Expansion in lifts of graphs

submitted in partial fulfillment of the requirements

for the degree of Bachelor of Arts with Honors in

Mathematics and Computer Science

Advisor: Professor Salil Vadhan

Aleksandar Makelov
Harvard University
March 31 2015

To N, who let me go.

Acknowledgements

First, I'd like to thank my family for their love and encouragement, without which I wouldn't have been able to follow my passion for mathematics. Any success I've had is rooted in the effort they invested in my upbringing.

Next, this thesis would not have been possible without the support of my advisor, Professor Salil Vadhan, who pointed me to the topic, and spent many hours discussing the problems with me and guiding me through the research process. He has been an amazingly clear and dedicated teacher of mathematics and computer science, and an overall inspirational figure for me for the past three years.

I would also like to thank all my teachers in mathematics and computer science – both here at Harvard, for teaching me an immense amount of those sciences, and during high school, for sparking my interest in competitive math and combinatorics. Special thanks go to Konstantin Matveev, Professors Curtis McMullen and Yum-Tong Siu, and Dr. Emily Riehl.

Finally, I'd like to thank my friends and mentors in math and beyond, who have been an integral part of my undergraduate experience and have influenced me a great deal. Special thanks go to Arpon Raksit, for teaching me the value of abstraction, and to him and Joy Zheng for providing feedback on this thesis; and to my teachers in English, especially Peli Grietzer and Stephen Burt, who got me excited about science fiction, and Damon Krukowski, who got me excited about music.

More formally, I'd like to thank my thesis readers, Professors Dennis Gaitsgory and Leslie Valiant, and the following people for our brief conversations related to this thesis: Karthekeyan Chandrasekaran, Ameya Velingker, Curtis McMullen, Alexandra Kolla, Jonathan Kelner, Nikhil Srivastava, Avi Wigderson, and Jeff Erickson.

Abstract[1]

The central goal of this thesis is to better understand, and explicitly construct, *expanding towers* $G_1, G_2, \ldots$, which are expander families with the additional constraint that G_{n+1} is a *lift* of G_n. A lift G of H is a graph that locally looks like H, but may be globally different; lifts have been proposed as a more structured setting for elementary explicit constructions of expanders, and there have recently been promising results in this direction by Marcus, Spielman and Srivastava [**MSS13**], Bilu and Linial [**BL06**], and Rozenman, Shalev and Wigderson [**RSW06**]; besides that, expansion in lifts is related to the Unique Games Conjecture (e.g., Arora et al [**AKK$^+$08**]).

We develop the basic theory of spectral expanders and lifts in the generality of directed multigraphs, and give some examples of their applications. We then derive some group-theoretic structural properties of towers, and show that a large class of commonly used graph operations 'respect' lifts. These two insights allow us to give a different perspective on an existing construction [**RSW06**], show that standard iterative constructions of expanders can be adjusted to give expander towers almost 'for free', and give a new elementary construction, along the lines of Ben-Aroya and Ta-Shma [**BATS11**], of a fully-explicit expanding tower of almost optimal spectral expanders.

[1] As required by the Computer Science concentration thesis guidelines.

Contents

CHAPTER 1

Introduction

Consider the problem of *noise* in communication. Suppose we have an unreliable channel that can damage the messages we send over it, but we know it's very unlikely to damage them *too much*; many channels in the real world have this property. Intuitively, by introducing redundancy in our messages, error-free communication should be feasible in this setting. It seems plausible that, with extreme redundancy, this task will become easy – but then the *efficiency* of our channel will be poor, as our messages will have to be very long, and it will thus take us more time and resources to deliver them! So, is there a clever way to achieve good results without greatly impairing the efficiency of communication?

Question 1.1. How do we introduce redundancy efficiently?

In the world of algorithms, *randomness* has been very useful - there are many practical tasks we don't know how to solve feasibly without it, and it is indispensable in *cryptography*, where it's not even clear how to define a secret without randomness. The software random number generators used by most computers are not *truly random*; they are based on complex, yet deterministic, functions, which are subject to attacks. So it is desirable to be able to extract 'real' randomness from unpredictable physical processes, like quantum phenomena. This is the motivation behind *hardware random generators*. But they can only generate a limited amount of randomness per unit time!

Question 1.2. Can we somehow reduce the amount of pure randomness our algorithms require while preserving performance?

For many important computational problems, we know how to efficiently *recognize* a solution, but we don't have an algorithm to *efficiently find* one, and in fact most researchers believe such algorithms don't exist; this is the famous **P** versus **NP** question. Naturally, we can hope that by relaxing the problem and looking for an *approximate* solution instead, we can avoid that hardness; and indeed approximate solutions are often almost as useful in practice. But this approach also has limitations: it turns out that, for some problems, we encounter the same sort of infeasibility barrier when we try to approximate them too well!

Question 1.3. What are the limits of the power of approximation?

♠

Somewhat surprisingly, it turns out that we can give non-trivial answers to the above questions – as well as to many others – from the perspective of a single class of mathematical objects called *expander graphs*, or *expanders* for short. They can be defined in many ways; one is as graphs that share important properties with *random* graphs. Yet, we know how to construct them without any use of randomness! This already sounds like the beginning of an answer to Question 1.2.

And while we know much more about expanders than we did several decades ago, they are still an active area of research, and there is more to be explored. The central problem has been constructing expanders *explicitly*, which is vital for most applications. And while we have very good explicit constructions of expanders, they have relied on deep mathematical results; it seems that elementary constructions should exist, and should give us a better understanding of expansion.

In this thesis, we begin by developing the basics of the story of expanders and describing some of their exciting applications. Then we move on to the question of constructions. We will focus on a beautiful

technique, *lifts of graphs*, that was proposed by researchers in the early 2000s as a new way towards elementary constructions. We will discuss how lifts connect various lines of work on expanders, give a new perspective on an existing construction involving lifts, and, drawing inspiration from the latter, describe a general iterative technique for expander constructions that are lifts.

1.1. Why expander graphs?

Graphs are everywhere, and for a reason – they are the simplest abstractions of discrete, local interactions in a global domain, and many real-world systems and reductionist models we invent are understood through such interactions. Specifically, we see this in *statistical physics* (on the scale of atoms), *computer science* (communication networks), *the social sciences* (social networks such as Facebook), and *engineering* (chip design) to name a few areas. As mathematical objects, they are correspondingly fundamental to combinatorics, and graph theory has rich connections to many other subjects, like group theory (*Cayley graphs*) and topology (*as 1-dimensional complexes*) to name a few.

The last several decades have taught us that the world of large graphs – with which we are more and more often faced in applications – can look very mind-bendingly different from the small pictures we can draw and comprehend[1]. Among non-trivial asymptotic properties of graphs, **expansion** – the quality of being sparse yet very well connected – is one of the most ubiquitous. Here's one innocent-looking definition:

Definition 1.4 (Vertex expanders). For d a constant, an infinite family of d-regular graphs $G_1, G_2, \ldots$ with $|V(G_n)| \to \infty$ is called an **expander family** if there exists a constant $\alpha > 1$ such that for n and all $S \subset V(G_n)$ with $|S| \leq |V(G_n)|/2$ we have $|\Gamma(S)| \geq \alpha|S|$, where $\Gamma(S)$ is the set of vertices that have a neighbor in S.

So, in an expander family, we have a *uniform* bound – which is why we say expansion is an asymptotic property – of how much neighborhoods of sets that are not too big grow, or 'expand', relative to their size. The bigger α is, the better the expansion is. **Why are expanders so ubiquitous?** A possible hint is that there are many ways to define them:

- **combinatorial**: graphs that are sparse, but well-connected - as in the definition we just gave, and several equivalent ones. It turns out that this is a fundamental extremal property.
- **spectral**: sparse graphs with small second eigenvalue – and in this sense, sparse spectral approximations of the complete graph.
- **probabilistic**: graphs that 'look random', and also ones on which the standard random walk behaves similarly to independent random samples from the set vertices, and converges rapidly to the uniform distribution.
- **representation-theoretic**: quotients of a Cayley graph of a group with Kazhdan property (T).
- **geometric** : graphs that are hardest to metrically embed in Euclidean space without too much distortion. Intuitively, one reason for that is the similarity between our Definition 1.4 and hyperbolic space, where the volume of a ball is exponential rather than polynomial in the radius.

This richness of perspectives brings a richness of results and applications. And while the existence, and in fact abundance, of high-quality expanders can easily be established by probabilistic arguments – and indeed we have simple probability spaces where *almost all* random graphs are expanders – explicit constructions matching this quality have been difficult and have often relied on deep mathematical theory. Today, there are still open problems in the area, and there remains a lot to be understood.

"It's not finding a needle in a haystack, but finding hay in a haystack." – Avi Wigderson

[1]For example, Szemeredi's regularity lemma says that given any k, any large enough graph can be split into at least k subsets of approximately equal size such that the edges between them behave almost like random edges! As another example, for every c and g, there exist (large) graphs that cannot be colored with fewer than c colors, and don't contain cycles with fewer than g edges. Notice that the ball of radius $g/2$ at any vertex in such a graph looks like a tree, which can easily be colored in only two colors; yet the entire graph is very far from being 2-colorable!

What have expanders been good for?

1.1.1. For the working computer scientist... expander graphs are combinatorial objects that find diverse applications in complexity, cryptography, sampling, and algorithm design. Explicitness is fundamental to computation, and thus almost all applications demand explicit constructions of expanders. In general, *the better the expansion is* – e.g., the larger α is in Definition 1.4, and the smaller the second eigenvalue is – the *stronger results* we get in applications, and some applications require very strong expansion.

In *pseudorandomness* – the study of objects that 'look' random but can be constructed using little or no randomness – expanders are central objects. The main question of pseudorandomness is whether **P = BPP**, which essentially asks, 'If we can efficiently solve a problem using randomness, can we also do so without randomness?'. While expanders are not directly relevant to this question, they give us results on *randomness reduction*, that is, ways to reduce the use of randomness by a randomized algorithm in a way that preserves efficiency. This gives an answer to Question 1.2, and we shall see an example application of that idea in Subsection 2.1.1.

In *complexity theory* - the study of efficient computation – one striking result that came out of the study of expanders is the collapse **L = SL** of the complexity classes *symmetric logspace* and *logspace* by Reingold [**Rei08**]; another is Dinur's new proof of the **PCP** theorem [**Din07**]. The **PCP** theorem, considered one of the most important results in complexity, is the cornerstone of the theory of *hardness of approximation*, thus of key importance to Question 1.3.

The extremal combinatorial properties of expanders lead to explicit constructions of nice combinatorial objects across computer science. A major example is the construction of *error-correcting codes* (for example, by Parvaresh and Vardy [**PV05**]). This provides an answer to Question 1.1. Of course, we can't hope to cover everything here – and there is much more; the book [**HLW06**] by Hoory, Linial and Wigderson is an excellent survey of applications to theoretical computer science.

1.1.2. For the working mathematician... the original explicit constructions of expanders involved some deep machinery from representation theory and number theory, such as *Kazhdan property (T)* and the *Ramanujan conjectures*, which were used by Lubotzky, Phillips and Sarnak in [**LPS88**] to construct optimal *spectral expanders*. Expanders have more recently become the focus of some exciting applications to group theory, number theory and geometry; see the excellent survey by Lubotzky [**Lub12**].

1.1.3. For the student... the study of expander graphs is a great way to be exposed to, and learn, a lot of mathematics and computer science in a more motivated, focused and problem-driven way. It is amazing how broad the span of expanders is in terms of mathematical sophistication, diversity of subjects, and range of applications. This gives the student great flexibility in the choice of topic, level of difficulty and real-world problem that are most suitable to her current progress as a mathematician/computer scientist!

1.1.4. History. A property equivalent to expansion seems to have been first studied by Kolmogorov and Barzdin [**KB67**], who used it to analyze embeddings of thick graphs in three dimensions. Pinsker [**Pin73**] defined expanders as we know them, invented the name, and pioneered their application to problems about telegraphic networks. The first application of expanders to theoretical computer science was by Valiant [**Val76**], who used *superconcentrators* to give lower bounds for certain computational models.

Before the 2000s, the explicit constructions of expanders were dominated by algebraic techniques and deep mathematical results; we discuss this a bit in Section 5.3. Then Reingold, Vadhan, and Wigderson introduced the *zig-zag product* of graphs (which we will also use), that allowed them to give an elementary explicit construction of expander families. Since then, the zig-zag product has been applied in various contexts to give interesting families of expanders; one we will study closely in Section 5.1 is by Rozenman, Shalev and Wigderson [**RSW06**]; it turns out to be an instance of an expander construction based on *lifts*.

1.2. Why lifts?

The interaction between local and global properties is key to graph theory, and **lifting** is a beautiful way to preserve aspects of the local structure of a graph while introducing freedom to change the global structure. A lift of a graph G, also called a **cover** of G, is a graph H that looks locally like G, but globally may be different. Lifts turn out to allow us to build upon a given graph in a precise way: various nice statements can be made relating the combinatorics and spectra of a graph and its lifts. For this section, we focus on undirected simple graphs, as that makes the intuition clearer.

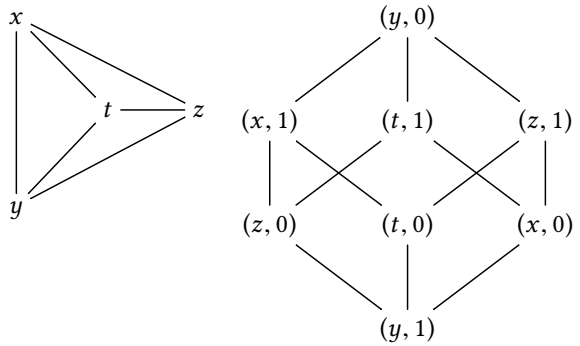
Covering spaces of topological spaces, and of graphs in particular, were first studied in algebraic topology, where they were related to the computation of fundamental groups; since then, they have found other applications across the subject. Here is the standard topological definition:

Definition 1.5 (Topological covering). A **covering space** of a space B is a space E with a continuous map $p : E \to B$ such that for every $x \in B$, there exists a neighborhood $x \in U$ such that $p^{-1}(U)$ is a disjoint union of open sets, each of which is mapped homeomorphically to U by p.

For those who are familiar with algebraic topology, keeping this definition in mind will be helpful, as many of our combinatorial results are special cases of general facts about covering spaces. We obtain the definition of a lift of a graph G when we let B in the above definition be the topological realization of G as a 1-dimensional simplicial complex. However, topological considerations have little direct relevance to the current work – in topology, one is usually concerned with spaces up to *homotopy* equivalence, which is too weak to capture the properties we want to study. So, we end with the formal discussion of topology here, and refer the interested reader to the wonderful book by Hatcher [**Hat02**].

