{1}{n^{l-1}} + O\left(\frac{1}{n^l}\right)$.*

We make the following connection to the walk-subgroup.

Proposition 5.6. *Let $H \in L_n(G)$. Then H is connected if and only if the walk–subgroup of (G, φ), where $H = G^\varphi$, is a transitive subgroup of $\mathcal{S}_n$.*

Proof. Suppose that H is connected. Then, starting on any vertex, there exists a walk which can hit every other vertex. In particular, if the walk starts on the vertex (v, i), it must be able to reach the vertices (v, j) for all $1 \leq j \leq n$. A walk can change the second coordinate only by taking some combination of the permutations on the non-flat edges, which by the previous corollary are elements of the walk–subgroup. So there must exist elements in the walk–subgroup which can change the second component of the walk from any i to any j. That is to say, the walk–subgroup must be a transitive subgroup of $\mathcal{S}_n$.

Conversely suppose that the walk–subgroup is transitive. Without loss of generality, suppose a walk starts on vertex $(v, 1)$. It can first walk along the lifts of the flat edges of G (which form a spanning tree of every section of H) to cover all vertices of the form $(u, 1)$. Then, it can take the lift of the walk associated with a permutation σ such that $\sigma(1) = 2$ to end up at a vertex $(a, 2)$. Such an element of the walk-subgroup exists by assumption. From here it can cover all vertices of the form $(b, 2)$ and continue similarly, covering the whole graph. This tells us that from every vertex there is a walk which can cover the entire graph, implying that the graph is connected. $\square$

Lemma 5.7. *Let G be a graph with l non-flat edges (or $l-1$ more edges than vertices). Then the probability that $H \in L_n(G)$ is connected is the probability that l random elements of $\mathcal{S}_n$ generate a transitive subgroup of S_n.*

Proof. This lemma is an immediate consequence of Proposition 5.6 and Corollary 5.3. $\square$

Proof of Theorem 5.5. This follows from Lemmas 5.7 and 4.3. $\square$

3. Edge Expansion: Lower Bound

Definition 5.8. *The isoperimetric constant or edge expansion of a graph G is defined to be*

$$\min_{S \subset V(G), |S| \leq V/2} \frac{E(S, S^c)}{|S|}$$

where $E(S, S^c)$ is number of edges leaving S.

Theorem 5.9 (Edge Expansion). *Let G be a simple connected graph with $l-1$ more edges than vertices ($l \geq 1$). Then there exists a constant $\xi(G) > 0$, such that a random n-covering of G (for $n \geq 3$) has edge expansion at least $\xi(G)$, with probability $1 - \frac{1}{n^{l-1}} + O\left(\frac{1}{n^l}\right)$.*

We make the following connection to the walk–subgroup.

PROPOSITION 5.10. *Let $H \in L_n(G)$. If the walk–subgroup of (G, φ), where $H = G^\varphi$, is a k–transitive subgroup of $\mathcal{S}_n$ for $k \geq n/3$, there exists a positive constant $\xi(G)$ such that H has expansion at least $\xi(G)$.*

PROOF. Let T be a subset of vertices of H such that $0 < |T| \leq |V(H)|/2$. For a vertex v of G, denote the fiber over v by F_v, and define $T_v = F_v \cap T$. Also denote $t_v = |T_v|$ and $m = \max_{v \in V(G)} t_v$. Note that $|T| < m|V(G)|$.

Fix $\varepsilon < \frac{1}{4}$. Now suppose that t_i are not all of 'similar size'. More precisely, suppose there exists u such that $t_u < (1-\varepsilon)m$. Let v be such that $t_v = m$. We know that there are n disjoint paths from F_u to F_v in H (using the fact that G is connected and the lifting property of paths), and in particular, it at least εm of these paths must connect T_v to a vertex outside T_u. Then we get

$$E(T, T^c) \geq \varepsilon m = \frac{\varepsilon m |V(G)|}{|V(G)|} \geq \frac{\varepsilon |T|}{|V(G)|}$$

and so $\phi(T) \geq \frac{\varepsilon}{|V(G)|}$. Now suppose that $t_u \geq (1-\varepsilon)m$ for all $u \in V(G)$. By the choice of ε it follows that $m \leq 2n/3$. Consider an aribitrary F_v. We know that F_v contains at least $n/3$ vertices not in T. But we know that there is an element σ in the walk subgroup such that $|T_v \cup \sigma(T_v)| = t_v + n/3$ or $2t_v$ (in case $t_v \leq n/3$). We will consider the first case, as the calculation for the second case is similar. Then there are $n/3$ indices in T_v such that $\sigma(k) \notin T_v$. For all such indices k, the lift of the walk associated with σ starting at k contains a unique edge in $E(T, T^c)$. In particular we have

$$E(T, T^c) \geq \frac{n}{3} \geq \frac{t_v}{2} \geq \frac{(1-\varepsilon)m}{2} = \frac{(1-\varepsilon)m|V(G)|}{2V(G)} \geq \frac{(1-\varepsilon)|T|}{2|V(G)|} \geq \frac{\varepsilon |T|}{|V(G)|}$$

□

PROOF OF THEOREM 5.9. The Dixon-Babai theorem combined with the fact the action of $\mathcal{S}_n$ is n-transitive and the action of $\mathcal{A}_n$ is $(n-2)$-transitive implies the lower bound on the probability in Theorem 5.9. The upper bound on the probability holds because strictly positive edge expansion implies connectedness, and the probability of connectedness in Theorem 5.5 matches the lower bound. □

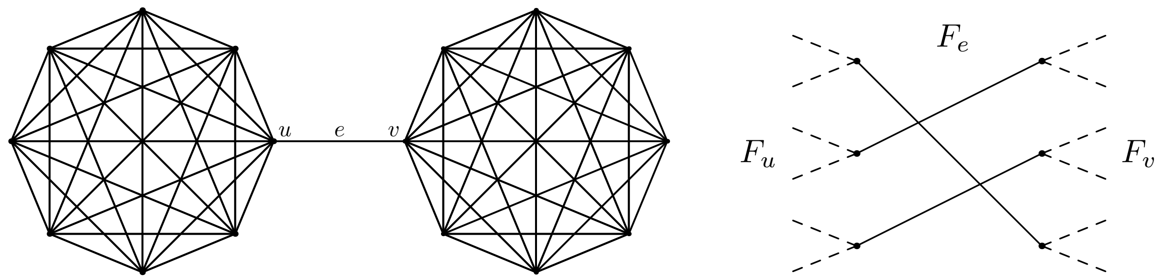
4. δ-Connectivity

Now that we have shown that not only are random lifts connected with high probability, but that large sets in covering graphs have large boundaries, we can prove the following theorem.

THEOREM 5.11 (δ-Connectivity). *Let G be a simple connected graph with minimum degree $\delta \geq 8$ (in fact, the same technique can be used to prove a (weaker) bound for $\delta \geq 5$). Then the probability that a random n-covering of G is δ-connected is at least $1 - O\left(\frac{1}{n^\delta}\right)$, given that $n > (\delta-1)^6|V(G)|^2$.*

First we show that if we desire a non-trivial bound which works for all graphs with a fixed minimum degree, we must impose a condition on n in terms of δ. Consider the following example:

Example 5.12. *The barbell graph B_k consists of two cliques of $k+1$ vertices connected by a single edge called the bridge. This graph has minimum degree k. However, no graph in $L_n(B_k)$, for $n < k$ is k-connected. This is because the bridge has only n copies, and cutting these n copies disconnects the graph.*



(a) (b)

Figure 5.3. 3(a) is the graph B_7 and 3(b) shows the fiber of bridge edge e, and in particular, that no degree 3 covering of 3(a) can be 7-connected as one can simply cut every edge in F_e to disconnect the graph.

This tells us we need n to be large enough for δ-connectivity to be possible, and the condition in our theorem, $n \geq (\delta-1)^6|V(G)|^2$, is not a mere artifact of the proof strategy.

Proposition 5.13. *Let $H \in L_n(G)$. Let $n > (\delta-1)^6|V(G)|^2$, where $\delta \geq 8$ is the minimum degree of G. If the walk–subgroup of (G, φ), where $H = G^\varphi$, is a δ-transitive subgroup of $\mathcal{S}_n$, then H is δ-connected with probability at least $1 - O\left(\frac{1}{n^\delta}\right)$.*

Proof. Let T be a subset of vertices of H such that $0 < |T| \leq |V(H)|/2$. For a vertex v of G, denote the fiber over v by F_v, and define $T_v = F_v \cap T$. Also denote $t_v = |T_v|$.

First we reduce the problem to the case when the fibers over every point are roughly evenly distributed. Suppose that there exist $u, v \in G$ such that $|t_u - t_v| \geq \delta$. Then consider a path in G which connects u to v. It lifts to n edge-disjoint paths in H which connect F_u to F_v, implying that $E(T, T^c) \geq \delta$. So we need only consider the case when $|x_u - x_v| \leq \delta - 1$ for all $u, v \in G$. Suppose a subset of vertices contains a fiber T_v such that $t_v \geq \delta$. We can assume that $|F_v \setminus T_v| \geq \delta$, because $n >> 4\delta$ implies there cannot exist a single fiber such that $|F_v \setminus T_v| \leq \delta$ since we are considering only sets with somewhat 'balanced' fibers. Since we assumed the walk subgroup to be δ-transitive, there is a loop based at v in G which corresponds to σ in the walk-subgroup which lifts to δ edge disjoint paths which take δ points in T_v to δ distinct points in $F_v \setminus T_v$. This implies that the boundary of such a set is at least δ.

Now we consider the only remaning case: when $t_u \leq \delta - 1$ for all $u \in V(G)$. These sets require the careful analysis of several cases. The first three cases show that such sets of vertices spread across a small number of fibers cannot have small boundary. The tedious case is the fourth, which (loosely) bounds the probability that the rest of such possible sets have small boundary. The argument is as follows: suppose such a set has small boundary, then it is enough to consider the case that it is a connected subgraph of H. In fact, we show it must be a subgraph which contains a large number of cycles, and therefore a large number of edges in H which are lifts of (not necessarily distinct) non-flat edges in G. Since many edges in such graphs need a random permutation to take them to the correct spot (in order to complete the necessary number of cycles), they occur with low probability. Let h be the number of non-empty fibers,

1. Suppose $h = 1$. Since fibers are totally disconnected and the minimum degree of any vertex is δ, the size of the boundary must be at least δ.
2. Suppose $2 \leq h \leq \delta - 1$. Then we know that each vertex in this set must have at least $\delta - h + 1$ edges leaving the set. This is because each vertex can at best connect to $h - 1$ other fibers (all of the fibers excluding itself). So the size of the boundary is at least $h(\delta - h + 1)$. This is minimized as a function of h in the given range when $h = 2$, giving us that the size of the boundary is at least $2(\delta - 1) \geq \delta$.
3. Let $h = \delta$. In this case, each vertex has at least one edge leaving K, and there are at least δ vertices. So the boundary must be $\geq \delta$.
4. Now let $h > \delta$. We may assume that such a set K (of size k), is a connected subgraph of H, since disconnected subgraphs have a boundary greater than or equal to the boundary of any of the components. We first show that any K with boundary $< \delta$ must have at least $2.5k$ edges more than vertices. The vertices of K have minimum degree δ, implying that the total degree of K is at least $k\delta$. Since K is connected it has a spanning tree with $k-1$ edges, which contributes $2k-2$ to the total degree of K. Of the remaining $k\delta - 2k + 2$ total degree, at least $(k-1)\delta - 2k + 3$ must be accounted for by edges that connect back into the graph. This is because at most $\delta - 1$ go outside K by assumption. By eliminating the double counting of edges that stay within K, the total number of non-spanning tree edges in K is at least
$$\frac{(k-1)\delta - 2k + 3}{2} \geq \frac{8k - 8 - 2k + 3}{2} \geq 2.5k + 1.5 > 2.5k + 1$$
where we use that $k > \delta \geq 8$. We argue that since K has at least $2.5k + 1$ edges in excess of a spanning tree, it must have at least $2.5k + 1$ edges which are lifts of (not necessarily distinct) non-flat edges in G. For the sake of contradiction suppose that K has less than $2.5k + 1$ non-flat edges. Then upon deleting them, we are left with lifts of flat edges only, but more edges than in a spanning tree of K. That means that we must have at least one cycle in K, which must come from a cycle in G. But a cycle in

G must contain at least one non-flat edge, and therefore K must still contain at least one edge which is a lift of a non-flat edge.

Now suppose that m of these edges lie above a single edge in G (note that $m \leq \delta - 1$). The probability that a random permutation takes them to the correct points in their destination fiber to keep them within the subgraph is less than

$$\frac{\delta-1}{n} \times \frac{\delta-2}{n-1} \times \cdots \times \frac{\delta-m-1}{n-m} \leq \left(\frac{\delta-1}{n}\right)^m$$

where the inequality follows since $n >> \delta$. Now notice that lifts of different non-flat edges of G are independent, which combined with the previous observation gives us that the probability that the necessary $2.5k+1$ edges stay within the subgraph is less than

$$\left(\frac{\delta-1}{n}\right)^{2.5k+1}$$

This shows us that the probability that a connected subgraph of k vertices has a small boundary is very small. The total number of such subgraphs is certainly less than $\binom{n|V(G)|}{k} = O(|V(G)|^k n^k)$. By union bound, the probability that any such subgraph of size k exists is on the order of

$$|V(G)|^k n^k \cdot \left(\frac{\delta-1}{n}\right)^{2.5k+1} = |V(G)|^k \cdot \frac{(\delta-1)^{2.5k+1}}{n^{k+1} \cdot n^{.5k}} \leq \frac{1}{n^{k+1}}$$

where the second inequality uses the fact that $n > (\delta-1)^6 |V(G)|^2$.

Finally through union bound, the probability that any bad subgraph of *any* size exists is less than

$$\sum_{i=\delta}^{(\delta-1)|V(G)|} \frac{1}{n^{i+1}} < (\delta-1)|V(G)| \frac{1}{n^{\delta+1}} \leq \frac{1}{n^\delta}$$

where we again use the fact that $n > (\delta-1)^6 |V(G)|^2$. This completes the proof. □

Proof of Theorem 5.11. Since for $\delta \geq 8$ (even 5) the number of non-flat edges is much greater than δ, the Dixon-Babai theorem and Proposition 5.13 imply Theorem 5.11 through the union bound. □

Definition 5.14. *$\underline{L_n(k,\delta)}$ is the set of all covering graphs of degree n of all connected simple graphs on k vertices with minimum degree δ.*

Theorem 5.15. *There exists $\gamma > 0$ such that for all $5 \leq \delta(n,k) \leq O\left(\frac{n^\gamma}{k}\right)$, asymptotically almost surely a random $H \in L_n(k,\delta)$ is δ-connected.*