What a covering amounts to combinatorially is more useful. Recall that for graphs G and H, a *graph homomorphism* f, denoted $f : G \to H$, is a pair of maps $f_V : V(G) \to V(H)$ and $f_E : E(G) \to E(H)$ that respect incidence, that is, whenever $v \in V(G)$ is incident to $e \in E(G)$, $f_V(v)$ is incident to $f_E(e)$.

Definition 1.6 (Combinatorial covering). A **lift** of a graph G is a graph H with a surjective graph homomorphism (adjacency preserving map) $p : H \to G$ which is locally an isomorphism, i.e. such that for every $v \in V(H)$, the edges incident to v are mapped bijectively to the edges incident to $p(v)$.



In the example above, we see how the cube graph C covers the tetrahedron graph T; the names of the vertices tell us what the map is: for $i \in \{0, 1\}$, (x, i) maps to x, (y, i) maps to y, and so on. We see that, if we forget the second coordinates of the vertices on C, the neighborhood of every vertex looks the same as the neighborhood of the vertex with the same name in T.

It may not seem from the outset that lifts are the right way to build a big graph using a small graph as a 'foundation' , but we will see that they have a range of beautiful and useful properties. Over the

last decade, lifts have turned out to be a meaningful model of random regular graphs[2] with interesting parameters, as shown by Alon, Linial and Matousek [**ALM**], Amit and Linial [**AL06**], and Linial and Rozenman [**LR05**] – and especially ones related to expansion, as shown by Friedman [**F⁺03**], Bilu and Linial [**BL06**], Linial and Puder [**LP10**], Marcus, Spielman, and Srivastava [**MSS13**], and Agarwal, Kolla and Madan [**AKM13**]. An idea that emerged from this line of work is to construct expander families by starting with a 'good' graph, and repeatedly lifting it in a way that preserves expansion, thus obtaining an infinite 'tower' of expanders. The papers we mentioned tell us that random lifts of good expanders tend to be good expanders as well, and that spectrally optimal expanders can be realized as such towers of lifts. As an application to the theory of expanders itself, lifts can be used to derive *lower* bounds on expansion, as we'll see in Section 2.6.

Finally, a major motivation behind the study of lifts is researchers' belief they will lead to explicit constructions by *elementary means*, in contrast to the deep classical constructions, and thus improve our understanding of expansion. Here, the picture is not nearly as complete as in the probabilistic world, and there have been two main explicit constructions that involve lifts, by Bilu and Linial [**BL06**], and by Rozenman, Shalev and Wigderson [**RSW06**]; jump to the introduction of Chapter 5 for context.

Thus, the questions one usually asks in this context are: *given a graph G, do there exist lifts of G that achieve very good expansion? how can we explicitly construct such lifts? which graphs G have expanding lifts?*

1.3. This thesis

...the sea advances insensibly in silence, nothing seems to happen, nothing moves, the water is so far off you hardly hear it...yet it finally surrounds the resistant substance. [Grothendieck 1985-1987, pp. 552-3]
[**McL03**]

An *expander tower* is an expander family $G_1, G_2, \ldots$ where there is a covering map $G_{n+1} \to G_n$ for every n. The central goal of the thesis is to understand expander towers better, and obtain constructions and existence results about them.

We begin by developing the basic theory of *spectral* expanders in the generality of directed multigraphs, *digraphs* for short; this requires more effort than the undirected simple case, but pays off later. In this setting, we describe some abstract properties of covering maps related to existing themes in the theory of expanders, namely the study of spectra of lifts, constructions based on graph operations, and group-theoretic constructions involving *Cayley/Schreier* graphs. Every individual proof feels almost trivial, but little by little they accumulate to the main contribution: a perspective that gives us clearer understanding of a somewhat 'mysterious' existing construction based on lifts, and ways to generalize it and simplify it.

In Chapter 2, we establish the basics. We...

- give an example application of expanders to answer Question 1.2, following Hoory, Linial and Wigderson [**HLW06**].
- develop the basics of spectral expanders, mostly following Vadhan [**Vad12**].
- define covering maps of digraphs, and study their well-known spectral properties; we also present an approach for lower bounds on expansion via lifts, following Friedman and Tillich [**FT05**].

In Chapter 3, we establish some algebraic properties of expanding towers. We...

- present a formalism, the *voltage assignments* of Gross and Tucker [**GT87**], for describing restricted classes of coverings. Lifting a graph G can be thought of as assigning a permutation from $\mathrm{Sym}(n)$ to every edge, and replacing this edge by a perfect matching $\{1, \ldots, n\} \to$

[2] The old workhorse of the theory of random graphs, the Erdős-Rényi model, has given us some great results, but it is not clear how to adapt it to a model of regular graphs!

$\{1, \ldots, n\}$ given by this permutation. Voltage assignments describe lifts where we restrict the permutations to a subgroup $\mathcal{G} \subset \mathrm{Sym}(n)$.

- present a representation-theoretic description of the spectrum of a lift obtained via voltage assignment; the proof is following Mizuno and Sato[**MS95**]. This generalizes the existing in the expander literature descriptions discovered by Bilu and Linial [**BL06**] and Agarwal, Kolla and Madan [**AKM13**], which turn out to correspond to voltage assignments in cyclic groups[3].
- show that the effect of repeated lifting on the group in a voltage assignment is a nice group operation, the *wreath product*, which is a special case of the *semidirect product*.

In Chapter 4, we establish relationships between coverings and various graph operations. We...

- show that a large class of graph operations typically used in iterative constructions of expanders, including *powering*, *tensor products*, the *zig-zag product*, and the *derandomized square*, respect covering maps. That is, whenever we have a covering $p : G \to H$, and α is one of the above operations that can be applied to both G and H, we get a covering $p : \alpha(G) \to \alpha(H)$. We note that the fact about the zig-zag product was independently observed by [**CDP06**]; the other results seem to be missing from the literature, but the proofs are easy.
- introduce two simple operations, the *backward-forward square* and *undirecting* (the latter following Ben-Aroya and Ta-Shma [**BATS11**]), that allow us to obtain expander towers of undirected graphs from expander towers of digraphs without losing too much spectral expansion. This shows that constructing expander towers of directed graphs is about as interesting as constructing such towers of undirected graphs.
- develop basic language from *category theory*, which allows us to express the niceness of graph operations with respect to coverings more concisely using *functors*.

In Chapter 5, we bring together the insights from the previous chapters, and apply them to show constructibility and existence of certain new expanding towers. We...

- apply the insights from Chapters 3 and 4 to provide a more abstract view of the Rozenman-Shalev-Wigderson [**RSW06**] construction of expanding towers of *Schreier* graphs of iterated wreath products.
- describe the main contribution: a general technique, inspired by the construction of Rozenman, Shalev and Wigderson, to explicitly construct expander towers using graph operations. While in [**RSW06**] they use some nontrivial properties of wreath products to guarantee explicitness, if we implement our technique 'right', we're able to use a simpler argument instead. We then proceed to use the technique to show the existence of fully explicit towers of almost optimal spectral expanders. It seems this has not been observed before in an elementary way.
- show that an existence result about spectrally optimal *bipartite*[4] expander towers of undirected simple graphs by Marcus, Spielman and Srivastava [**MSS13**] generalizes to undirected multigraphs, using our description of the spectrum of a lift from Chapter 3. Then using the effect of repeated lifting on the voltage assignment group, we get the existence of bipartite Schreier expanders of $\mathbb{Z}/2$; again, this seems to not have been known in an 'elementary' way (though one can argue how elementary the paper [**MSS13**] is) .
- outline how one can get expander towers from the classical constructions of expanders, and how one can get *new* towers from these towers.

The background we assume is basic linear algebra, group theory, graph theory, probability, and complexity theory; the aim is for the exposition to be accessible to mathematicians and computer scientists alike.

[3] It seems that researchers in expanders and researchers in voltage assignments don't talk much to each other and ended up solving the same problems twice :)

[4] *Bipartite expanders* are weaker than expanders, but still useful for some applications.

CHAPTER 2

Expanders: a first encounter

2.1. A taste of the magic

In an attempt to seize the attention of even the most apathetic reader for the rest of this thesis, here we outline one application of expanders; this was more or less the first encounter of the author with these objects, and the one that made him so enthusiastic about the topic in the first place.

2.1.1. The problem: derandomization in RP. One of the main achievements of theoretical computer science is the theory of randomized algorithms. For many important problems, we have efficient randomized algorithms, while the best known deterministic-time algorithms take prohibitively long to finish; and in cases when we have deterministic algorithms of matching complexity, the randomized ones tend to be simpler. There are whole fields which have no foundation without randomness, such as cryptography, where it's not even clear how to define a 'secret' if one is not allowed to randomize. Yet, history has taught us that often after an efficient randomized solution to a problem is found, a deterministic one is around the corner. A central question, related to our motivating Question 1.2, is whether randomness is as useful as it seems, and in fact most researchers believe that we can dispense of it altogether; recall that formally this says that **P** = **BPP**. Here **P** is the class of decision problems[1] solvable in *polynomial-time*, which intuitively captures properties we can efficiently decide deterministically. **BPP** is the class of decision problems solvable by a randomized algorithm in *polynomial-time* with high probability and two sided error; that is, whatever the real answer to the decision problem is, a **BPP** algorithm is allowed to make a mistake with some small probability. Intuitively, **BPP** captures properties we can efficiently decide with randomness.

But, perhaps most intriguingly, the study of pseudorandomness is also linked to purely deterministic fundamental problems. For example, there is an equivalence between *pseudorandom generators* and hardness results (e.g., Nisan and Wigderson [**NW94**]). Outside of computer science, attempts to dispense of randomness lead to explicit constructions of interesting combinatorial objects. We refer the curious about pseudorandomness reader to the wonderful monograph by Vadhan [**Vad12**].

In this setting, reductions in the use of randomness can have interesting implications! Here, we'll present a classical application of expanders to give a partial answer to Question 1.2. We'll focus on a cousin of **BPP**, the class of decision problems that can be efficiently solved with *one-sided* error:

Definition 2.1. **RP** is the class of decision problems L such that there exists a polynomial-time randomized algorithm $\mathcal{A}$ using a string r of $r(n)$ random bits on inputs of length n, and a constant $1 > \varepsilon > 0$ such that

$$x \notin L \implies \mathbf{Pr}_r\left[\mathcal{A}(x, r) = 0\right] = 1 \text{ and } x \in L \implies \mathbf{Pr}_r\left[\mathcal{A}(x, r) = 0\right] \leq \varepsilon$$

Problem 2.2. Suppose we're handed a black box that implements an **RP** algorithm $\mathcal{A}$ for the decision problem L that uses $r(n)$ random bits on inputs of size n, and fails with probability $\leq 1/6$. How many more random bits do we need to reduce the failure probability to any given ε?

[1] A **decision problem** requires from us to give an algorithm that decides membership in some language $L \subset \{0,1\}^*$; for example, we can encode boolean formulas using 0s and 1s, and let L be the language of all satisfiable boolean formulas.

2.1.2. A solution following Hoory-Linial-Wigderson [HLW06]. One natural thing to do is independent repetitions: we can run the algorithm about $k = \log_2 1/\varepsilon$ times with independent random bits to bring down the error probability to $1/2^k = \varepsilon$; but this requires $kr(n)$ random bits. Can we do better than that?

It turns out that if we're willing to wait longer, we can solve the problem *with no additional random bits* beyond the $r(n)$ required by the algorithm! More precisely, we will show how to bring the failure probability to $O(1/d)$ for any given constant d using d repetitions. We will use a single $r(n)$-bit random string to obtain many dependent random strings, and run the algorithm with each; but our dependent strings will be chosen in a very special way.

Definition 2.3. We say that a bipartite graph $G = (L, R, E)$ with $|L| = |R| = n$ where each vertex in the left part L has d neighbors is an (n, d, α, β)–**expander** if for every $S \subset L$ with $|S| \leq \frac{n}{\alpha d}$ we have $|\Gamma(S)| > \beta d|S|$.

Now believe us that for every $d \geq 200$, we can take a $G_n = (L_n, R_n, E_n)$ which is a $(2^{r(n)}, d, 3, 1/2)$-expander for all n large enough, and moreover, *we can compute the neighbors of $l \in L_n$ in time polynomial in* $\log |L_n|$. The existence of such graphs follows by a simple counting argument; a very similar one is presented in [**HLW06**], to which we refer the interested reader. If you believe us, you're ready to go into the next proof:

Proposition 2.4 (Error reduction in **RP**). *In the terminology of 2.2, for every $d \geq 200$, there is an* **RP** *algorithm that uses $r(n)$ random bits, runs $\mathcal{A}$ d times on x, and has error probability $\leq \frac{1}{3d}$.*

Proof. With G_n as above, our strategy is simple: using $r(n)$ random bits, pick a uniformly random $l \in L_n$, let $r_1, \ldots, r_d$ be its neighbors in R_n, and return $\bigvee_{i=1}^{d} \mathcal{A}(x, r_i)$.

What's the probability of failure? We know there is a set $B_R \subset R_n$ with $|B_R| \leq |R_n|/6$ of 'bad' random strings that fool the algorithm. Thus a string $l \in L_n$ will fail iff all its neighbors are in B. So let

$$B_L = \left\{ l \in L_n \;\middle|\; \Gamma(l) \subset B_R \right\}$$

be the set of bad strings on the left. The key point is that the expansion property forces B_L to be smaller than B_R! Indeed, suppose that $|B_L| > \frac{|L_n|}{3d}$. Then we have

$$|R_n|/6 \geq |B_R| \geq |\Gamma(B_L)| \geq |\Gamma(B'_L)| > \frac{1}{2} d \frac{|L_n|}{3d} = |L_n|/6$$

where B'_L is any subset of B_L of size $\frac{n}{3d}$. But this is a contradiction! Thus, the failure probability is $|B_L|/|L_n| \leq 1/3d$. □

2.1.3. Discussion. This might seem like magic, but we cheated a bit – how do we 'take' a graph on $2^{r(n)}$ vertices? We can't hope to store it in memory! But what we really needed from the graph was, given a vertex name, a list of that vertex's neighbors. This is not that obviously infeasible, since vertex names are $r(n)$ bits long.

In fact, it turns out that this level of explicitness is achievable! Moreover, in some applications of expanders, exponentially-sized graphs are not an issue. This motivates the following terminology:

Definition 2.5 (Explicitness). An expander family $(G_n)_{n \in \mathbb{N}}$ is **mildly explicit** if we can construct G_n in time $\text{poly}(|V(G_n)|)$, and **fully explicit** if we can compute the i-th neighbor of a vertex $v \in V(G_n)$ in time $\text{polylog}(|V(G_n)|)$.

Explicitness has merits beyond coping with huge graphs; for many applications of expanders (like the one we just saw), the purpose is to reduce the use of randomness – so even though a typical graph is an expander, picking one at random defeats the point. Moreover, being able to write down new expanders explicitly feels like we *understand* expansion better.