Proof. We will closely follow the proof of Proposition 5.13. If $H \in L_n(k,\delta)$, then $H \in L_n(G)$ for some graph G with k vertices and minimum degree δ. We know that a.a.s. the walk-subgroup of all such covering graphs is $\delta(n,k)$-transitive (because there are at least two non-flat edges). Therefore, by analogy to the previous proof, we only need to worry about sets which have at most $\delta - 1$ points in any fiber, and are spread across more than δ fibers. We may also assume that such a set is a connected subgraph of H. As we saw in Proposition 5.13, such a set (say S of size s) must have at least

$$\frac{(s-1)\delta - 2s + 3}{2} \geq \frac{3s-2}{2} \geq 1.5s - 1 \geq 1.3s$$

edges which are lifts of non-flat edges of its base graph if it is to have a boundary of size less than $\delta - 1$. Therefore the probability that that the required number of edges end up in the correct point in their destination fiber is certainly bounded by $\left(\frac{\delta}{n}\right)^{1.3s}$, as was seen in the previous theorem. The number of such sets of size s is certainly less than $\binom{kn}{s} = O(n^s k^s)$, therefore the probability that any such set of size s exists is less than the order of $\frac{\delta^{1.3s} k^s n^s}{n^{1.3s}} \leq \frac{1}{n^{.05s}}$, where we chose $\gamma = .19$ so that $\delta k \leq n^{.19}$. Now we use the union bound to show that the probability that any such set of any possible size exists is less than

$$\sum_{i=\delta}^{\delta k} \left(\frac{1}{n^{.05}}\right)^i < \frac{\delta k}{n^{.05\delta}} \leq \frac{\delta k}{n^{.25}} \leq \frac{1}{n^{.06}}$$

which clearly goes to zero has n increases. $\square$

CHAPTER 6

Connectivity Properties of Iterated Random Covering Graphs

1. The Walk-Subgroup of an Iterated Covering Graph

The walk-subgroup of an iterated random covering is defined analogously to the random covering case. It is the group generated by the elements in the image of voltage assignments from the non-flat edges of the base graph to a wreath product of symmetric groups. Only note that since it is a group generated by random elements of a wreath product of symmetric groups, it is a subgroup of such a wreath product.

2. Connectivity

THEOREM 6.1. *Let G be a simple connected graph with $l-1$ more edges than vertices ($l \geq 1$). Suppose $H \in L_{n_k \dots n_1}(G)$. Then H is connected with probability*

$$\left(1 - \frac{1}{n_1^{l-1}} + O\left(\frac{1}{n_1^l}\right)\right) \prod_{i=2}^{k} \left(1 - \frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)}} + O\left(\frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)+1}}\right)\right)$$

PROOF. Following our discussion of iterated random coverings: a random graph H in $L_{n_k \dots n_1}(G)$ is a random covering of a random graph in $L_{n_{k-1} \dots n_1}(G)$ and so on, beginning with a random graph in $L_{n_1}(G)$. By independence, the probability that H is connected is just the product of the probabilities that each graph in this iterated process is connected. We have already calculated this probability as a function of the number of edges and vertices in each graph of this iterated process. Since G has $l-1$ more edges than vertices, we can easily calculate that a graph in $L_{n_i \dots n_1}(G)$ has $(l-1)n_1 \dots n_i$ more edges than vertices, and the result follows from our work on random coverings. □

We may now complete the deferred proof of Theorem 4.11, which follows immediately from the following proposition linking walk-subgroups of iterated random coverings to connectivity.

PROPOSITION 6.2. *Suppose $H \in L_{n_k \dots n_1}(G)$. Let T be a spanning tree of G, without loss of generality we may assume that H is the derived graph of a voltage assignment of G to $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ where non-trivial voltages are only assigned to edges not in T. H is connected if and only if the walk-subgroup of G is a subgroup of $\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}$ which acts transitively on the set $N_1 \times \cdots \times N_k$.*

PROOF. As before: let $(e_1, e_2, \dots, e_k) \in N_1 \times \cdots \times N_k$ denote the $e_k th$ child of the $e_{k-1} th$ child of the $\dots$ $e_1 th$ child of an original edge e in $E(G) - T$. Since each vertex in

H also comes from an ancestor in G in this way, we may see that $N_1 \times \cdots \times N_k$ can also be viewed as the indexing set of every fiber F_u in H of $u \in G$. Since every section of G_k inherits a lift of T, to conclude that the entire graph is connected it is enough to show that every point in a particular fiber can be reached from any other point in the same fiber. If the walk-subgroup of G is a subgroup of $S_{n_k} \wr \cdots \wr S_{n_1}$ which acts transitively on the set $N_1 \times \cdots \times N_k$, there is a walk in G which corresponds to an element of the walk subgroup which can send any element in $N_1 \times \cdots \times N_k$ to any other element. This shows that H is connected. Conversely, if H is connected, there must be a walk in it which takes a point in F_u to any other point in F_u. This walk comes from a closed walk starting at u in G and therefore an element of the walk-subgroup, showing that the action of the walk-subgroup on $N_1 \times \cdots \times N_k$ must be transitive. $\square$

3. Edge Expansion: Lower Bound

We show a lower bound on the edge expansion of iterated coverings.

THEOREM 6.3 (Edge Expansion). *Let G be a simple connected graph with $l-1$ more edges than vertices ($l \geq 1$). Then there exists a constant $\xi'(G) > 0$, such that $H \in L_{n_k \dots n_1}(G)$ (where $n_i \geq 3$ for all i) has edge expansion at least $\xi'(G)$, with probability*

$$\left(1 - \frac{1}{n_1^{l-1}} + O\left(\frac{1}{n_1^l}\right)\right) \prod_{i=2}^{k} \left(1 - \frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)}} + O\left(\frac{1}{n_i^{(l-1)(\prod_{j=1}^{i-1} n_j)+1}}\right)\right)$$

PROOF. This proof is similar to Theorem 6.1. The probability that H has edge expansion bounded by some constant calculated in terms of G is lower bounded by the product of the probabilities that each graph in the iterated process which creates H has the same. We have already calculated this probability for each step in the iterated process in Theorem 5.9. Since G has $l-1$ more edges than vertices and we know that a graph in $L_{n_i \dots n_1}$ has $(l-1)n_1 \dots n_i$ more edges than vertices. This shows that the required probability is lower bounded by the expression above. Since strictly positive edge expansion implies connectivity, and the lower bound matches the probability of connectivity in Theorem 6.1, the result follows. $\square$

4. δ-Connectivity

THEOREM 6.4 (δ-Connectivity). *Let G be a simple connected graph with minimum degree $\delta \geq 8$ (in fact, the same technique can be used to prove a (weaker) bound for $\delta \geq 5$). Then the probability that $H \in L_{n_k \dots n_1}(G)$ is δ-connected is at least*

$$\prod_{i=1}^{k} \left(1 - O\left(\frac{1}{n_i^{\delta}}\right)\right)$$

given that for $i \geq 2$, $n_i > (\delta-1)^6(|V(G)| \prod_{j=1}^{i-1} n_i)^2$ and $n_1 \geq (\delta-1)^6 |V(G)|^2$.

Proof. Following the work of the previous two proofs, simply note that the required probability is a lower bound on the probability that all graphs in the iterated process which generates H (therefore H) are δ-connected. $\square$

Definition 6.5. $\underline{L_{n_k \ldots n_1}(g,\delta)}$ *is the family of iterated* $(n_1, \ldots, n_k)$*-covering graphs of all connected simple graphs on* g *vertices with minimum degree* δ*.*

Theorem 6.6. *There exists* $\gamma > 0$ *such that for all* $5 \leq \delta(n_1, \ldots, n_k, g) \leq O\left(\min\left\{\left(\frac{n_1^\gamma}{g}\right), \left(\frac{n_i^\gamma}{g\prod_{j=1}^{i-1} n_i}\right) : 2 \leq i \leq k\right\}\right)$*, asymptotically almost surely a random* $H \in L_{n_k n_2 \ldots n_1}(k,\delta)$ *is* δ*-connected.*

Proof. We can pick $\gamma = .19$. If the given condition on δ holds, and then Theorem 5.14 tells us that the probability that all graphs in the iterated process which generates H (therefore H) are δ-connected with probability at least $\prod_{i=1}^{k}\left(1 - O\left(\frac{1}{n_i^{.06}}\right)\right)$. This clearly goes to one as $n_i \to \infty$ for all i. $\square$

CHAPTER 7

Topological Applications

1. Homotopy Invariants of Random Covering Graphs

It is easily shown that covering spaces of topological spaces inherit structure from their base space, for example if $\rho : \tilde{X} \to X$ is a covering projection, then we have an injection of fundamental groups $\pi_1(\tilde{X}) \to \pi_1(X)$. Since homotopy equivalent spaces have the same homotopy [and homology] groups, this indicates connections between random coverings of different spaces which have the same homotopy type. Indeed, we show that there exist graphical properties of random covering graphs whose probability only depends on the homotopy type of their base graph. This approach is different from the previous work connecting homology and randomization which focuses on computing the distribution of homology groups of random spaces, for example, the work of [**LM**, **2006**] and [**MW**, **2009**] on random simplicial complexes. For the case of random covering graphs the computation of homology groups turns out to be easy*. We demonstrate a new way to study randomization in topology by showing how *random* covering spaces inherit structure based on the homotopy type of their base space.

It is not straightforward in general to determine whether two spaces are homotopy equivalent, however, the situation is easy for graphs (viewed as topological spaces). It is well known that two graphs are homotopy equivalent if and only if the rank of their fundamental group [first homology group or first Betti number] is the same. Using this we show that the probability that a random covering graph of G is connected or has edge expansion bounded below by $\xi(G)$ only depends on the homotopy type of G. Following this, we will define the walk-subgroup of coverings created from voltage assignments in general groups using any distribution (so far we have focused on uniform probability assignments from the symmetric group as in the Amit-Linial model). Such assignments produce more restricted models which may not describe every possible covering space of the base graph, but may be more suitable for certain applications. We show that even in this general setting the probability that a covering space is connected only depends on the homotopy type of the base graph. While random models of covering spaces have only been studied for graphs so far, we expect such invariants to exist for any model of random covering spaces of abstract topological spaces. In the following discussion we assume some

*One may work it out case by case for trees, cycles and connected graphs with more than one non-flat edge.

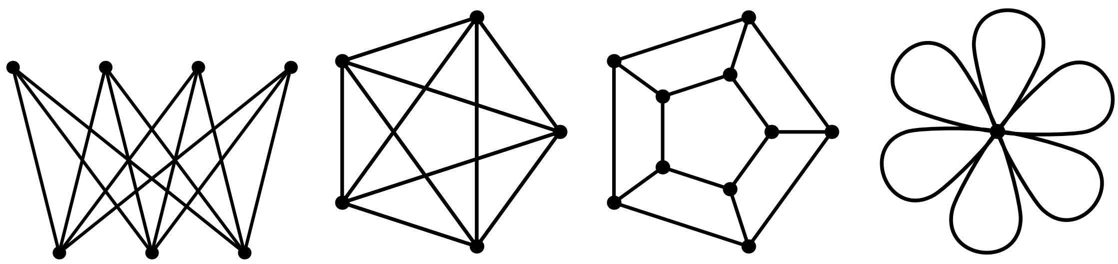
familiarity with algebraic topology and only sketch the proofs of the required background results. Complete proofs of the background material may be found in [**Hat**, **2002**].

PROPOSITION 7.1. *Given a connected graph G and a spanning tree T of G, the fundamental group $\pi_1(G)$ is isomorphic to the free group on $|E(G) - T|$ generators, and the first homology group is the free abelian group of rank $|E(G) - T|$, i.e. the first Betti number of G is $|E(G) - T|$.*

PROOF. The proof begins with the following observation: Given a CW complex X and a subcomplex A, if the pair (X, A) has the homotopy extension property (i.e. $X \times \{0\} \cup A \times I$ is a deformation retract of $X \times I$), then the projection map $X \to X/A$ is a homotopy equivalence. Now note that if a subcomplex A of X is contractible, the pair always has the homotopy extension property and we have the equivalence $X \to X/A$. A graph is easily seen to be a 1-dimensional CW complex constructed by attaching 1-dimensional cells to (edges) to a 0-dimensional skeleton of points (vertices). Also, since a spanning tree is contractible to a point, we get the homotopy equivalence $G \to G/T$ by the previous claim. G/T is just the wedge sum of $|E(G) - T|$ circles. The fundamental group of the wedge sum of $|E(G) - T|$ circles is the free group on $|E(G) - T|$ generators as may be computed using Van Kampen's theorem. The fact about the Betti number follows since the first homology group is the abelianization of the fundamental group. $\square$

PROPOSITION 7.2. *Two connected graphs G and H are homotopy equivalent if and only if they have isomorphic fundamental groups, i.e. if and only if the number of edges minus the number of vertices is the same for both.*

PROOF. From the proof of the previous proposition, this immediately reduces to showing that the wedge sum of m circles, C_m, is homotopy equivalent to the wedge sum of n circles, C_n, if and only if $m = n$. Suppose $m \neq n$, in this case we may simply use Van Kampen's theorem to show that $\pi_1(C_m) \ncong \pi_1(C_n)$. If $m = n$ there is nothing to prove. $\square$



(a) $K_{3,4}$ (b) K_5 (c) P_5 (d) C_6

FIGURE 7.1. Some homotopy equivalent graphs.

Now we show the existence of homotopy invariants in random covering graphs and iterated random covering graphs.

THEOREM 7.3. *Let G and H be simple connected graphs. Then the probabilities that $G' \in L_n(G)[L_{n_k \ldots n_1}(G)]$ and $H' \in L_n(H)[L_{n_k \ldots n_1}(H)]$ are connected are equal if and only if G is homotopy equivalent to H.*

PROOF. We already know that the probability that G' and H' are connected are simply the probabilities that the walk-subgroups of G' and H' are subgroups of $\mathcal{S}_n$ $[\mathcal{S}_{n_k} \wr \cdots \wr \mathcal{S}_{n_1}]$ which act transitively on $\{1, \ldots, n\}$ $[N_1 \times \cdots \times N_k]$. These probabilities only depend on the number of generators for the respective walk-subgroups, which is the first Betti number of the graphs in question. Graphs with the same first Betti number are homotopy equivalent by the previous proposition. □

THEOREM 7.4. *Let G and H be simple connected graphs. Let $n, n_1, \ldots, n_k \geq 3$. Then the probabilities that $G' \in L_n(G)[L_{n_k \ldots n_1}(G)]$ and $H' \in L_n(H)[L_{n_k \ldots n_1}(H)]$ have edge expansion bounded below by $\xi(G)$ and $\xi(H)$ respectively are equal if and only if G is homotopy equivalent to H.*

PROOF. Similar to the previous proof, these probabilities only depend on the properties of the walk-subgroup, which in turn depend only on the number of generators for the walk-subgroup. □

So far we have focused on Amit and Linial's model of random covering graphs obtained by uniform probability voltage assignments to the symmetric group. In fact, we may relax both of these conditions and still obtain connectivity has a homotopy invariant of the [restricted] model of random covering graphs obtained in this way.