The other important aspect of expansion this application illustrates is that it is an *asymptotic* notion; this requirement came very naturally from the fact that we quantify computational resources asymptotically in complexity theory. Most applications outside complexity also require a uniform bound on expansion for larger and larger graphs – and it's not interesting to say that a single graph is an 'expander', because any graph will have some expansion as long as it's connected (Proposition 2.15); when we say that, we usually mean it has 'small' spectral expansion in the current context.

Finally, we remark that our example doesn't illustrate the full power of expanders: an analogous error reduction result can be achieved by limited independence techniques - see Motwani & Raghavan [**Mot95**]. But it is possible, using a k-step random walk on an expander (instead of the one-step walk we used in this application) to achieve error $\leq 1/2^k$ with $r(n) + k$ random bits! We don't know how to do that without expanders; see Vadhan [**Vad12**].

2.2. Digraphs

In this section, we lay out some of the more specific terminology we'll be using to describe graphs. Many of our results are true for finite **directed multigraphs**, or **digraphs** for short, so to keep things general, *this will be our default notion of a graph unless otherwise specified.* This will introduce some more complicated notation, but what we gain from the additional abstraction far outweighs the effort we put into setting it up:

(1) Certain multigraphs, like the bouquet of circles, will be of key importance in our constructions;
(2) For many special cases, like *Cayley* and *Schreier* graphs, it is far more natural to work with directed graphs;
(3) For the most part, the theory of directed expanders and their covering properties is a proper generalization of the theory of undirected ones, so we don't lose much from the story of undirected expanders either. Moreover, we'll show how to get undirected expanding towers from directed ones.

Still, sometimes we'll restrict to undirected and/or simple graphs. A **directed** graph carries one-way orientations on its edges that walks on the graph must respect; in an **undirected** graph, edges can be traversed in both directions. A **multigraph** is allowed to have multiple edges and self-loops; a **simple** graph is not.

We will usually denote digraphs as $G = (V(G), E(G))$, where $V(G)$ is the set of vertices and $E(G)$ is the set of edges. We will write $u \xrightarrow{e} v$ for a directed edge e oriented from u to v. For an edge $u \xrightarrow{e} v$, we denote the **tail** (also called **source**) of e by $e^- = u$, and the **head** (also called **target**) of e by $e^+ = v$. We will treat undirected graphs as special cases of digraphs where for every edge $u \longrightarrow v$ with $u \neq v$ there is a corresponding edge $v \longrightarrow u$; we will call such a digraph together with the pairing of its edges an **undirected digraph**. Given such a digraph, the corresponding undirected graph is obtained by collapsing pairs of opposite edges into single undirected edges, and forgetting the direction of loops. The theory of directed expanders usually descends to the theory of undirected ones under this correspondence, with the occasional additional assumptions we'll need to make.

The **in-degree** of a vertex v is the number of edges with head v, and the **out-degree** of v is the number of edges with tail v. In particular, *loops contribute 1 to both the in-degree and out-degree.* A digraph is d-**regular** if each vertex has in-degree and out-degree d. *In this thesis, all digraphs are assumed regular unless otherwise specified.*

A common theme when defining graph operations is that we care about bijections between various sets to keep track of edge names; so it is somewhat cleaner to work with abstract sets instead of numbers. For example, it will be convenient to consider graphs where the out-edges at every vertex are in bijection with a set S, and similarly the in-edges at every vertex are in bijection with S; such a digraph will be called S-**regular**.

Digraphs are characterized by their matrices. We'll make use of two kinds of matrices describing a digraph G: the **adjacency matrix** of G, denoted by A_G, is the matrix given by

$$(A_G)_{uv} = \text{number of directed edges from } u \text{ to } v$$

Notice that, when $u = v$, *a loop contributes 1 to this count.* This might appear strange at first, but various considerations show it's the 'right' convention. Thus the sum of the u-th row of A_G is precisely the out-degree of u, and similarly the sum of the u-th column is the in-degree of u. When G is d-regular, we additionally define the **random walk matrix** of G, denoted W_G, to be $W_G = A_G/d$. The reason behind the name is that $(W_G)_{uv}$ is the probability of going to v from u in the simple random walk on G.

2.3. Lifts

We now define lifts of digraphs, make basic observations, and give some examples; most of the results have been in the literature (e.g. Chapter 6 of the survey by Hoory, Linial and Wigderson [**HLW06**]) for some time in the case of undirected graphs, and here we give the obvious generalizations to digraphs.

A lift is a special case of an adjacency-preserving map between graphs, which is naturally called a homomorphism:

Definition 2.6 (Digraph homomorphism). A **digraph homomorphism** $f : G \to H$ is a pair of maps $f_V : V(G) \to V(H), f_E : E(G) \to E(H)$ such that if $u \xrightarrow{e} v \in E(G)$, then $f_V(u) \xrightarrow{f_E(e)} f_V(v) \in E(H)$.

There is an analogy with group homomorphisms here; for example, a group homomorphism $h : \mathcal{G} \to \mathcal{H}$ induces a natural graph homomorphism[2] $\mathrm{Cay}(\mathcal{G}, S) \to \mathrm{Cay}(\mathcal{H}, h(S))$. One can also think of a graph homomorphism as a 'continuous' function between graphs.

Definition 2.7 (Covering of digraphs). A **covering map** $p : G \to H$ **of digraphs** is an edge-surjective graph homomorphism such that for every $v \in V(G)$, the set of edges with tail (head) v is mapped bijectively to the set of edges with tail (head) $p_V(v)$. That is, the restrictions

$$p_E : \left\{e \in E(G) \;\middle|\; e^- = v\right\} \to \left\{e \in E(H) \;\middle|\; e^- = p_V(v)\right\}$$
$$p_E : \left\{e \in E(G) \;\middle|\; e^+ = v\right\} \to \left\{e \in E(H) \;\middle|\; e^+ = p_V(v)\right\}$$

are bijections. G is called a **lift** of H.

In the world of undirected digraphs, the above definition of a covering does not work automatically; we have to add some additional constraints, and that will be a common theme for many of our definitions. The below makes precise the correspondence between covering maps of undirected graphs and their directed analogues:

Definition 2.8 (Covering of undirected digraphs). For G and H undirected digraphs, a **covering map** $p : G \to H$ **of undirected digraphs** is a covering map $p : G \to H$ of digraphs that respects the pairs of opposite edges in G and H: that is, the preimage of any pair of opposite edges in H is a union of pairs of opposite edges of G.

In topology, one of the first observations made about covering maps is that the preimage, called the **fiber**, of an evenly covered neighborhood (the 'stack of pancakes', as the topologists call it) has constant cardinality when the base space B from Definition 1.5 is path-connected. We borrow the terminology and give the corresponding statement for digraphs:

Proposition 2.9 (Degree). *If $p : G \to H$ is a covering and H is weakly connected, the fibers $p_V^{-1}(v)$ and $p_E^{-1}(e)$ have the same cardinality for all $v \in V(H)$ and $e \in E(H)$; this number is called the **degree** of the covering.*

[2] if you're not familiar with the notation, Subsection 2.3.1 explains it.

PROOF. Suppose we have an edge $e = (u, v) \in E(H)$ with $u \neq v$. Let $F_u = p^{-1}(u)$, $F_v = p^{-1}(v)$ and $F_e = p^{-1}(e)$ be the fibers. For every $x \in F_u$, since p maps the out-edges of x bijectively to the out-edges of u, there is exactly one out-edge with image e. Moreover, the tail of every edge in F_e is in F_u because p is a homomorphism. This gives a function $f : F_u \to F_e$ which is injective and surjective, so a bijection. We similarly get a bijection between F_e and F_v, showing that all three sets have the same cardinality.

Reapplying this argument shows that whenever two vertices/edges are connected by a path (ignoring directions), their fibers have the same cardinality. By connectedness, we conclude the statement of the proposition. □

Our current view of coverings is not very *constructive*; it seems hard to give an explicit combinatorial description of all coverings of a given graph, or to think about them in concrete terms. But the above proof points to something more useful:

PROPOSITION 2.10 (COVERS BY PERMUTATIONS ON EDGES). *Suppose H is a digraph and S is a set. Then all lifts[3] G of H with degree $|S|$ can be obtained by letting $V(G) = V(H) \times S$, and picking bijections $f_e : S \to S$ for every $e \in E(H)$, so that the edges of G are precisely $e_s = ((e^-, s), (e^+, f_e(s)))$ as s ranges over S and e ranges over $E(H)$.*

PROOF. As we established in the proof of 2.9, if $G \to H$ is a covering, then for any edge $e = (u, v) \in E(H)$, the fiber F_e gives a perfect matching from F_u to F_v. So a covering certainly fits the above description. Conversely, given a graph G as in the proposition, we can define a natural map $p : G \to H$ by $(v, s) \mapsto v$ and $e_s = ((e^-, s), (e^+, f_e(s))) \mapsto (e^-, e^+)$ which is readily seen to be a covering. □

In this thesis we call s a **lift coordinate**. Given a covering $p : G \to H$ of degree d, we will call G a **d-lift**, also called a **d-cover**, of H. Similarly, given a covering $p : G \to H$ of the form from the above proposition, so that $V(G)$ is identified with $V(H) \times S$, we will call G an **S-lift**, also called an **S-cover**, of H.

EXAMPLE 2.11 (BIPARTITE DOUBLE COVER). For any digraph H, we can define a special $\{1, 2\}$-lift G of H called the **bipartite double cover**, by assigning to every edge $u \xrightarrow{e} v$ of H the transposition (1 2). It's then easy to see that G is a bipartite digraph, with the two parts being $V(H) \times \{1\}$ and $V(H) \times \{2\}$. As an example, the bipartite double cover of a bouquet of n loops is the graph on two vertices u and v, with n directed edges $u \longrightarrow v$, and n directed edges $v \longrightarrow u$.

Proposition 2.10 is a fairly trivial observation, but shifting the perspective to edges allows us to construct and think of coverings in very reductionist terms, which will help us a great deal.

REMARK 2.12. We remark that if we want to restrict ourselves to *undirected* digraphs, we have to make sure that we lift every pair of opposite edges e, e' with inverse permutations $f_e = f_{e'}^{-1}$.

Finally, the following is immediate by composing the bijections from the definition of a covering: If $p : G \to H$ and $q : H \to K$ are covering maps, then the composition $q \circ p : G \to K$ is also a covering map. This allows us to talk about **towers** of lifts, where we have a sequence of covering maps $G_n \xrightarrow{p_n} G_{n-1} \xrightarrow{p_{n-1}} \dots \to G_1 \xrightarrow{p_1} G_0$, and G_i is a lift of G_j whenever $i > j$; this will be our setting for constructing expander families from lifts.

2.3.1. Cayley and Schreier graphs. An important example of covering maps comes from *Cayley* and *Schreier* graphs, so we'll devote some time to them. We keep the names 'Cayley *graph*' and 'Schreier *graph*' used in the literature, but in this thesis all Cayley and Schreier graphs are implicitly *digraphs*. Here is the digraph structure:

[3] This description is redundant, in the sense that there will be many isomorphic lifts obtained through this process. It's not hard to see that we can assign the identity permutation to the edges in any tree, and still get all lifts using the remaining freedom; see [**GT87**]

Definition 2.13 (Cayley and Schreier graphs). For a group $\mathcal{G}$ and a multiset S of elements of $\mathcal{G}$, the **Cayley graph** $\mathrm{Cay}(\mathcal{G}, S)$ is the digraph with vertex set the underlying set of $\mathcal{G}$, and edges $g \longrightarrow sg$ for every $g \in \mathcal{G}$ and every $s \in S$. If we're additionally given a subgroup $\mathcal{H} \subset \mathcal{G}$, we can also form the **Schreier coset graph** $\mathrm{Sch}(\mathcal{G}, \mathcal{H}, S)$ with vertex set the left cosets $\mathcal{G}/\mathcal{H}$, and edges $g\mathcal{H} \longrightarrow sg\mathcal{H}$ for every coset $g\mathcal{H}$ and every $s \in S$. Finally, given a set X with a left $\mathcal{G}$-action, we can define the **Schreier graph** $\mathrm{Sch}(\mathcal{G}, X, S)$ to be the graph with vertex set X and an edges $x \longrightarrow sx$ for every $x \in E$ and $s \in S$.

Clearly, a Cayley graph is a Schreier coset graph where $\mathcal{H} = \mathrm{id}$, and a Schreier coset graph is a Schreier graph for the action of $\mathcal{G}$ on left cosets; so a Schreier graph is the most general notion of the three.

Since in the theory of expanders we often work with undirected graphs, it is desirable to get natural undirected versions of Cayley/Schreier graphs. This is done by making S a *symmetric* generating set, so that $S = T \cup T^{-1}$ as multisets, where inversion is elementwise. Then we have the natural pairs of opposite edges $u \longrightarrow tu$ and $tu \longrightarrow t^{-1}tu = u$, which make $\mathrm{Sch}(\mathcal{G}, X, S)$ into an undirected digraph.

Finally, observe that any Schreier graph $\mathrm{Sch}(\mathcal{G}, X, S)$ covers the **bouquet of circles** B_S, which is the digraph with one vertex and directed loops in bijection with S: just map every edge coming from the element $s \in S$ to the s-th loop. Since every $x \in X$ has exactly one out-edge $x \longrightarrow sx$ labeled by s and exactly one in-edge $s^{-1}x \longrightarrow x$ labeled by s, this gives a covering map. This example will be very important for us later on.

2.4. Spectral expansion

There are many qualitatively equivalent measures of expansion – Definition 1.4 is one of them, called *vertex expansion* – and we can transition from one to another, losing some quantity along the way; we refer the reader to Hoory et al [**HLW06**] and Vadhan [**Vad12**] for a more comprehensive account. There is no 'best' measure of expansion – the transition functions deteriorate near certain values of the parameters, and different measures are needed for different applications. In this thesis, we will use the spectral expansion, which is amenable to algebraic methods:

Definition 2.14 (Spectral expansion). For a digraph G, we define the **spectral expansion** of G by

$$\lambda(G) = \max_{x \perp u_G} \frac{\|W_G x\|}{\|x\|}$$

where u_G is the uniform probability distribution over $V(G)$, and the maximum[4] is over all nonzero vectors $x \in \mathbb{R}^{V(G)}$ orthogonal to u_G.

The distribution $W_G\pi$ represents taking a random step *backwards* in G; a forward step would be represented by $W_G^T\pi$. The reason for the unusual convention is that we prefer all our actions to be on the left in this thesis. But this doesn't matter, since $\lambda(G)$ is the second *singular value* of W_G, which is invariant under matrix transposition – see Proposition 2.18!