DEFINITION 7.5. *Given a graph G with unoriented edges, a group $\mathcal{K}$ acting on a set Ω of size n and a distribution D on $\mathcal{K}$, a labeled $(\mathcal{K}, D, n)$-covering is the derived graph produced by arbitrarily orienting the edges of G and making a voltage assignment with voltages in $\mathcal{K}$ by sampling independently from D. Similar to the case of random coverings, we may pick a spanning tree T of G and assume that non-trivial voltages are only assigned to edges of G outside T and obtain an equivalent model as far as graphical properties are concerned.*

The lack of an analog of the Gross-Tucker theorem necessitates extra care in proving that we can assume T to have trivial voltages, however the main ideas and the result remain the same as Theorem 2.9. We define the walk-subgroup of a labeled $(\mathcal{K}, D, n)$-covering of a graph G as the subgroup of $\mathcal{K}$ generated by elements in the image of the voltage assignment in $\mathcal{K}$.

PROPOSITION 7.6. *Let H be a labeled $(\mathcal{K}, D, n)$-covering of a simple connected graph G. Let $\mathcal{K}$ be as above, i.e. $\mathcal{K}$ acts on Ω which is a set of size n, and H is a $n-$covering of G. Then H is connected if and only the walk-subgroup, $\mathcal{W}$, of H acts transitively on Ω.*

PROOF. As in previous proofs, we point out that each section of H has a spanning tree inherited from G. So to prove connectivity of the entire graph, we just need to show connectivity in the fiber of any vertex of G, say v. Suppose the walk-subgroup is transitive. Then to get to any (v, ω') from any (v, ω) in H, simply take the lift of the walk associated with $\sigma \in \mathcal{W}$ such that $\sigma(\omega) = \omega'$. Conversely, if H is connected then the projection of the path from (v, ω) to (v, ω') gives an element of the walk-subgroup such that $\sigma(\omega) = \omega'$. □

THEOREM 7.7. *Let G and H be simple connected graphs. Then the probabilities that labeled $(\mathcal{K}, D, n)$-coverings of G and H are connected are equal if and only if G is homotopy equivalent to H.*

PROOF. Both these probabilities depend only on the properties of the walk-subgroup as shown in the previous proposition, which in turn depend only on the number of generators. □

Homotopy invariants are readily also seen in generalized iterated coverings. To avoid excessive repetition, we only mention the definitions and theorems. The details may readily be filled in from this thesis itself.

DEFINITION 7.8. *Given a graph G with unoriented edges, groups $\mathcal{K}_i$ acting on a sets Ω_i of size n_i and distributions D_i on $\mathcal{K}_i$, a labeled $\{\mathcal{K}_i, D_i, n_i : 1 \leq i \leq k\}$-covering is the derived graph produced by arbitrarily orienting the edges of G and making a voltage assignment with voltages in $\wr_i \mathcal{K}_i$ by sampling independently from each D_i the appropriate number of times. Similar to the case of random iterated coverings, we may pick a spanning tree T of G and assume that non-trivial voltages are only assigned to edges of G outside T and obtain an equivalent model for graphical properties.*

PROPOSITION 7.9. *Let H be a labeled $\{\mathcal{K}_i, D_i, n_i : 1 \leq i \leq k\}$-covering of a simple connected graph G. Let the $\mathcal{K}_i$ be as above, i.e. the $\mathcal{K}_i$ act on Ω_i which are sets of size n_i, and H is a $n_k \ldots n_1-$covering of G. Then H is connected if and only the walk-subgroup, $\mathcal{W}$, of H acts transitively on $\Omega_1 \times \cdots \times \Omega_k$.* □

THEOREM 7.10. *Let G and H be simple connected graphs. Then the probabilities labeled $\{\mathcal{K}_i, D_i, n_i : 1 \leq i \leq k\}$-coverings of G and H are connected are equal if and only if G is homotopy equivalent to H.* □

It is important to note that the proofs in this section do not require that the base graph be simple. This convention was continued from previous sections, where it was adopted due to its necessity in the proofs pertaining to δ-connectivity. This will be evident from the next section.

2. Random Regular Graphs or Random Coverings of C_d

Let us quickly recall that in our discussion of constructing covering graphs from voltage assignments in the symmetric group, we do not require that the graphs be simple. If a graph has parallel edges, we assign a random permutation to each parallel edge, and construct a covering graph as usual. For example:

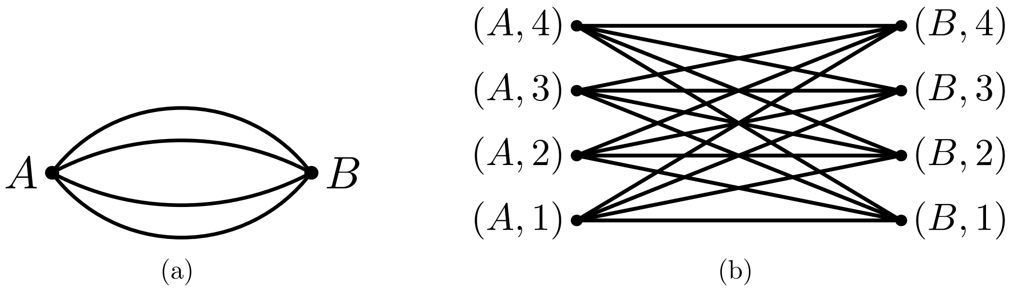


FIGURE 7.2. 2(b) is a degree 4 covering graph of 2(a), where the edges are assigned the permutations $(1), (1234), (13)(24)$ and $(14)(23)$ of $\mathcal{S}_4$ respectively.

We have seen that given any graph G and a spanning tree T where $d = |E(G) - T|$, we may contract the subtree to a point and end up with a homotopy equivalent graph. We call this graph C_d and it consists of a single vertex with d loops. This observation will help us show a connection between random covering graphs and random $2d$-regular [multi-]graphs (denoted by $\mathcal{G}_{n,2d}$) which have been studied by [**BS**, **1987**], [**FKS**, **1989**] amongst many others. A random $2d$-regular graph on n vertices is obtained by choosing d permutations $\sigma_1, \ldots, \sigma_d$ independently and randomly from $\mathcal{S}_n$, and adding the edges $(j, \sigma_i(j))$ for all i to the n (initially isolated) vertices. Note that loops count as incoming and outgoing edges in such graphs. Clearly, random n-covering of C_d produces exactly the same distribution on $2d$-regular graphs as $\mathcal{G}_{n,2d}$. So by just accounting for parallel edges and self-loops in our previous work, we get new results for random regular graphs as well.

PROPOSITION 7.11. *Let $H \in L_n(C_d) = \mathcal{G}_{n,2d}$. H is connected if and only if the walk-subgroup of C_d is a transitive subgroup of S_n.*

PROOF. All we need is that the walk-subgroup of C_d is indeed the subgroup generated by the $\sigma_1, \ldots, \sigma_d$. This is clear since the loops may be traversed in all possible orders. Now suppose the walk-subgroup is transitive. Then to get to any u from any v in H, simply take the lift of the walk associated with $\sigma \in S_n$ such that $\sigma(u) = v$. Conversely, if H is connected then the projection of the path from any u to v gives an element of the walk-subgroup σ, such that $\sigma(u) = v$. □

THEOREM 7.12. *Let $G \in \mathcal{G}_{n,2d}$. The probability that G is connected is $1 - \frac{1}{n^{d-1}} + O\left(\frac{1}{n^d}\right)$.* □

PROPOSITION 7.13. *Let $H \in L_n(C_d) = \mathcal{G}_{n,2d}$. If the walk-subgroup of C_d is a k-transitive subgroup of S_n for $k \geq n/2$, then the edge expansion of H is at least 1.*

PROOF. Suppose the walk-subgroup is $n/2$-transitive, then for any set T of size $\leq n/2$, we may use the lift of the walk associated with element of the walk subgroup σ such that $\sigma(t) \neq t$ for any $t \in T$ to show that there must be at least $\min(|T|, n/2)$ edges leaving it. In either case, the edge expansion has to be greater than one, concluding the proof. $\square$

THEOREM 7.14. *Let $G \in \mathcal{G}_{n,2d}$ (for $n \geq 4$). With probability $1 - \frac{1}{n^{d-1}} + O\left(\frac{1}{n^d}\right)$, G has edge expansion at least* 1. $\square$

In particular these results show that the homotopy invariants of random covering graphs can simply be studied as properties of coverings of C_d, or equivalently, random regular graphs.

CHAPTER 8

Conclusion

Before concluding remarks, we mention four things which may be of interest to the engaged reader. First, the probability bound from the Dixon-Babai theorem can be explicitly computed up to any order term using a computational technique shown in [**Dix**, **2005**]. We have focused on the first term for ease of proof. Second, the reader may have noticed that in our proofs pertaining to edge expansion and δ-connectivity, we use the fact that the action of $\mathcal{S}_n$ or $\mathcal{A}_n$ is highly transitive on $\{1, \ldots, n\}$. Such actions are rare, so cannot immediately generalize our techniques to voltages in other groups. However we do not explicitly *need* high transitivity, but rather a much weaker condition: that the action of the permutation group can send any set of size, say k, to some different such set. Clearly k-transitivity implies this, but group actions such as these, which we call *k-different*, should be much more common and our techniques should generalize well. Third, as the degree of the covering goes to infinity, the proportion of covering graphs which are iterated coverings goes to zero. This means that the work we did was necessary: there is no trivial reason by which a.a.s. results for random coverings must also hold for iterated random coverings. Fourth, our technique in the proof of δ-connectivity does not seem to work for $\delta = 3$ or 4, it may be possible to tighten some of the bounds to achieve this.

The interplay of groups and random covering graphs has been very fruitful. Chapter 2.2 contains a summary of the new results for random covering graphs, while Chapters 4 and 7 show how it lead to new ideas and results in group theory and topology respectively. There is much that can still be done in several directions and many entirely new avenues have been opened up for exploration:

1. **The Design and Analysis of Randomized Algorithms**
   Most known results from literature about random covering graphs give probability estimates of the form $1 - o_n(1)$; we give actual rates of convergence to one, making it possible to analyze randomized algorithms which require the construction of δ-connected random covering graphs.
2. **Properties of Random Covering Graphs**
   We focused on connectivity properties, but our technique of studying coverings through random permutations or random permutation groups is very likely to have wider applications. For example, it is a conjecture of Linial stated in [**LWW**, **2015**] that a.a.s. random coverings of d-regular graphs are hamiltoninan if $d \geq 3$. They show the best known result, which is for $d \geq 5$ where the graph has two edge disjoint hamiltonian

cycles which do not form a bipartite graph. With only a little more work, our methods show that a.a.s. coverings of a hamiltonian graph with at least one parallel edge in a hamilton cycle are hamiltonian. It is likely possible to improve this result. Also, the very popular method of word maps used to study expansion properties of covering graphs could be simplified using our techniques, possibly leading to improved results.

3. **Group Theory**
   The connections we show between covering graphs and groups motivate the study of wreath products of general groups, k-different group actions and transitivity properties of randomly generated groups in a new way. It would also be of independent interest to complete the generalization of the Dixon-Babai theorem to wreath products of symmetric groups, a crucial step of which has been proved in Theorem 4.11.
4. **Topology of Random Covering Spaces**
   The construction of random covering spaces of simplicial complexes, as attempted in [**AL**, **2002**], has proved hitherto intractable. Our topological viewpoint might help overcome these challenges. Since random graphs can by described by assigning permutations to edges outside a spanning tree, which are in bijection with the generators of the first homology group, we think similar methods of construction based on higher homology groups could work for describing random covering spaces of general simplicial complexes. Finally, continuing the study of homotopy invariants in random covering graphs as initiated in this thesis would be important for further understanding the interaction of homology and randomization.

Bibliography

[AKK, 2008] S. Arora, S. Khot, A. Kolla, D. Steurer, M. Tulsiani, and N. Vishnoi. 2008. *Unique games on expanding constraint graphs are easy.* In Proceedings of the fortieth annual ACM Symposium on Theory of Computing, pp. 21-28.

[AL, 2002] Alon Amit and Nathan Linial. 2002. *Random Graph Coverings I: General Theory And Graph Connectivity.* Combinatorica 22(1):1–18.

[AL, 2006] Alon Amit and Nathan Linial. 2006. *Random Lifts of Graphs: Edge Expansion.* Combinatorics, Probability and Computing, 15: 317-332.

[ALM, 2002] A. Amit, N. Linial, and J. Matouek. 2002. *Random lifts of graphs: independence and chromatic number.* Random Structures and Algorithms, 20(1):1-22.

[Bab, 1989] Lazlo Babai. 1989. *The Probability of Generating the Symmetric Group.* Jounral of Combinatorial Theory, Series A, 52: 148-153.

[BL, 2006] Y. Bilu and N. Linial. 2006. *Lifts, discrepancy and nearly optimal spectral gap.* Combinatorica, 26(5):495-519.

[Bol, 1981] B. Bollobas. 1981. *Random graphs.* Combinatorics, London Mathematical Society Lecture Note Series, 52, Cambridge University Press, Cambridge, 80-102.

[BS, 1987] Andrei Broder and E. Shamir. 1987. *On the Second Eigenvalue of Random Regular Graphs.* Proceddings of the Twenty-Eighth Annual IEEE Symposium on the Foundations of Computer Science, 286-294.

[Cam, 1981] P.J. Cameron. 1981. *Finite Permutation Groups and Finite Simple Groups.* Bulletin of the London Mathematical Society 13: 1-22.

[DF, 1984] D. Dummit and R. Foote. 2004. *Abstract Algebra.* Wiley.

[Dix, 1969] John Dixon. 1969. *The Probability of Generating the Symmetric Group.* Mathematische Zeitschrift 110(3): 199-205.

[Dix, 2005] John Dixon. 2005. *Asymptotics of Generating the Symmetric and Alternating Groups.* Electronic Journal of Combinatorics 12:56.

[FKS, 1989] J. Friedman, J. Kahn and E. Szemeredi. 1989. *On the Second Eigenvalue of Random Regular Graphs.* Proceedings Twenty-First Annual ACM Symposium on Theory of Computing, 587-598.

[Fri, 2003] J. Friedman. 2003. *Relative expanders or weakly relatively Ramanujan graphs.* Duke Mathematical Journal, 118(1):19-35.

[GT, 1987] Jonathan Gross and Thomas Tucker. 1987. *Topological Graph Theory.* Courier Dover Publications.

[HPS, 2016] C. Hall, D. Puder, and W. Sawin. 2015. *Ramanujan Coverings of Graphs.* arXiv:1506.02335, to appear at STOC 2016.

[LM, 2006] N. Linial and R. Meshulam. 2006. *Homological connectivity of random 2-complexes.* Combinatorica, 26(4):475-487.

[LR, 2005] N. Linial and E. Rozenman. 2005. *Random lifts of graphs: perfect matchings.* Combinatorica, 25(4):407-424.

[Luc, 1992] T. Luczak. 1992. *Sparse random graphs with a given degree sequence*. Random Graphs Vol. 2, Wiley, New York, 165-182.

[LWW, 2015] T. Luczak, L. Witkowski, and M. Witkowski. 2015. *Hamilton cycles in random lifts of graphs*. European Journal of Combinatorics, 49:105-116.