We want $\lambda(G)$ to be *small*. Intuitively, $\lambda(G)$ is the factor by which the distance from uniformity of a probability distribution on $V(G)$ shrinks after taking a single step in the random walk on G; so it's not surprising that it tells us a lot about the random walk on G. Alternatively, we can think of $x \perp u_G$ as a function on the vertices of G that has expectation zero, and of our graph as of trying to estimate that expectation via 'sampling' by the adjacency operator W_G; how good the estimate is, as measured by $\lambda(G)$, tells us something about how sampling via the random walk looks like random sampling.

In the undirected case, the *eigenvalues* tell us a lot about the connectivity properties of the graph, and we can give a more familiar definition of $\lambda(G)$:

[4] Note that the use of max instead of sup is justified. By normalization it suffices to restrict our attention to $\|x\| = 1$. Orthogonal complements are closed in finite dimensional vector spaces, thus intersecting $u^\perp$ with the sphere gives a closed compact set, where the continuous function $\|W_G x\|$ achieves its supremum.

Proposition 2.15 (Undirected spectral graph theory basics). *For an undirected d-regular digraph $G = (V, E)$,*

(1) W_G has real eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ with $|\lambda_i| \leq 1$ and $\lambda_1 = 1$;
(2) 1 is an eigenvalue of multiplicity > 1 iff G is disconnected;
(3) $\lambda(G) = \max\{|\lambda_2(G)|, |\lambda_n(G)|\}$.

Proof. (1) For undirected G, the adjacency matrix and thus the random walk matrix are symmetric, so we can apply the spectral theorem to get an orthonormal basis of eigenvectors $e_1, e_2, \ldots, e_n$ with respective eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$. Since G is d-regular, we have $W_G u_G = A_G u_G/d = du_G/d = u_G$, so the uniform distribution is an eigenvector of eigenvalue 1. Next, we observe that W_G is a contraction in l_1 norm, and in particular if f is an eigenvector with eigenvalue λ, we have

$$|\lambda| \times \|f\|_1 = \|W_G f\|_1 \overset{\triangle\neq}{\leq} \sum_{v\in V}\sum_{u\in V}(W_G)_{vu}|f_u| = \sum_{u\in V}|f_v|\sum_{v\in V}(W_G)_{uv} = \sum_{u\in V}|f_v| = \|f\|_1$$

Since eigenvectors are nontrivial, we conclude that $|\lambda| \leq 1$.

(2) If G is disconnected, pick two connected components C_i and vectors v_i constant on C_i and zero otherwise; then v_i are independent eigenvectors of W_G with eigenvalue 1. Conversely, if we have two independent eigenvectors of eigenvalue 1, it's easy to see by considering the maximum coordinate that each is constant on connected components; by independence, these components have to be different!

(3) Observe that for $x \perp u_G$, if we decompose $x = \sum_i \alpha_i e_i$ along the basis, the $e_1 = u_G$ component is $\langle x, u_G\rangle = 0$, so

$$\|W_G x\| = \sum_{i=2}^{n}\lambda_i^2\alpha_i^2 \leq \max\{|\lambda_2|, |\lambda_n|\}^2\sum_{i=2}^{n}\alpha_i^2 = \max\{|\lambda_2|, |\lambda_n|\}^2\|x\|$$

□

For directed digraphs, we can do something very similar, using the *singular value decomposition*, a generalization of the spectral theorem; so here's a linear-algebraic detour devoted to that:

Definition 2.16. For a matrix A, the **singular values** of A are the square roots of the eigenvalues of the symmetric matrix A^TA.

It's easy to see the eigenvalues of A^TA are non-negative, so the above definition makes sense: suppose $A^TAv = \lambda v$; then $\|Av\| = v^TA^TAv = v^T(\lambda v) = \lambda\|v^Tv\| = \lambda\|v\|$ and hence $\lambda \geq 0$. The singular values provide something of an analogue of the eigenvalues when the matrix in question is not symmetric:

Theorem 2.17 (Singular value decomposition for real square matrices). *Any square real $n \times n$ matrix A admits a factorization of the form $A = U\Sigma V^T$ where:*

(1) U and V are $n \times n$ orthogonal matrices, and Σ is an $n \times n$ diagonal matrix with the singular values $\sigma_1 \geq \ldots \geq \sigma_n$ on the diagonal.
*(2) The columns $v_1, \ldots, v_n$ of V and the columns $u_1, \ldots, u_n$ of U, called **left-** and **right-singular vectors** of A, satisfy*

$$Av_i = \sigma_i u_i \text{ and } A^Tu_i = \sigma_i v_i$$

(3) We are free to choose the columns of V to be any orthonormal basis of eigenvectors for A^TA.

Proposition 2.18 (Spectral expansion = second singular value). *For a regular digraph G, the singular values of W_G are $1 = \sigma_1 \geq \sigma_2 \geq \ldots \geq 0$, and $\lambda(G) = \sigma_2$.*

Proof. This is a generalization of Proposition 2.15, where we made use of the eigenvalue decomposition for symmetric matrices, so here we naturally use the singular value decomposition. First observe that, since G is both in- and out-regular, $W_G^T W_G u_G = W_G^T u_G = u_G$, and the proof from Proposition 2.15 that W_G is a contraction in l_1 norm carries over to W_G^T to give

$$\|W_G^T W_G x\|_1 \leq \|W_G x\|_1 \leq \|x\|_1$$

for any x, hence $W_G^T W_G$ is also a contraction in l_1. Thus, the eigenvalues of $W_G^T W_G$ lie in $[0, 1]$. Next, pick any $x \perp u_G$, and pick a spectral decomposition $W_G = U\Sigma V^T$ where the first column of V is u_G, as provided by 2.17. Decompose $x = \sum_{i=1}^n \alpha_i v_i$ in the basis of right-singular vectors; then $\alpha_1 = \langle x, u_G \rangle = 0$, so using the orthonormality of the $u_1, \ldots, u_n$ we compute

$$\|W_G x\| = \left\| \sum_{i=2}^n \alpha_i \sigma_i u_i \right\| = \sqrt{\sum_{i=2}^n \alpha_i^2 \sigma_i^2} \leq \sigma_2 \sqrt{\sum_{i=2}^n \alpha_i^2} = \sigma_2 \|x\|$$

with equality when x is a multiple of v_2. □

In analogy with Definition 1.4, we define the objects we want to construct, hopefully fully explicitly.

Definition 2.19 (Expander families and expander towers). An infinite family of d-regular digraphs $G_1, G_2, \ldots$ with $|V(G_n)| \to \infty$ is called an **expander family** if there is a constant $\lambda < 1$ such that $\lambda(G_n) \leq \lambda$ for all n. It is called an **expander tower** if, additionally, there are covering maps $G_{n+1} \to G_n$ for all $n \in \mathbb{N}$.

2.5. Basic expansion properties of lifts

We will think of vectors as functions, so that for example for a set S the vector space $\mathbb{C}^S$ is identified with the vector space of functions $S \to \mathbb{C}$; this makes the notation more natural. We will identify the adjacency matrix A_G of a graph G with the linear operator on $\mathbb{C}^{V(G)}$ given by multiplication on the left: $v \mapsto A_G v$.

The following proposition is the basis of the niceness of coverings with respect to expansion:

Proposition 2.20. *If $p : G \to H$ is a covering of finite graphs, and $\mathbb{F}$ is any field, there is a natural induced linear transformation $L_p : \mathbb{F}^{V(H)} \to \mathbb{F}^{V(G)}$ given by $f \mapsto f \circ p_V$ which fits in the following commutative diagram of vector spaces:*

$$\begin{array}{ccc} \mathbb{F}^{V(G)} & \xrightarrow{A_G} & \mathbb{F}^{V(G)} \\ {\scriptstyle L_p}\uparrow & & \uparrow{\scriptstyle L_p} \\ \mathbb{F}^{V(H)} & \xrightarrow{A_H} & \mathbb{F}^{V(H)} \end{array}$$

Proof. Denote the standard bases for $\mathbb{F}^{V(H)}$ and $\mathbb{F}^{V(G)}$ by $(f_v)_{v \in V(H)}$ and $(f_{v,s})_{(v,s) \in V(G)}$. By linearity, it suffices to prove that for all f_v we have $A_G L_p f_v = L_p A_H f_v$. So fix v and observe that

$$L_p A_H f_v = L_p \left(\sum_{e: u \to v} f_u \right) = \sum_s \sum_{e: u \to v} f_{u,s}$$

and

$$A_G L_p f_v = A_G \left(\sum_s f_{v,s} \right) = \sum_s A_G f_{v,s} = \sum_s \sum_{e: (u,s') \to (v,s)} f_{u,s'}$$

In the first sum, the coefficient of $f_{u,s}$ for arbitrary u and s is precisely the number[5] of edges from u to v in H; in the second sum, the coefficient of $f_{u,s}$ is the size of

$$S = \left\{ e \in E(G) \;\middle|\; e^- = (u,s) \text{ and } e^+ = (v,s') \text{ for some } s' \right\}$$

Since p_E maps the edges with tail (u,s) bijectively to the edges with tail u, and any edge with head (v,s') for some s' is mapped to an edge with head v, it follows that p_E also maps S bijectively to the set of edges with tail u and head v. Thus, the coefficients of $f_{u,s}$ in the two sums are the same. □

We will only need this for $\mathbb{R}$ or $\mathbb{C}$. The undirected analogues of the following consequences have long been known in the literature on lifts (e.g. Bilu and Linial [**BL06**]):

Corollary 2.21 (Covers can't expand better). *If $p : G \to H$ is a covering of digraphs, then:*

1. *If $f : V(H) \to \mathbb{C}$ is an eigenvector of H with eigenvalue λ, then $f \circ p_V : V(G) \to \mathbb{C}$ is an eigenvector of G with eigenvalue λ. Similarly, if $f, g : V(H) \to \mathbb{C}$ are a pair of left- and right-singular vectors with singular value σ, so are $f \circ p_V, g \circ p_V$.*
2. *$\lambda(G) \geq \lambda(H)$.*

Proof. From Proposition 2.20, it follows that

$$A_G(f \circ p) = A_G(L_p f) = L_p A_H f = L_p(\lambda f) = \lambda(L_p f) = \lambda(f \circ p)$$

as we wanted; the analogous argument works for singular vectors. The second part now follows from the interpretation of $\lambda(G)$ as the second singular value/eigenvalue.

□

Thus, whenever we have a covering $p : G \to H$, G inherits all eigenvalues of H – the **old** eigenvalues – and also has **new** eigenvalues that we want to bound; similarly for singular values.

2.6. Lower bounds on spectral expansion via lifts

How good can spectral expansion be? It's easy to observe that for any d-regular simple undirected digraph G with two vertices u, v a distance > 2 apart, we have $\lambda(G) \geq 1/\sqrt{d}$. Indeed, pick the vector $x_{uv} = (0, \ldots, 1, \ldots, -1, \ldots, 0)$ with a 1 in the u-th position and -1 in the v-th position; then $\lambda(G) \geq \|W_G x\|/\|x\| = \sqrt{2/d}/\sqrt{2} = 1/\sqrt{d}$. It turns out that this can be improved to $2\sqrt{d-1}/d - o_n(1)$ for an n-vertex graph and d fixed. In this section, we will show how to use covering maps to give lower bounds for $\lambda(G)$ of *undirected digraphs*; later on, we will (somewhat) reduce the directed case to the undirected one. The following observations are the basis of lower bounds based on lifts; the idea of using the numbers $p_l^v(G)$ is taken from Vadhan [**Vad12**]:

Notation 2.22. *Given a digraph G, denote by $p_l^v(G)$ the probability that a random walk started at v comes back to v after l steps.*

Proposition 2.23. *For an undirected d-regular digraph $H = (V, E)$ on n vertices,*

(1) $\sum_{v \in V} p_l^v(H) \leq 1 + (n-1)\lambda(H)^l$
(2) If $p : G \to H$ is a covering of digraphs, $p_l^v(H) \geq p_l^x(G)$ for any $x \in p^{-1}(v)$.

Proof. (1) It's a standard calculation that $p_l^v(H)$ is the v-th diagonal entry of W_H^l, hence $\sum_{v \in V} p_l^v(H) = \operatorname{tr} W_H^l$. Since H is undirected, the eigenvalues of W_H^l are the l-th powers of the eigenvalues of W_H; the largest of those is 1, and all others are bounded by $\lambda(H)^l$, so the first part follows.

[5] In the proof we implicitly assume $\operatorname{char}\mathbb{F} = 0$; the proof in the other case is analogous, though tedious to write.

(2) Consider a closed walk of length l in G starting at $x \in p^{-1}(v)$; when we project it to H, we get a closed walk of length l starting at v. Since for every edge $u \xrightarrow{e} w$ in H and $x \in p^{-1}(u)$ there is a unique edge $x \xrightarrow{e'} y$ with $y \in p^{-1}(w)$ that is a lift of e, a step-by-step argument shows that if two walks in G are sent to the same walk in H, they have to be the same in G as well! Thus, there are fewer l-step closed walks at x in G than at v in H, which implies the result.

□

The point is that sometimes G is simpler to describe than H, so it's easier to count closed walks in G than in H. An analogous approach was used by Friedman in [**FT05**] to bound the second-largest (not in absolute value) eigenvalue of expanders related to error-correcting codes. As an application, we now show how the famous Alon-Boppana theorem follows from that approach:

THEOREM 2.24 (ALON-BOPPANA). *Given a family of d-regular connected undirected digraphs $G_1, G_2, \ldots$ with $|V(G_n)| \to \infty$, we have*

$$\lambda(G_n) \geq 2\sqrt{d-1}/d - o_n(1)$$

PROOF. Observe that the infinite d-regular tree T_d, realized as an undirected digraph, covers any d-regular undirected connected digraph G. The proof is by a simple generalization of the argument for undirected simple graphs, found in Section 6 of [**HLW06**]. Fix $v_0 \in V(G)$, and define the following graph: the vertex set consists of all finite walks $w_0 \xrightarrow{e_0} w_1 \xrightarrow{e_1} \ldots \xrightarrow{e_k} e_{k+1}$ with $w_0 = v_0$ in G that don't *backtrack*: that is, e_{n+1}, e_n are never a pair of opposite edges in G for all n. There is a directed edge between two such walks iff one is an extension of the other by one edge. It's easy to see this defines a d-regular undirected digraph such that the corresponding undirected graph is the infinite d-regular tree. The covering map sends a walk ending at w to w, and an edge e between two walks to the edge in G that gave rise to e (or the opposite edge, if directions don't match).

By symmetry, $p_l^x(T_d)$ is independent of x; so we have to lower bound the closed walks of length l on T_d, which is a combinatorial problem. For l odd, that's zero, but by a counting argument (see Hoory, Linial and Wigderson [**HLW06**]) it turns out that $p_{2l}^x(T_d) \geq \binom{2l}{l} \frac{(d-1)^l}{(l+1)d^{2l}} \geq \frac{(2\sqrt{d-1})^{2l}}{d^{2l}l^{3/2}}$ and hence $\lambda(G_n)^{2l} \geq \frac{|V(G_n)|}{|V(G_n)|-1} \frac{(2\sqrt{d-1})^{2l}}{d^{2l}l^{3/2}} - \frac{1}{|V(G_n)|-1}$. After taking $2l$-th roots, we get our result. □

It turns out that *explicit* undirected families of expanders $(G_n)_{n\in\mathbb{N}}$ that achieve this bound exist, in the sense that $\lambda(G_n) \leq 2\sqrt{d-1}/d$ for all n; this was shown in the celebrated paper [**LPS88**] of Lubotzky, Phillips and Sarnak, but only for very special degrees $d = p + 1$ for p prime. Such optimal spectral expanders are called **Ramanujan graphs**, and recently an existence proof for bipartite Ramanujan graphs of *all degrees* was given by Marcus, Spielman and Srivastava [**MSS13**], using a completely different approach. We'll discuss it and give some generalizations in Section 5.2.

CHAPTER 3

Voltage assignments

3.1. Terminology and basic properties

A tool, called *a voltage assignment*, for describing certain restricted lifts of graphs, was studied by Gross and Tucker in their book [**GT87**], which we follow in this section. They used voltage assignments to tackle the central problem of topological graph theory: given a graph and a topological surface, can one draw the graph on the surface without edge intersections, and if so, how? In the process of answering those questions, they found passing to covering surfaces to be useful, which led them to covering graphs as well.

In short, a voltage assignment is simply an association of an element of some fixed permutation group $\mathcal{G}$ to every edge of a digraph H. Then, as we saw in Proposition 2.10, we can define a covering map $p : G \to H$ where G is obtained using the permutations as matchings between fibers. It's not immediately obvious why restricting $\mathcal{G}$ to be a proper subgroup of the full permutation group would be beneficial at all – we expect that the more freedom to introduce 'chaos' we have, the easier it is to make graphs that look random. Here are some reasons in favor of more abstraction:

- The case when $\mathcal{G} = \mathbb{Z}/k\mathbb{Z}$ has been studied in previous work, where it was shown that expanding lifts do exist in this restricted case, and the representation-theoretic structure of $\mathbb{Z}/k\mathbb{Z}$ was used in the analysis [**AKM13**].
- The study of voltage assignments in the abstract sheds more light on the parallels between lifts and Cayley/Schreier graphs. Indeed, we will obtain known characterizations of the spectra of Cayley/Schreier graphs [**HLW06**] as special cases of the results in Section 3.2.
- Even when the permutations are not restricted to a proper subgroup, when we perform a sequence of several lifts, the permutations describing the top lift *will* be restricted; we will compute exactly how. The short answer turns to be 'iterated wreath products', which will help us understand the construction in [**RSW06**] better.

It seems that voltage assignments are absent from the recent developments in expansion in lifts; consequently, we shall see that authors re-invented special cases of some results from the 90s, e.g. Bilu and Linial and Agarwal, Kolla and Madan [**BL06, AKM13**]. We shall show how these generalize. We now review the terminology of Gross and Tucker and some of their basic results, generalizing them in the obvious manner to digraphs along the way.

Definition 3.1 (Ordinary voltage assignment). Given a digraph G and a group $\mathcal{G}$, an **ordinary voltage assignment** is a function $\alpha : E(G) \to \mathcal{G}$. The **derived graph** associated with α, denoted by G^α, is the $\mathcal{G}$-lift of G where the permutation on an edge e is the permutation on $\mathcal{G}$ given by the left action $\alpha(e) : g \mapsto \alpha(e)g$.

Example 3.2. We obtain all Cayley graphs as a special case of derived graphs for ordinary voltage assignments: if $G = B_S$, and the image of α with multiplicity is $S \subset \mathcal{G}$, G^α is exactly $\mathrm{Cay}(\mathcal{G}, S)$, as we discussed in Subsection 2.3.1.

Definition 3.3 (Permutation voltage assignment). Given a digraph G and a group $\mathcal{G}$, a **permutation voltage assignment** is a function $\alpha : E(G) \to \mathrm{Sym}(S)$ for some set S. The **derived graph** associated with α, denoted by G^α, is the S-lift of G where the permutation on an edge e is $\alpha(e)$.

Clearly, since we can realize the left action of a group $\mathcal{G}$ on itself as a subgroup of $\mathrm{Sym}(\mathcal{G})$, the derived graph of an ordinary voltage assignment is a special case of the derived graph of a permutation voltage assignment. Moreover, as we saw in Proposition 2.10, permutation voltage assignments are expressive enough to describe all possible lifts. Ordinary voltage assignments, on the other hand, are not: they correspond to a stronger notion of covering, called *regular covering*, where the bottom graph is a quotient of the top graph under a free group action. Gross and Tucker considered one more kind of voltage assignments:

Definition 3.4 (Relative voltage assignment). Given a graph G, a group $\mathcal{G}$ and a subgroup $\mathcal{H} \subset \mathcal{G}$, a **relative voltage assignment** is a function $\alpha : E(G) \to \mathcal{G}$. The **derived graph** associated with α, denoted $G^{\alpha/\mathcal{H}}$, is the lift of G where the permutation on an edge e is the permutation on $\mathcal{G}/\mathcal{H}$ given by the left action on cosets $\alpha(e) : g\mathcal{H} \to \alpha(e)g\mathcal{H}$.

Example 3.5. We obtain all Schreier coset graphs as a special case of relative derived graphs: if $G = B_S$ and the image of α with multiplicity is $S \subset \mathcal{G}$, we have that $G^{\alpha/\mathcal{H}}$ is exactly $\mathrm{Sch}(\mathcal{G}, \mathcal{G}/\mathcal{H}, S)$, as we saw in Subsection 2.3.1.

So we arrive at the intuition that ordinary voltage assignments are to relative voltage assignments as Cayley graphs are to Schreier graphs; we will come back to this several times later on. To specialize the above notions to undirected digraphs, we simply require that, for a pair of opposite edges, the voltage assignment α assigns inverse group elements, in analogy with Remark 2.12. Relative voltage assignments, while being more abstract, still capture all possible lifts:

Proposition 3.6 (From permutation voltages to relative voltages). *If $p : G \to H$ is an S-covering of digraphs given by permutation voltages $\alpha : E(H) \to \mathrm{Sym}(S)$, G is isomorphic to the derived graph $H^{\alpha/\mathcal{H}}$ of the voltage assignment α relative to $\mathcal{H} = \mathrm{stab}_{\mathrm{Sym}(S)}(s)$ where $s \in S$ is arbitrary.*

Proof. It suffices to show that the action of $\mathrm{Sym}(S)$ on the left cosets of $\mathcal{H}$ is isomorphic to the action of $\mathrm{Sym}(S)$ on S by permutations. What do the cosets of $\mathcal{H}$ look like? For $t \in S$, denote the transposition between s and t by $(s\ t) \in \mathrm{Sym}(S)$; then we claim that the cosets are precisely $\left\{(s\ t)\mathcal{H} \;\middle|\; t \in S\right\}$. Indeed, any $\phi \in \mathrm{Sym}(S)$ such that $\phi(s) = t$ can be written as $\phi = (s\ t)(s\ t)\phi = (s\ t)((s\ t)\phi)$ and $(s\ t)\phi(s) = (s\ t)(t) = s$, hence $(s\ t)\phi \in \mathcal{H}$, so the coset $(s\ t)\mathcal{H}$ consists of exactly those permutations that send s to t.

Now it's clear what to do: define a bijection $f : \mathrm{Sym}(S)/\mathcal{H} \to S$ by $(s\ t)\mathcal{H} \mapsto t$. Suppose we have $\phi \in \mathrm{Sym}(S)$ such that $\phi(t) = u$; then ϕ sends the coset $(s\ t)\mathcal{H}$ to the coset $\phi(s\ t)\mathcal{H}$ which is the same as the coset $(s\ u)\mathcal{H}$, as $\phi(s\ t)(s) = \phi(t) = u$. So f gives an isomorphism between the two actions. □

3.1.1. Basic expansion properties. Let's think about the random walk on the derived graph G^α for an ordinary voltage assignment $\alpha : E(G) \to \mathrm{Sym}(n)$. A vertex in G^α is a pair (v, π) where v is a vertex of G and π is a permutation. In a random walk, the v coordinate performs a random walk on G, and the π coordinate changes as $\pi_0, \pi_1\pi_0, \ldots, \pi_k \ldots \pi_1\pi_0$ where $\pi_1, \ldots, \pi_k$ are the permutations assigned to the edges of the random walk in G. Convergence to uniformity means that *both* the random walk on G converges to uniform, and the permutation $\pi_k \ldots \pi_1$ converges to uniform. We can interpret $\alpha : E(G) \to \mathrm{Sym}(n)$ as a permutation voltage assignment as well: in this case, the second coordinate will be a point instead of a permutation, and to approach uniformity we will need $\pi_k \ldots \pi_1(s)$ to approach a uniformly random point.

Clearly, $\pi_k \ldots \pi_1$ approaching a uniform permutation is a stronger condition than $\pi_k \ldots \pi_1(s)$ approaching a uniform point; thus, we expect the derived graph from the permutation voltages to be at least as goon an expander as the one derived from the ordinary voltages. This intuition is matched and generalized by the following observation:

Proposition 3.7 (Ordinary voltages expand less than relative ones). *For a relative voltage assignment $\alpha : E(G) \to \mathcal{G}$ relative to $\mathcal{H} \subset \mathcal{G}$, there is a natural covering map $p : G^\alpha \to G^{\alpha/\mathcal{H}}$*

PROOF. We do the obvious thing: given a vertex $(v, g) \in G^\alpha$, we map it down to $(v, g\mathcal{H})$; given an edge $(v, g) \to (u, hg)$ where (v, u) is lifted by the permutation h, we map it down to $(v, g) \to (u, hg\mathcal{H})$; this is easily seen to give a covering. □

As a corollary, we see that a Cayley graph covers any of its corresponding Schreier coset graphs – so constructing Cayley expanders is *harder* than constructing Schreier expanders.

3.2. Signing matrices for all lifts

Intuitively, given a lift $p : G \to H$, there is a way to block-diagonalize the adjacency matrix of a lift and to separate the 'old' part of the matrix that comes from H from the interesting part. The motivation is to have a nice algebraic object, which has been called the *signing matrix*, that captures the new eigenvalues of G; it is the block-diagonalized version of A_G without the piece coming from H. The reason this works is that any permutation action of the group $\mathcal{G}$ from which we draw the voltages can be 'diagonalized' in a precise sense using the language of representation theory; by linearity, this diagonalization induces a 'diagonalization' of the adjacency matrix of G.

In the literature on expanders, this has been observed for simple graphs in very special cases of $\mathcal{G}$ by Bilu and Linial and Agarwal, Kolla and Madan [**BL06**, **AKM13**]; in the literature on voltage assignments, this has been observed for ordinary voltage assignments of simple graphs by Mizuno and Sato [**MS95**]. Here we use their manipulation to give the obvious generalization to relative voltage assignments and digraphs, thus capturing all lifts.

3.2.1. Representation theory review. We will make use of some basic results from the *representation theory* of finite groups. Representation theory aims to describe abstract groups by studying the homomorphisms from such groups to the more concrete setting of linear operators on vector spaces[1]. A *representation* of $\mathcal{G}$ is like a 'manifestation' of $\mathcal{G}$ as a group of linear operators, to which linear algebra can be applied with the hope of understanding the structure of $\mathcal{G}$ better. Representation theory has been an incredibly successful tool in many areas of mathematics, and, like expanders, is at the intersection of several fields; it occasionally makes its way into computer science as well!

We will work with *unitary representations*, where the setting is that of unitary operators over complex vector spaces; for finite groups, this is without loss of generality. Here we barely scratch the surface – for a comprehensive introduction, we refer the reader to Artin [**Art**] (who we follow), and Serre [**Ser77**].

DEFINITION 3.8 (REPRESENTATION). For a finite group $\mathcal{G}$, a **matrix representation** of $\mathcal{G}$ is a homomorphism $\rho : \mathcal{G} \to \mathrm{GL}(\mathcal{V})$ for some finite dimensional complex vector space $\mathcal{V}$. The **dimension of** ρ is $\dim \mathcal{V}$.

EXAMPLE 3.9. There are two extreme, trivial examples that show up frequently. The **trivial representation** has $\mathcal{V} = \mathbb{C}$ and $\rho(g) = 1$ for all g; this representation 'forgets' everything about $\mathcal{G}$.

The **(left) regular representation** has $\mathcal{V} = \mathbb{C}^{\mathcal{G}}$ and $\rho(g) = P_g$ is the permutation matrix associated to the left action of g on $\mathcal{G}$ by $h \mapsto gh$; this representation 'remembers' everything about $\mathcal{G}$, and such representations are called **faithful**.

Between these two, it's easy to spot some more representations: given a subgroup $\mathcal{H} \subset \mathcal{G}$, the **(left) permutation representation** of $\mathcal{G}$ relative to $\mathcal{H}$ has $\mathcal{V} = \mathbb{C}^{\mathcal{G}/\mathcal{H}}$ and $\rho(g) = P_g$ is the permutation matrix associated to the left action of g on $\mathcal{G}/\mathcal{H}$ by $h\mathcal{H} \mapsto gh\mathcal{H}$; by taking $\mathcal{H}$ to be $\mathcal{G}$ or the trivial group, we get the above examples.

[1] Any group $\mathcal{G}$ can be seen as a *category* with one element $C_{\mathcal{G}}$, and a homomorphism from $\mathcal{G}$ to a vector space is a functor from $C_{\mathcal{G}}$ to the category of vector spaces. Thus, representation theory is somewhat similar to algebraic topology, which considers *functors*, like homology and homotopy, from the category of topological spaces to the category of groups. The main point is that in both cases the target category is better understood in some sense. For more on categories, see Section 4.7

Example 3.10. Let's consider a cyclic group $\mathbb{Z}/k/\mathbb{Z}$. We know that roots of unity behave like elements of $\mathbb{Z}/k\mathbb{Z}$, and they feel like a 'manifestation' of $\mathbb{Z}/k\mathbb{Z}$. Can we get some representations out of that? Indeed, we can: let ω be a primitive k-th root of unity, and for any $t \in \{0, \dots, k-1\}$, define the map $f_t : \mathbb{Z}/k\mathbb{Z} \to \mathbb{C}$ given by $a \mapsto \omega^{ta}$. Then every f_t gives us a 1-dimensional representation of $\mathbb{Z}/k\mathbb{Z}$.

In the world of finite groups, any representation is conjugate to a restricted kind of representation called a *unitary representation*:

Definition 3.11. For a finite group $\mathcal{G}$, a **unitary representation** of $\mathcal{G}$ is a homomorphism $\rho : \mathcal{G} \to \mathrm{U}(\mathcal{V})$ for some finite dimensional Hermitian inner product space $\mathcal{V}$.