[Mak, 2015] Aleksandar Makelov. 2015. *Expansion in lifts of graphs*. Senior Thesis, Harvard University.

[Mar, 1973] G. A. Margulis. 1973. Explicit construction of concentrators. Problemy Peredachi Informatsii 9(4):71-80. (English translation: Problems of Information Transmission, Plenum, New York (1975)).

[MSS, 2015] A. Marcus, D. Spielman, and N. Srivastava. 2015. *Interlacing families I: Bipartite Ramanujan graphs of all degrees.* Ann. of Math. 182(1):307-325.

[MW, 2009] R. Meshulam and Nathan Wallach. 2009. *Homological connectivity of random kdimensional complexes.* Random Structures and Algorithms 34(3):408-417.

[Tre, 2014] Luca Trevisan. 2014. *Lecture notes on expansion, sparsest cut, and spectral graph theory.* Lectures Notes, University of California, Berkeley.

[Wit, 2010] L. Witkowski. *Random Coverings of Graphs*. DIMAP Workshop on Extremal and Probabilistic Combinatorics, 2010.

APPENDIX A

A Theorem of Babai

THEOREM A.1. *The probability that l random permutations generate a primitive group other than $\mathcal{A}_n$ or $\mathcal{S}_n$ is* $O\left(\left(\frac{n^{\sqrt{n}}}{n!}\right)^{l-1}\right)$.

First we state the following fact about characteristically simple groups, which are products of isomorphic simple groups.

FACT A.2. *The number of simple groups of order $\leq m$ is $O\left(\frac{m}{\log(m)}\right)$. In particular, the number of characteristically simple groups of order $\leq m$ is $O\left(\frac{m}{\log(m)}\right)$.*

Now define two permutation groups $\mathcal{G}$, $\mathcal{H}$ which act on S and T respectively to be equivalent if there is a bijection $\varphi : A \to B$ such that $\varphi^{-1}\mathcal{G}\varphi = \mathcal{H}$.

CLAIM A.3. *The number of inequivalent characteristically simple transitive permutation groups of order $\leq m$ is $O\left(m^{1+\log(m)}\right)$.*

To derive this claim we need a result from elementary group theory.

LEMMA A.4. *Suppose $\mathcal{G}$ acts transitively on the two sets X and Y. Let $\mathcal{H}$ be the stabilizer of a point in the first action. Then the two actions are equivalent if and only if $\mathcal{H}$ is also the stabilizer of a point in the second action.*

PROOF. Let $\sigma : \mathcal{G} \to \mathcal{S}_X$ and $\tau : \mathcal{G} \to \mathcal{S}_Y$ be the permutation representations of the two actions. Let $\mathcal{H}$ be the stabilizer of $x \in X$. Suppose there exists an equivalence of the actions given by a bijection $\varphi : X \to Y$. Let $h \in \mathcal{H}$, then $\varphi(\sigma(h)(x)) = \varphi(x) = \tau(h)(\varphi(x))$, where the first equality is due to the fact that $\mathcal{H}$ is the stabilizer of x and the second because φ is an equivalence between the actions. This shows that H is indeed the stabilizer of $\varphi(x) \in Y$. Conversely suppose that $\mathcal{H}$ is the stabilizer for $x \in X$ and $y \in Y$. Define $\varphi : X \to Y$ by $\varphi(\sigma(g)x) = \tau(g)y$ for all $g \in \mathcal{G}$. First note that φ is well-defined because $\sigma(g)x = \sigma(g')x$ implies that $\sigma(gg'^{-1})(x) = x$ and therefore $\tau(gg'^{-1})(y) = y$ and φ is defined for all points in $\mathcal{S}_X$ since the action σ is transitive. The previous statement in fact also shows that φ is injective. It is surjective because τ is transitive. Finally, we show that φ is indeed an equivalence of actions. We know that for all $z \in X$ there exists a $g \in \mathcal{G}$ such that $\sigma(g)x = z$, so for each $k \in \mathcal{G}$ we have that, $\varphi(\sigma(k)z) = \varphi(\sigma(k)\sigma(g)x) = \varphi(\sigma(kg)x) = \tau(kg)y = \tau(k)\tau(g)y = \tau(k)(\varphi(\sigma(g)x)) = \tau(k)(\varphi(z))$, which concludes the proof. $\square$

PROOF OF CLAIM A.3. The lemma says that a transitive representation of a permutation group is determined up to equivalence by the choice of the stabilizer subgroup of a point. So the number of subgroups of a group certainly bounds the number of its inequivalent transitive permutation representations. Note that the number of subgroups of a group of order m is $\leq m^{\log(m)}$ because any subgroup can be generated by $\log(m)$ elements. The claim follows. $\square$

A primitive subgroup of $\mathcal{S}_n$ is called maximal if it is maximal among the primitive groups other than $\mathcal{S}_n$ and $\mathcal{A}_n$.

LEMMA A.5. *The number of inequivalent maximal primitive groups of degree n is less than $2^{\log^4(n)(1+o(1))}$.*

PROOF. This proof requires rather technical results from the classification of finite simple groups. We will sketch the proof and the details may be obtained from [**Bab**, **1989**]. Let $\mathcal{M}$ be a maximal primitive group of degree n. We consider the two cases:

1. Let $\mathcal{M}$ act on the sth power of the set of all r-subsets (for $r \leq \frac{k}{2}$) of a k element set as the product action of the wreath product $\mathcal{S}_k \wr \mathcal{S}_s$. Here we know that $n = \binom{k}{r}^s$ and therefore $rs < 2\log(n)$. So the number of choices for k and s is less than $4\log(n)$, and these determine $\mathcal{M}$ up to equivalence.
2. We can use Theorem 6.1 of [**Cam**, **1981**] to show that in all remaining cases that $|\mathcal{M}| \leq 2^{\log^2(n)(1+o(1))}$. Now let $\mathcal{N}$ be a minimal normal subgroup of $\mathcal{M}$. Clearly $\mathcal{M}$ is the normalizer of $\mathcal{N}$ in $\mathcal{S}_n$, and therefore it is uniquely determined by $\mathcal{N}$. But $\mathcal{N}$ is a minimal normal subgroup, and therefore characteristically simple. Now we may use Claim A.3 to deduce that the possibilities for $\mathcal{M}$ are at most $(2^{\log^2(n)(1+o(1))})^{1+\log(2^{\log^2(n)(1+o(1))})} = 2^{\log^4(n)(1+o(1))}$.