Permutation representations are clearly unitary. The main fact we need about unitary representations is that any such representation decomposes orthogonally into a direct sum of *irreducible* ones:

Definition 3.12 (Irreducible representation). For a representation $\rho : \mathcal{G} \to \mathrm{GL}(\mathcal{V})$, a subspace $\mathcal{W} \subset \mathcal{V}$ is **invariant** under ρ if $\rho(g)\mathcal{W} \subset \mathcal{W}$ for all $g \in \mathcal{G}$. A representation is **irreducible** if it has no proper invariant subspace.

Theorem 3.13 (Maschke). *For any unitary representation $\rho : \mathcal{G} \to \mathrm{U}(\mathcal{V})$, there is a unique, up to isomorphism, orthogonal decomposition $\mathcal{V} = \bigoplus_i \mathcal{V}_i$ where each $\mathcal{V}_i$ is invariant under ρ, and the restriction $\rho : \mathcal{G} \to \mathrm{U}(\mathcal{V}_i)$ is an irreducible unitary representation.*

Example 3.14. For any permutation representation $\rho : \mathcal{G} \to \mathrm{U}(\mathbb{C}^{\mathcal{G}/\mathcal{H}})$, there is a one-dimensional invariant subspace spanned by the all ones vector; this gives a copy of the trivial representation sitting inside ρ.

For the symmetric group $\mathrm{Sym}(n)$, the **standard representation** is what's left after we take out the copy of the trivial representation from the permutation representation of $\mathrm{Sym}(n)$ on $\{1, \dots, n\}$. The standard representation is irreducible, but a proof of that is beyond the scope of this thesis.

Example 3.15. The representations of $\mathbb{Z}/k\mathbb{Z}$ we found are unitary, as $\omega^{ta}\overline{\omega^{ta}} = 1$, and are irreducible by virtue of being 1-dimensional. In fact, it turns out that (see Artin [**Art**]) they are all irreducible representations of $\mathbb{Z}/k\mathbb{Z}$, and the regular representation $\mathbb{Z}/k\mathbb{Z}$ decomposes as a their direct sum!

3.2.2. Tensor product of matrices. We will also make use of the tensor product of matrices, which has a number of nice properties we state without proof.

Definition 3.16. For matrices A and B, the **tensor product** $A \otimes B$ is defined by the block matrix

$$\begin{pmatrix} a_{11}B & \dots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nm}B \end{pmatrix}$$

The following is a straightforward exercise in matrix manipulation:

Fact 3.17. *The matrix tensor product has the following properties (whenever the corresponding matrix dimensions match):*

(1) Bilinearity: $(A + B) \otimes C = A \otimes C + B \otimes C$, $A \otimes (B + C) = A \otimes B + A \otimes C$.
(2) Associativity: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.
(3) Mixed product: $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, *in particular* $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

3.2.3. The computation. In this section we use the trick of Mizuno and Sato [**MS95**] to compute signing matrices for all lifts. In this section, for matrices A_i, let $\bigoplus_i A_i$ denote the block-diagonal matrix with blocks A_i. Here is the main observation:

Theorem 3.18 (General signing matrices). *Let $\alpha : E(G) \to \mathcal{G}$ be a voltage assignment on an N-vertex digraph G relative to $\mathcal{H} \subset \mathcal{G}$, and $\rho_{\mathcal{G}/\mathcal{H}}$ the left permutation representation of $\mathcal{G}$ relative to $\mathcal{H}$.*

Let $\rho_{\mathcal{G}/\mathcal{H}}$ decompose into irreducibles as $\rho_{\mathcal{H}} = \bigoplus_j \rho_j$. For $g \in \mathcal{G}$, define the matrix A_g by $(A_g)_{uv} = (A_G)_{uv} \times \left|\left\{e \mid \alpha(e) = g, e^- = u, e^+ = v\right\}\right|$. Then A_G is conjugate to the block matrix

$$\bigoplus_j \sum_{g\in\mathcal{G}} A_g \otimes \rho_j(g)$$

Proof. Let P_g be the permutation matrix acting on $\mathbb{C}^{\mathcal{G}/\mathcal{H}}$ according to the left action $h\mathcal{H} \mapsto gh\mathcal{H}$. Then it's easy to see that

$$A_{G^{\alpha/\mathcal{H}}} = \sum_{g\in\mathcal{G}} A_g \otimes P_g$$

when $V(G^{\alpha/\mathcal{H}})$ is indexed by the dictionary order of $V \times \mathcal{G}/\mathcal{H}$. On the other hand, $\rho_{\mathcal{G}/\mathcal{H}} : g \mapsto P_g$, so by Maschke's theorem there is some change of basis matrix P such that $\forall g \in \mathcal{G} : PP_gP^{-1} = \bigoplus_j \rho_j(g)$. Using Fact 3.17, we have

$$(I_N \otimes P)A_{G^{\alpha/\mathcal{H}}}(I_N \otimes P^{-1}) = \sum_{g\in\mathcal{G}} A_g \otimes (PP_gP^{-1}) = \sum_{g\in\mathcal{G}} A_g \otimes \left(\bigoplus_j \rho_j(g)\right) = \bigoplus_j \sum_{g\in\mathcal{G}} A_g \otimes \rho_j(g)$$

Finally, $(I_N \otimes P^{-1}) = (I_N^{-1} \otimes P)^{-1} = (I_N \otimes P)^{-1}$ by the mixed product property, so we have the conjugation we wanted. □

As we discussed in Example 3.14, we have that, say, ρ_1 is the trivial representation; then $\sum_{g\in\mathcal{G}} A_g \otimes \rho_1(g) = A_G$; the remaining blocks $S_{\alpha/\mathcal{H}}$ give us the *signing matrix* of the lift. We now show how the above is a common generalization of some known results:

Example 3.19. Let's recover and generalize the signing matrix for the special cases [**BL06, AKM13**]. Bilu and Linial studied 2-lifts of simple graphs, so we're looking at ordinary voltage lifts in $\mathbb{Z}/2$. From Examples 3.10 and 3.15, we know that the regular representation splits into the trivial representation and the *sign* representation $0 \mapsto 1, 1 \mapsto -1$. Applying Theorem 3.18 tells us that the matrix that captures the new eigenvalues of the lift (when the base graph is undirected) in this case is the matrix where the (u, v) entry equals the number of edges $u \to v$ lifted via the identity permutation, *minus* the number of edges $u \to v$ lifted via the transposition (1 2). This generalizes their signing matrix to digraphs.

Agarwal, Kolla and Madan studied so-called *shift k-lifts*, which are equivalent to derived graphs of ordinary voltage assignments in $\mathbb{Z}/k\mathbb{Z}$. Here we have $k-1$ nontrivial representations, so there are $k-1$ matrices that capture the new eigenvalues, one for each representation $a \mapsto \omega^{ta}$ where $t \neq 0$; the analogous generalization to undirected digraphs holds here.

Example 3.20. Let's recover the special case of the spectra of Cayley/Schreier graphs presented in Section 11 of the survey [**HLW06**]. As we saw in Example 3.1, a Cayley graph $\mathrm{Cay}(\mathcal{G}, S)$ can be thought of as the derived graph of an ordinary voltage assignment of B_S with voltages in $\mathcal{G}$. Then our signing matrix takes a very simple form: it is block-diagonal, with the block corresponding to the irreducible representation ρ_j given by $\sum_{s\in S} \rho_j s$. The analogous statement holds for Schreier graphs.

3.3. Voltage groups for towers of lifts

In this section, we show that taking a sequence of lifts with permutation voltages in the permutation groups $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n$ respectively is equivalent to taking a single lift with permutation voltages in the *wreath product* $\mathcal{G}_n \wr \ldots \wr \mathcal{G}_2 \wr \mathcal{G}_1$. Note that it is not obvious in advance that such a sequence of lifts should be *equivalent* to a single lift in any voltage group!

One way to think of wreath products is as certain restricted groups of symmetries of *rooted regular trees*; another is as special cases of *semidirect products*. We now provide some background for these terms,

loosely following [**RSW06**]; the semidirect product will be useful again in our discussion of the zig-zag product later on.

3.3.1. Semidirect products and wreath products. We know from group theory a natural way to 'put two groups $\mathcal{G}$ and $\mathcal{H}$ together': just take the direct product $\mathcal{G} \times \mathcal{H}$, which treats the two groups independently. When there is some interaction between the two groups, one can define a generalization of the direct product called the *semidirect product*. One motivation comes from solving the following *extension problem*: suppose we have a *short exact sequence* of groups

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

that is, α is an injective homomorphism, β is a surjective homomorphism, and $\operatorname{im}\alpha = \ker\beta$. Suppose we know $\mathcal{G}$ and $\mathcal{H}$; can we recover $\mathcal{K}$? Intuitively, the short exact sequence is telling us that $\mathcal{K}$ should be in some sense 'assembled' from $\mathcal{G}$ and $\mathcal{H}$. In the case of abelian groups, which comes up frequently in homological algebra, if we require the existence of a homomorphism $\gamma : \mathcal{H} \to \mathcal{K}$ such that $\beta \circ \gamma = \mathrm{id}_{\mathcal{H}}$, the sequence is said to *split*, and $\mathcal{K} = \mathcal{G} \oplus \mathcal{H}$. For general groups however, failure of $\gamma(\mathcal{H})$ being normal in $\mathcal{K}$ complicates things, and instead $\mathcal{K}$ is a *semidirect product* $\mathcal{G} \rtimes \mathcal{H}$[2]. More concretely, one way to define the semidirect product which is convenient for us is

Definition 3.21. Suppose we have groups $\mathcal{G}$ and $\mathcal{H}$, and that $\varphi : \mathcal{H} \to \mathrm{Aut}(\mathcal{G})$ is a homomorphism to the right automorphism group of $\mathcal{G}$, i.e. $\mathcal{H}$ acts on $\mathcal{G}$ on the right by automorphisms φ_h. Then the **semidirect product** $\mathcal{G} \rtimes_\varphi \mathcal{H}$ with respect to φ is the group with underlying set $\mathcal{G} \times \mathcal{H}$ and group law[3]

$$(g_1, h_1) \circ (g_2, h_2) = (\varphi_{h_2}(g_1)g_2, h_1h_2)$$

It's immediate that this indeed defines a group structure with identity element $(\mathrm{id}_{\mathcal{G}}, \mathrm{id}_{\mathcal{H}})$. The *wreath product* is a special case of the semidirect product for permutation groups:

Definition 3.22. Suppose $\mathcal{G}$ and $\mathcal{H}$ are finite permutation groups acting on sets $S_{\mathcal{G}}, S_{\mathcal{H}}$ respectively. Then the **wreath product** $\mathcal{G} \wr \mathcal{H}$ is the semidirect product $\mathcal{G}^{S_{\mathcal{H}}} \rtimes \mathcal{H}$ with the action of $h \in \mathcal{H}$ on $\mathcal{G}^{S_{\mathcal{H}}}$ is given by permuting the coordinates as $\varphi_h : (g_1, g_2, \ldots) \mapsto (g_{h(1)}, g_{h(2)}, \ldots)$.

Note that it is somewhat confusing that this gives a right action on $\mathcal{G}^{S_{\mathcal{H}}}$, but you can easily verify for yourself that it does! It turns out that the wreath product naturally inherits the structure of a permutation group:

Proposition 3.23. *The group $\mathcal{G} \wr \mathcal{H}$ acts faithfully on the set $S_{\mathcal{G}} \times S_{\mathcal{H}}$ in a natural manner.*

Proof. Given $\mu \in \mathcal{G}^{S_{\mathcal{H}}}$ and $\pi \in \mathcal{H}$, we define the action of $(\mu, \pi) \in \mathcal{G} \wr \mathcal{H}$ on a point $(s, t) \in S_{\mathcal{G}} \times S_{\mathcal{H}}$ as $(\mu, \pi)(s, t) = (\mu_t(s), \pi(t))$. We have to verify this is indeed an action of $\mathcal{G} \wr \mathcal{H}$. The identity element has $\mu = (\mathrm{id}_{\mathcal{G}}, \ldots, \mathrm{id}_{\mathcal{G}})$ and $\pi = \mathrm{id}_{\mathcal{H}}$ so it fixes every (s, t). Next, for $(\mu', \pi') \in \mathcal{G} \wr \mathcal{H}$, we have

$$(\mu', \pi')[(\mu, \pi)(s, t)] = (\mu', \pi')(\mu_t(s), \pi(t)) = (\mu'_{\pi(t)}\mu_t(s), \pi'\pi(t))$$

and

$$[(\mu', \pi') \circ (\mu, \pi)](s, t) = [\varphi_\pi(\mu')\mu, \pi'\pi](s, t) = (\mu'_{\pi(t)}\mu_t(s), \pi'\pi(t))$$

Finally, assuming $(\mu, \pi)(s, t) = (\mu', \pi')(s, t)$ for all (s, t) gives us $\mu_t(s) = \mu'_t(s)$ and $\pi(t) = \pi'(t)$ for all s, t, from which $\mu = \mu'$ and $\pi = \pi'$ so the action is faithful. □

[2] A way to remember which factor goes on which side of the $\rtimes$ is to keep in mind the short exact sequence: the order is the same.

[3] The reason for the somewhat non-standard convention of using $\varphi_{h_2}(g_1)g_2$ instead of $g_1\varphi_{h_1}(g_2)$ has to do with issues of handedness in the discussion that follows: one of the actions that arise is more natural as a right action, and we'd rather keep in mind one right action than keep dragging around inverses.

3.3.2. Automorphisms of regular rooted trees and iterated wreath products. Our central example of wreath products comes from the automorphism groups of regular trees; in fact, they provide such a convenient visualization of wreath products and make so many of their properties obvious that they are arguably the 'right' way to think about wreath products.

NOTATION 3.24. *Let $T_{S_1,\dots,S_n}$ stand for the rooted tree of depth n in which every node at distance $i < n$ from the root has children labelled by the elements of the set S_{i+1}.*

To describe a vertex in this tree, we can give the tuple of labels along the unique path from the root: so the root is represented by the empty tuple () and in general $(s_1, s_2, \dots, s_n)$ stands for the s_n-th child of the s_{n-1}-th child of ... of the s_1-th child of the root. Any automorphism of $T_{S_1,\dots,S_n}$ must carry the set of leaves bijectively to itself, and thus the set of nodes a distance one from a leaf bijectively to itself, and so on, inductively we see that every level is carried to itself bijectively; moreover, nodes with a common parent are carried to children of the image of that parent.

Thus, to describe an automorphism of $T_{S_1,\dots,S_n}$ it suffices to give, for each vertex $(s_1, \dots, s_i)$ at distance $i < n$ from the root, an element $\pi_{s_1,\dots,s_i} \in \mathrm{Sym}(S_{i+1})$ according to which the children of that vertex are permuted. Then the automorphism ϕ described by these permutations moves vertices by

$$\phi : (s_1, s_2, \dots, s_i) \mapsto (\pi_{()}(s_1), \pi_{s_1}(s_2), \dots, \pi_{s_1,\dots,s_{i-1}}(s_i))$$

This formula captures the similarity to the wreath product, and much more. Now consider the **restricted automorphism group** of $T_{S_1,\dots,S_n}$ with respect to the groups $\mathcal{G}_i \subset \mathrm{Sym}(S_i)$, where a node at distance i from the root can permute its children only by elements of some permutation group $\mathcal{G}_{i+1}$.

PROPOSITION 3.25. *The wreath product is associative, and in fact the restricted automorphism group of $T_{S_1,\dots,S_n}$ with respect to $\mathcal{G}_i \subset \mathrm{Sym}(S_i)$ is $\mathcal{G}_n \wr \dots \wr \mathcal{G}_1$, realized as a permutation group on the set of leaves $S_1 \times \dots \times S_n$.*

PROOF. The proof is by induction on n: the main point is that the automorphism group is completely determined by the permutations it induces on the leaves! For $n = 1$ there is nothing to prove. For $n = 2$, the automorphism that acts by π on the root and by μ_s on $s \in S_1$ acts on $S_1 \times S_2$ in the same way as $\mathcal{G}_2 \wr \mathcal{G}_1$, and since the action is faithful, the automorphism group is isomorphic to $\mathcal{G}_2 \wr \mathcal{G}_1$.

For $n > 2$, assume for now right-associative notation for wreath products. Denote $T_n = T_{S_1,\dots,S_n}$ and $T_{n-1} := T_{S_1,\dots,S_{n-1}}$. We can imagine replacing the subtree T_{n-1} by the depth-1 tree $T_{S_1\times\dots\times S_{n-1}}$ with the same set of leaves. Since the restricted automorphism group of T_{n-1} is $\mathcal{G}_{n-1} \wr \dots \wr \mathcal{G}_1$ by hypothesis, and where the leaves can go depends only on where their parents can go and the group $\mathcal{G}_n$, we see that the leaves of T_n can be permuted in the same way by the restricted automorphism group of T_n and that of $T_{S_1\times\dots\times S_{n-1},S_n}$ with respect to $\mathcal{G}_{n-1} \wr \dots \wr \mathcal{G}_1$ and $\mathcal{G}_n$, By the case $n = 2$, the latter permutation group is $\mathcal{G}_n \wr \mathcal{G}_{n-1} \wr \dots \wr \mathcal{G}_1$, and it equals the group we wanted to find.

Finally, here's a sketch proof of associativity: if we have a depth-3 tree T, there are two ways we can split it into depth-1 and depth-2 trees; replacing the depth-2 trees by depth-1 trees as in the above induction step gives us the restricted permutation groups $(\mathcal{G}_3 \wr \mathcal{G}_2) \wr \mathcal{G}_1$ and $\mathcal{G}_3 \wr (\mathcal{G}_2 \wr \mathcal{G}_1)$ on the leaves of T; but these should both equal the restricted automorphism group of T with respect to $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$! □

We also describe some common inclusions into the iterated wreath product that will be helpful in Section 5.1:

EXAMPLE 3.26. Given $\mathcal{G}_n \wr \dots \wr \mathcal{G}_1$, there is a natural inclusion $\mathcal{G}_m \wr \dots \wr \mathcal{G}_1 \hookrightarrow \mathcal{G}_n \wr \dots \wr \mathcal{G}_1$ whenever $m < n$ by mapping an automorphism of the first m levels to an automorpism on the first n levels that acts by the identity permutation on every node below the m-th level. There is the 'orthogonal' inclusion $(\mathcal{G}_n \wr \dots \wr \mathcal{G}_{m+1})^{S_1\times\dots\times S_m} \hookrightarrow \mathcal{G}_n \wr \dots \wr \mathcal{G}_1$ by acting on the first m levels trivially, and permuting the children of the leaf $(s_1, \dots, s_m)$ of $T_{S_1,\dots,S_m}$ via the $(s_1, \dots, s_m)$-th coordinate. The special cases $m = n-1$ and $m = 1$ will be useful in Section 5.1.

EXAMPLE 3.27. For any $\mathcal{G}_n \wr \ldots \wr \mathcal{G}_1$, there is an inclusion $\mathcal{G}_1 \times \ldots \times \mathcal{G}_n \hookrightarrow \mathcal{G}_n \wr \ldots \wr \mathcal{G}_1$ obtained by sending $(g_1, \ldots, g_n)$ to the automorphism that acts by g_i on every node at level i.

3.3.3. The computation. Here is the main observation[4]:

PROPOSITION 3.28 (VOLTAGE GROUPS OF TOWERS). *Suppose we have a sequence of covering maps $G_n \xrightarrow{p_n} G_{n-1} \xrightarrow{p_{n-1}} \ldots \to G_1 \xrightarrow{p_1} H$, where p_i is obtained by permutation voltages in the permutation group $\mathcal{G}_i$ acting on the set S_i. Then the composition $p_1 \circ \ldots \circ p_n : G_n \to H$ is obtained by permutation voltages in $\mathcal{G}_n \wr \ldots \wr \mathcal{G}_1$.*

Conversely, given any covering $p : G \to H$ with permutation voltages in $\mathcal{G}_n \wr \ldots \wr \mathcal{G}_1$, it corresponds to a tower of lifts of the above kind.

PROOF. This is really all about the case $n = 2$; the rest is induction. So, we induct on n: for $n = 1$, there is nothing to prove, and we will establish the $n = 2$ case later; now suppose that for some $k \in \mathbb{N}$, the assertion holds true with $n = k$. Let $\widetilde{\mathcal{G}_k} = \mathcal{G}_k \wr \ldots \wr \mathcal{G}_1$ and $\widetilde{S_k} = S_k \times \ldots \times S_1$. For the first direction, let $\widetilde{p_k} = p_1 \circ \ldots \circ p_k$. Then we have coverings $G_{k+1} \xrightarrow{p_{k+1}} G_k \xrightarrow{\widetilde{p_k}} H$, and by the induction hypothesis $\widetilde{p_k}$ is obtained by permutation voltages in $\widetilde{\mathcal{G}_k}$ which acts on $\widetilde{S_k}$. Using the case $n = 2$, this means that the composition $\widetilde{p_k} \circ p_{k+1}$ is obtained by permutation voltages in $\mathcal{G}_{k+1} \wr \widetilde{\mathcal{G}_k} = \mathcal{G}_{k+1} \wr \ldots \wr \mathcal{G}_1$ as we wanted. For the other direction, we have a lift with voltages in $\mathcal{G}_{k+1} \wr \ldots \wr \mathcal{G}_1 = \mathcal{G}_{k+1} \wr \widetilde{\mathcal{G}_k}$. Using the case $n = 2$, this means that we have a sequence of coverings $G_{k+1} \xrightarrow{p_{k+1}} G_k \xrightarrow{\widetilde{p_k}} H$ where p_{k+1} has voltages in $\mathcal{G}_{k+1}$, and $\widetilde{p_k}$ has voltages in $\widetilde{\mathcal{G}_k}$. Applying the induction hypothesis to $\widetilde{p_k}$, we're done.

It remains to establish the case $n = 2$; it suffices to think about a single edge $u \xrightarrow{e} v$ in H, and what permutations it can be assigned by our lifts. For the forward direction, let e be assigned $\pi \in \mathcal{G}_1$ by p_1, thus lifting to S_1 edges; then let the one with tail (v, s) be assigned $\mu_s \in \mathcal{G}_2$ by p_2. The resulting permutation σ on $S_1 \times S_2$ that is assigned to e by $p_1 \circ p_2$ is then given by

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

Now consider the depth-2 rooted tree T where the root has children labelled by S_1, and each child has leaves labelled by S_2: then the leaves are in bijection with $S_1 \times S_2$, and as we saw in Proposition 3.23, the above formula means that σ is precisely an element of its restricted automorphism group $\mathcal{G}_2 \wr \mathcal{G}_1$.

For the reverse direction, given a covering $p : G \to H$ with permutation voltages in $\mathcal{G}_2 \wr \mathcal{G}_1$ and a permutation $\sigma \in \mathcal{G}_2 \wr \mathcal{G}_1$ assigned to e, represent sigma as an element $((\ldots, \mu_s, \ldots), \pi) \in \mathcal{G}_2^{S_1} \rtimes \mathcal{G}_1$ of the automorphism group of T. Then reasoning analogously to the previous direction, we see that lifting e according to π and then lifting the copy of e with tail (v, s) according to μ_s gives us exactly G; the intermediate lift K fits into the diagram $G \xrightarrow{p_2} K \xrightarrow{p_1} H$ that we wanted to find.

□

[4]This is easy once one knows the answer; the proof we present here was optimized for conciseness. The way one comes up with the result in the first place is by considering the case $n = 2$, realizing $\mathcal{G}_1$ and $(\mathcal{G}_2)^{S_1}$ as certain natural subgroups of the conjectured voltage group of $p_1 \circ p_2$, and then reasoning about their interaction to arrive at a semidirect product.

CHAPTER 4

Lifting graph operations

It turns out that several common graph operations that have useful effects on expansion respect covering maps, in the sense that, for an operation α, if $G \to H$ is a covering, we get a covering $\alpha(G) \to \alpha(H)$. This is perhaps not so surprising for well-behaved operations with an 'algebraic' flavor, like *powering* and *tensoring*, but it also works for the more 'twisted' *derandomized graph products*, namely the *zig-zag product* of Reingold, Vadhan and Wigderson [**RVW02**] that is the cornerstone of elementary explicit constructions of expanders, the *generalized zig-zag product* of Ben-Aroya and Ta-Shma [**BATS11**], and the *derandomized square* of Rozenman and Vadhan [**RV05**] that is related to the zig-zag product and was used to give an alternative proof that **L** = **SL**. It seems the reason all these results work is because these graph operations are defined *locally*, and local structure is preserved by lifts. We remark that the result on zig-zag products was independently observed by Cooper, Dotterrer and Prassidis [**CDP06**]. We also introduce a graph product, called the *backward-forward square*, which can be used instead of the ordinary square in iterative constructions where we desire undirected graphs, and which allows us to translate expanding towers of directed graphs into expanding towers of undirected graphs without terrible losses – so we don't have to worry too much about issues of directedness!

We will use these operations' compatibility with covering maps as the key step in a general technique to iteratively construct expanding towers of coverings inspired by a construction by Rozenman, Shalev and Wigderson [**RSW06**] in Section 5.1. Another implication of these results is that whenever we have an expanding tower, we can apply any of our operations to all graphs in it to translate it to another expanding tower. Since various classical explicit constructions of expanders can be tweaked to give an expanding tower of Cayley/Schreier graphs, this gives us a way of producing some new expander families from them.

The operations we introduce act in various ways on number of vertices, degree and expansion, so it's convenient to define

Definition 4.1. An (n, d, λ)-**graph** is a d-regular digraph G on n vertices with $\lambda(G) \leq \lambda$; similarly, an (N, D, λ)-**graph** is a D-regular digraph G on vertex set N with $\lambda(G) \leq \lambda$.

4.1. Rotation maps and their lifts

A *rotation map* is a way of keeping track of edges in graphs by specifying labels to the edges incident to each vertex and the way these labels interact. Rotation maps were initiated by Reingold, Vadhan and Wigderson in [**RVW02**], where they were used to define and study the zig-zag product. They were further generalized by Rozenman and Vadhan in [**RV05**] to directed graphs; this is the source we follow in this section (except when talking about lifts).

Rotation maps are useful when we want to reason about multigraphs where there might be many edges between a pair of vertices, and when we want to reason about the explicitness of various operations on graphs (which can be encoded in terms of their rotation maps). In this section, we state the definition of a rotation map for directed and undirected digraphs, and prove some basic facts about the interaction between rotation maps and coverings.

Definition 4.2. For a d-regular digraph $G = (V, E)$, we define a **two-way labelling** to be, for each $v \in V$, a pair of bijections $\left\{e \in E \;\middle|\; e^- = v\right\} \to D$ and $\left\{e \in E \;\middle|\; e^+ = v\right\} \to D$ for some set D with $|D| = d$.

In other words, giving a two-way labeling to a digraph is making it into a D-regular graph.

NOTATION 4.3. *For a digraph G and a two-way labeling l_G of G, we will write $(G; l_G)$ for the version of G labeled by l_G. We will use the $(G; l_G)$ notation whenever there might be confusion about which labels a digraph is given; if there is an obvious labeling from context, we just write G. Whenever we have an edge $u \xrightarrow{e} v$ with label i at u and j at v, we will denote it by $u \xrightarrow{i\ e\ j} v$ to simplify notation. When the name of the edge is not important, we omit it.*

DEFINITION 4.4. For a D-regular digraph G, define the **rotation map** of G with respect to the labeling to be the function $\mathrm{Rot}_G : V(G) \times D \to V(G) \times D$ given by

$$\mathrm{Rot}_G(u, i) = (v, j) \text{ when } u \xrightarrow{i\quad j} v \in E(G)$$

Observe that the rotation map completely specifies the graph and the two-way labelling, and it is a permutation of $V(G) \times D$. We will very often encode a rotation $\mathrm{Rot}_G(u, i) = (v, j)$ by the more visually appealing $u \xrightarrow{i\quad j} v \in E(G)$. The corresponding notion for undirected graphs needs some additional structure:

DEFINITION 4.5. For an undirected digraph G, an **(undirected) two-way labeling** is a two-way labeling of G where we require that if $u \xrightarrow{i\ e\ j} v \in E(G)$, the edge opposite to e is labeled as $v \xrightarrow{j\ e'\ i} u$.

Another property of two-way labelings we will need later on is

DEFINITION 4.6. A digraph G is called **consistently two-way labeled** if, for every edge, the label at the tail is the same as the label at the head.

Given the 'local' view of a graph that rotation maps give us, it's expected that given a covering of graphs and a rotation map for the base graph, there is a natural way to define a rotation map for the lift. It is fortunate that the formula for the rotation map is the same in the directed and undirected cases: the conventions from Definition 4.5 and Remark 2.12 take care of this behind the scenes.

PROPOSITION 4.7. *Suppose $p : G \to H = (V, E)$ is a covering of directed (respectively undirected) d-regular digraphs via permutation voltage assignment $\pi : E \to \mathrm{Sym}(S)$, and H is a directed (respectively undirected) two-way labeled digraph with rotation map Rot_H. Then there is a natural induced rotation map on G given by*

$$\mathrm{Rot}_G([v, s], i) = ([u, \pi_e(s)], j)$$

where $(u, j) = \mathrm{Rot}_H(v, i)$ and e is the i-th edge out of v. Moreover, if H is consistently labeled, G inherits such a labeling.