Clearly the number of possibilities from the second case dominate the possibilities from the first case, and the lemma follows. $\square$

CLAIM A.6. *If $\mathcal{M}$ is a permutation group of degree n, then the number of subgroups of $\mathcal{S}_n$ which are equivalent to $\mathcal{M}$ is $\leq \frac{n!}{|\mathcal{M}|}$.*

PROOF. Two elements of $\mathcal{S}_n$ will produce the same conjugate of $\mathcal{M}$ if and only if they belong to the same coset of the normalizer of $\mathcal{M}$ in $\mathcal{S}_n$. Therefore the number of subgroups equivalent to $\mathcal{M}$ is the index of the normalizer of $\mathcal{M}$ in $\mathcal{S}_n$. The claim follows since the size of the normalizer is certainly greater than $|\mathcal{M}|$. $\square$

Let $\mathcal{M}$ be a permutation group of degree n. Note that the probability that l random permutations generate a subgroup of a group which is equivalent to $\mathcal{M}$ is less than $\left(\frac{|\mathcal{M}|}{n!}\right)^{l-1}$. This is because the probability that all of these permutations is in $\mathcal{M}$ is less than $\left(\frac{|\mathcal{M}|}{n!}\right)^{l}$ and there are $\frac{n!}{|\mathcal{M}|}$ groups equivalent to $\mathcal{M}$. This tells us that the probability that l random permutation generate a subgroup of $\mathcal{S}_n$ other than $\mathcal{S}_n$ or $\mathcal{A}_n$ is,

$$\sum_{\rho} \left(\frac{|\mathcal{M}|}{n!}\right)^{l-1}$$

where the sum is taken over all inequivalent maximal primitive permutation groups. Again we refer to Theorem 6.1 in [**Cam**, **1981**] to say that size of the largest such group is $\leq 2(\sqrt{n}!)^2$, and all other such groups have order less than $n^{\sqrt{\frac{n}{2}}}$. Then, using Lemma A.5 we may bound this sum by,

$$\left(\frac{2(\sqrt{n}!)^2}{n!}\right)^{l-1} + 2^{\log^4(n)(1+o(1))}\left(\frac{n^{\sqrt{\frac{n}{2}}}}{n!}\right)^{l-1} = O\left(\left(\frac{n^{\sqrt{n}}}{n!}\right)^{l-1}\right)$$

This concludes the proof of Theorem A.1. $\square$

APPENDIX B

Deferred Proofs: Wreath Products Through Rooted Trees

LEMMA B.1. *The automorphism group of $T_{S_1,\ldots,S_n}$ generated by the action of $\mathcal{G}_{i+1}$ on $(s_1,\ldots,s_i)$ is $\mathcal{G}_n \wr \cdots \wr \mathcal{G}_1$. It is a permutation group on on the set of leaves, which may be indexed by $S_1 \times \cdots \times S_n$.*

PROOF. The case $n = 1$ is trivial. For $n = 2$ the proof follows from the definition of the action of $\mathcal{G}_2 \wr \mathcal{G}_1$ on $S_1 \times S_2$. The leaf (s_1, s_2) is sent to $(\pi(s_1), \mu_{s_2}(s_1))$ by the action of $(\mu, \pi) \in \mathcal{G}_2 \wr \mathcal{G}_1$, and also by first permuting the children of the root by π, and then permuting each of the children of $s_2 \in S_2$ by μ_{s_2}. Since determining where the leaves go determines where their parents, their parents parents and so on must end up, we see that $\mathcal{G}_i \wr \cdots \wr \mathcal{G}_1$ realized as a permutation group on the leaves in fact determines the automorphism group of the tree up to depth i.

Now consider the case when $n > 2$. Given a tree $T_{S_1,\ldots,S_n}$, we may replace it with the two level tree $T_{S_1\times\cdots\times S_{n-1},S_n}$. Since, the automorphism group of the tree is determined by the permutation action on the leaves, so the automorphism group of $T_{S_1\times\cdots\times S_{n-1}}$ matches that of $T_{S_1,\ldots,S_{n-1}}$. From this we deduce that the automorphism group of $T_{S_1,\ldots,S_n}$ is the same as the automorphism group of $T_{S_1\times\cdots\times S_{n-1},S_n}$. Now we have reduced this problem to the case when $n = 2$, and we have that the automorphism group of $T_{S_1,\ldots,S_{n-1}}$ is $\mathcal{G}_{n-1} \wr \cdots \wr \mathcal{G}_1$ by hypothesis. The claim follows. $\square$

PROPOSITION B.2. *Suppose we have a sequence of covering graphs $G_n \to \cdots \to G_1 \to G$ where each G_i is obtained from its predecessor by a voltage assignment to a group of permutations $\mathcal{H}_i$ acting on a set S_i. Note that the degree of G_i as a cover of its predecessor is $|S_i|$. Then G_n is the derived graph of a voltage assignment of G to elements of $\mathcal{H}_n \wr \cdots \wr \mathcal{H}_1$ where the domain of their action is $S_1 \times \cdots \times S_n$. Conversely, any covering of graphs $G_n \to G$ which is the derived graph of a voltage assignment of $\mathcal{H}_n \wr \cdots \wr \mathcal{H}_1$ (with the action defined on on $S_1 \times \cdots \times S_n$) is an iterated covering as described above.*

PROOF. We will begin with the case $n = 2$, as when $n = 1$ there is nothing to prove. We prove the forward direction first. Consider a single edge e in G. The main intuition is that in the covering of a covering e must be assigned a permutation which is compatible with the intermediate covering map. Indeed, in the first covering e is assigned a permutation π from $\mathcal{H}_1$ acting on S_1 and it lifts to $|S_1|$ edges. For clarity we will consider the lifts of e as indexed by (e, s_i) where $s_i \in S_1$. One way to think of this as a well defined indexing is the following: suppose e connects $u \to v$ in G, then we may take (e, s_i) to be the lift of e with one end attached to (v, s_i). Now each lift (e, s_i) is assigned a permutation μ_{s_i} from G_2 acting on S_2. It is easy to see now that the $S_1 \times S_2$ lifts of e in the covering of a covering must be assigned permutations such that children of the copies of e in the intermediate covering are sent only to each other. Concretely, they must be assigned permutations σ such that,

$$\sigma(s_1, s_2) = (\pi(s_1), \mu_{s_1}(s_2))$$

But this is the same formula we obtain for permutations in the automorphism group of the tree T_{S_1,S_2} where the children of the root are permuted by a permutation of $\mathcal{H}_1$ on S_1, and each of their children is permuted according to the action of $\mathcal{H}_2$ on S_2. We know this automorphism group to be $\mathcal{H}_2 \wr \mathcal{H}_1$.

Conversely suppose that we have a covering $G_2 \to G$ of degree $|S_1 \times S_2|$ where the permutations on each edge are given by the action of $\mathcal{H}_2 \wr \mathcal{H}_1$ on $S_1 \times S_2$. Let G_1 be a covering graph of G defined the following way: if the edge e of G was assigned the permutation $(\mu, \pi) \in \mathcal{H}_2 \wr \mathcal{H}_1$ to create G_2, we now assign it only the permutation π. This clearly a covering of G. G_2 is seen to be a covering of G_1 by simply attaching the permutation μ_{s_i} (recall that $\mu \in \mathcal{H}_2^{|S_1|}$) to each lift (e, s_i) of e. Therefore we may view the covering $G_2 \to G$ created by the action of $\mathcal{H}_2 \wr \mathcal{H}_1$ on $S_1 \times S_2$ as an iterated covering $G_2 \to G_1 \to G$ created by the action of H_1 on S_1 and then $\mathcal{H}_2$ on S_2.

The inductive case reduces to the case when $n = 2$ with the observation that the composition of covering maps is a covering map. Suppose the statement is true for some $n = k$. Then given a covering $G_{k+1} \to \cdots \to G_1$, we may replace it by $G_{k+1} \to G_k \to G_1$ where $G_k \to G_1$ is obtained by the action of $\mathcal{H}_k \wr \cdots \wr \mathcal{H}_1$ on $S_1 \times \cdots \times S_k$ by the inductive hypothesis. But this is now the case when $n = 2$, which is already proved. Conversely, suppose we have a covering $G_{k+1} \to G$ created by the action of $\mathcal{H}_{k+1} \wr \cdots \wr \mathcal{H}_1$ on $S_1 \times \cdots \times S_{k+1}$. By the inductive hypothesis, we may replace with a covering $G_{k+1} \to G_k \to K$ where $G_k \to G$ is created by the action of $\mathcal{H}_k \wr \cdots \wr \mathcal{H}_1$ on $S_1 \times \cdots \times S_k$. This direction is now also reduced to the case when $n = 2$, which is proved above. $\square$