PROOF. This is a routine computation. First, let's deal with directed digraphs. Observe that G inherits a two-way labeling by composing the labeling on H with the bijections $\left\{e \in E(G) \;\middle|\; e^{\pm} = v\right\} \xrightarrow{p_E} \left\{e \in E(H) \;\middle|\; e^{\pm} = p_V(v)\right\}$. This induces a rotation map on G. Consider a vertex $[v, s] \in V(G)$, and let $v \xrightarrow{i\ e\ j} u$ in H. Then, if e_s is the lift of e with tail $[v, s]$, by the definition of the labelling in G we have $[v, s] \xrightarrow{i\ e_s\ j} [u, \pi_e s]$ which encodes the rotation map we wanted.

For undirected digraphs, we need to verify that G inherits an undirected two-way labeling from H. So consider a pair of opposite edges $v \xrightarrow{i\ e\ j} u$ and $u \xrightarrow{j\ e'\ i} v$ in H. Let e_s be the lift of e with tail $[v, s]$ and e'_s the lift of e' with tail $[u, \pi_e s]$; since by convention we assign inverse permutations to pairs of opposite edges, the head of e'_s is $[v, \pi_e^{-1}\pi_e s] = [v, s]$. So by the previous paragraph, in G we have the pair of opposite edges $[v, s] \xrightarrow{i\ e_s\ j} [u, \pi_e s]$ and $[u, \pi_e s] \xrightarrow{j\ e'_s\ i} [v, s]$, as needed. Finally, it's obvious from our definition of the two-way labeling on G that if H is consistently labeled, so is G. □

The above result is in a particularly simple form: it says that to obtain the rotation map of the lift, we simply need to 'insert' one more coordinate, a **lift coordinate**, in the rotation map of the base, and change that coordinate according to the relevant permutation; moreover, it applies equally well to directed and undirected graphs. It will be convenient to define the following terms:

Definition 4.8. A **labeled covering map** $p : (G; l_G) \to (H; l_H)$ of S-regular digraphs is a covering map of digraphs $p : G \to H$ such that, when H is given labels l_H, the labels induced on G by the process from Proposition 4.7 are l_G; clearly the composition of labeled covering map is again a labeled covering map.

Notation 4.9. *For a cover $p : G \to H$ and an edge $u \xrightarrow{i \quad j} v \in E(H)$, denote the permutation assigned by p to that edge by $\pi_{u,i}$.*

4.1.1. Graphs that cover B_S. Later on, we will be very interested in which digraphs cover a bouquet of circles. We provide two points of view: one via two-way labelings, the other via Schreier graphs:

Proposition 4.10. *For an $|S|$-regular digraph G, the following are equivalent:*

(1) There exists a covering map $p : G \to B_S$;
(2) There is a consistent two-way labeling of G;
(3) G is a Schreier graph.

Proof. (1) $\iff$ (2): For the forward direction, if an edge of G projects to the s-th loop of B_S, label that edge by s on the head and tail. Since p is a covering map, the out-labels at each vertex are in bijection with S, and so are the in-labels at each vertex. For the backward direction, given such a labeling, project an edge $u \xrightarrow{s \quad s} v$ to the s-th loop; since the labeling is valid, it gives a covering map.

(2) $\iff$ (3): The method used here is similar to the one Gross used [**Gro77**] to show that any connected *undirected* regular digraph of even degree is a Schreier coset graph. For the forward direction, observe that, for every $s \in S$, the map $\pi_s : V(G) \to V(G)$ given by $v \mapsto u$ where $v \xrightarrow{s \quad s} u \in E(G)$ is a permutation, since every u has a unique in-edge and out-edge labeled by s at u. Letting $\mathcal{G} \subset \mathrm{Sym}(V(G))$ be the group of permutations generated by $T = \left\{ \pi_s \;\middle|\; s \in S \right\}$, we see that G is exactly $\mathrm{Sch}(\mathcal{G}, V(G), T)$.

For the reverse direction, notice that in an $|S|$-regular Schreier digraph, every edge $u \xrightarrow{s} v$ has a natural name given by the generator s that gives rise to it. Then labeling it as $u \xrightarrow{s \; s \; s} v$ gives us a consistent two-way labeling. □

Example 4.11. Suppose G is an undirected digraph of even degree $2d$. Then Gross [**Gro77**] (notice that the paper works in the generality of undirected multigraphs) tells us[1] that every connected component of G can be realized as the Schreier coset graph of some group $\mathcal{G}$ with respect to some symmetric generating set $S = T \cup T^{-1}$. Thus we have a covering map from every component of G to B_{2d}, which when joined together give us a covering map $G \to B_{2d}$. Notice that, however, it's not obvious how to compute a Schreier structure on G efficiently!

4.2. Powering

4.2.1. Definition and expansion properties. *Powering* is a basic graph operation that takes a graph and forms another graph on the same vertex set where the edges correspond to length k walks in the original graph. Formally,

Definition 4.12. For a digraph G, the **k-th power** G^k of G is the graph with vertices $V(G^k) = V(G)$ and edges given by all k-step walks on G:

$$E(G^k) = \left\{ (e_1, \ldots, e_k) \;\middle|\; e_i \in E(G) \text{ and } e_i^+ = e_{i+1}^- \right\}$$

[1] Also see the discussion after Theorem 11.16 in Hoory et al [**HLW06**].

with $(e_1, \dots, e_k)^- = e_1^-$ and $(e_1, \dots, e_k)^+ = e_k^+$. When G is two-way labeled, the standard choice of rotation map is

$$\mathrm{Rot}_{G^k}(w_0, (l_1, l_2, \dots, l_k)) = (w_k, (r_k, r_{k-1}, \dots, r_1))$$

where the right side is defined inductively by $w_{i-1} \xrightarrow{l_i \quad r_i} w_i \in E(G)$.

Moreover, this preserves undirected graphs: if G comes with an undirected two-way labeling, the above rotation map is easily seen to induce an undirected two-way labeling on G^k.

The random walk on G^k is a random walk on G that takes k steps at a time, so we can think of it as a 'k times faster' copy of the random walk on G. Correspondingly, we expect it to converge to the uniform distribution k times faster! Since in our bounds time is in the exponent of λ_2, we expect the spectral expansion of G^k to be $\lambda(G)^k$. Indeed, a standard calculation gives $A_{G^k} = (A_G)^k$, and thus

Proposition 4.13. *For an (n, d, λ)-digraph G, G^k is an (n, d^k, λ^k)-digraph.*

Proof. When walking a d-regular digraph, there are d choices at each step for the next edge to take; thus the number of k-step walks out of any given vertex is d^k. Similarly, there are d edges to come from, so the k-step walks that end at any given vertex are also d^k. Next, since W_G preserves the subspace u_G, it preserves the orthogonal complement $u_G^\perp$, and thus for any $x \perp u_G$ we have

$$\|W_{G^k} x\| = \|(W_G)^k x\| = \|W_G(W_G^{k-1} x)\| \le \lambda \|(W_G)^{k-1} x\| \le \dots \le \lambda^k \|x\|$$

□

We remark that when G is undirected, using the eigenvalues this can be strengthened to say that in fact $\lambda(G^k) = \lambda(G)^k$; but for general digraphs, no such result holds (see footnote 5 in [**RV05**]).

4.2.2. Lifting properties. The main observation in this section is that graph powering 'respects' covering maps:

Proposition 4.14. *If $p : G \to H$ is a labeled covering map, there is a natural labeled covering map $q : G^k \to H^k$ for all k. Moreover, this is compatible with undirected graphs: if $G \to H$ is a covering of undirected digraphs, so will be q.*

Proof. Suppose we have an edge $w_0 \xrightarrow{(l_1,\dots,l_k) \quad (r_k,\dots,r_1)} w_k \in E(H^k)$ coming from a walk

$$w_0 \xrightarrow{l_1 \ e_1 \ r_1} w_1 \xrightarrow{l_2 \ e_2 \ r_2} \dots \longrightarrow w_{k-1} \xrightarrow{l_k \ e_k \ r_k} w_k$$

in H. Then every edge in that walk gives rise to edges in the lift G; in particular, we have edges

$$(w_0, s) \xrightarrow{l_1 \quad r_1} (w_1, \pi_{e_1} s) \in E(G), \ (w_1, \pi_{e_1} s) \xrightarrow{l_2 \quad r_2} (w_2, \pi_{e_2}\pi_{e_1} s) \in E(G),$$
$$\dots, (w_{k-1}, \pi_{e_{k-1}} \dots \pi_{e_1} s) \xrightarrow{l_k \quad r_k} (w_k, \pi_{e_k}\pi_{e_{k-1}} \dots \pi_{e_1} s) \in E(G)$$

These in turn define an edge in $E(G^k)$:

$$(w_0, s) \xrightarrow{(l_1,\dots,l_k) \quad (r_k,\dots,r_1)} (w_k, \pi_{e_k}\pi_{e_{k-1}} \dots \pi_{e_1} s) \in E(G^k)$$

Since the permutation $\pi_{e_{k-1}} \dots \pi_{e_1}$ is uniquely determined by w_0 and $l_1, \dots, l_k$, this means that G^k is exactly the labeled cover of H^k where the $(l_1, \dots, l_k)$-th edge out of w_0 lifts via the permutation $\pi_{e_k} \dots \pi_{e_1}$!

To deal with undirected graphs, observe that if $p : G \to H$ is a covering of undirected digraphs, then the permutations assigned to opposite edges in H^k are $\pi_{e_k} \dots \pi_{e_1}$ and $\pi_{e_1}^{-1} \dots \pi_{e_k}^{-1}$, which are inverses of each other, so $p^k : G^k \to H^k$ is a covering of undirected digraphs as well! □

4.3. Tensoring

4.3.1. Definition and expansion properties. The tensor product of two graphs, as the name suggests, is the tensor product of their corresponding adjacency matrices:

Definition 4.15. For digraphs G and H, the **tensor product** $G \otimes H$ is the digraph with adjacency matrix $A_{G\otimes H} = A_G \otimes A_H$.

The adjacency matrix hides some of the information if we care about the labels; but there is a natural way to track which edge of $G \otimes H$ comes from which edges of G and H, and so we can give a definition in terms of rotation maps:

Definition 4.16. For two-way labeled regular digraphs G and H, the **tensor product** $G \otimes H$ is the regular digraph with vertex set $V(G) \times V(H)$, and rotation map

$$\mathrm{Rot}_{G\otimes H}((u,u'),(l,l')) = ((v,v'),(r,r'))$$

where $u \xrightarrow{l\quad r} v \in E(G)$ and $u' \xrightarrow{l'\quad r'} v' \in E(H)$.

It's easy to check this gives the same digraph. Thus, we can think of the random walk on the tensor product $G \otimes H$ as two simultaneous, independent copies of the random walks on G and H. Each of these approach uniformity at some rate, so we would expect the combined walk to approach uniformity at the rate of the walk that approaches uniformity more slowly; for example, imagine that the H walk takes longer to approach uniformity, and consider a walk on $G \otimes H$ that starts out as uniform on each $V(G) \times \{v\}$: then it's easy to see this walk is a 'blown-up' version of the random walk on H.

This is indeed the case, but before we can prove that, we will need the following

Fact 4.17. *For square matrices A and B with singular values $\sigma_1, \ldots, \sigma_n$ and $\mu_1, \ldots, \mu_m$, the singular values of $A \otimes B$ are*

$$\left\{\sigma_i\mu_j \;\middle|\; 1 \le i \le n, 1 \le j \le m\right\}$$

With this, we easily prove our intuition is right:

Corollary 4.18. *$\lambda(G_1 \otimes G_2) = \max\{\lambda(G_1), \lambda(G_2)\}$, so in particular, if G_1 is an (n_1, d_1, λ_1) graph, and G_2 is an (n_2, d_2, λ_2) graph, then $G_1 \otimes G_2$ is an $(n_1n_2, d_1d_2, \max\{\lambda_1, \lambda_2\})$-graph.*

Proof. We know that W_{G_1}, W_{G_2} have singular values $1 \ge \sigma_2 \ge \ldots \ge 0$ and $1 \ge \mu_2 \ge \ldots \ge 0$; hence the second singular value of $W_{G_1} \otimes W_{G_2}$ is the larger of $\sigma_2 \times 1$ and $1 \times \mu_2$. □

4.3.2. Lifting properties. It turns out that tensoring is also compatible with lifts. Some intuition for that comes from the observation that the tensor product $G \otimes H$ when H is d-regular can be thought of as a special lift of the graph obtained by replacing each edge of G by d identical copies of itself. This is not surprising if we recall the proof of Theorem 3.18 where we made heavy use of tensors! Here is the general statement:

Proposition 4.19. *If $p_1 : G_1 \to H_1$ and $p_2 : G_2 \to H_2$ are respectively a labeled S_1- and labeled S_2-covering of digraphs, there is a natural induced $S_1 \times S_2$-covering map $q : G_1 \otimes G_2 \to H_1 \otimes H_2$. Moreover, if p_i are coverings of undirected digraphs, so is q.*

Proof. Let's have edges $u_i \xrightarrow{l_i\quad e_i\quad r_i} v_i \in E(H_i)$. These give rise to the edge $(u_1,u_2) \xrightarrow{(l_1,l_2)\quad (r_1,r_2)} (v_1,v_2) \in E(H_1 \otimes H_2)$. We can now define an $S_1 \times S_2$ lift of $H_1 \otimes H_2$ by lifting the latter edge via the product permutation of $S_1 \times S_2$ that acts independently on the factors by $\pi^{(i)}_{(u_i,l_i)}$; that is, the rotation map of the lift is encoded by

$$[(u_1,u_2),(s_1,s_2)] \xrightarrow{(l_1,l_2)\quad (r_1,r_2)} \left[(v_1,v_2), \left(\pi^{(1)}_{u_1,l_1}(s_1), \pi^{(2)}_{u_2,l_2}(s_2)\right)\right]$$

On the other hand, e_i give rise to edges $(u_i, s_i) \xrightarrow{l_i \quad r_i} \left(v_i, \pi^{(i)}_{u_i,l_i} s_i\right) \in E(G_i)$ in the respective lifts. These combine to give an edge

$$[(u_1, s_1), (u_2, s_2)] \xrightarrow{(l_1,l_2) \quad (r_1,r_2)} \left[\left(v_1, \pi^{(1)}_{u_1,l_1} s_1\right), \left(v_2, \pi^{(2)}_{u_2,l_2} s_2\right)\right] \in E(G_1 \otimes G_2)$$

We see that this is the same rotation map as that of the $S_1 \times S_2$ lift we defined – only the order in which we give the coordinates of a vertex are different. The covering map is obtained by mapping $[(u_1, s_1), (u_2, s_2)]$ down to (u_1, u_2), and so on.

Finally, compatibility with undirected digraphs is a straightforward exercise; the key is that the inverse of the product permutation is the component-wise inverse. □

Remark 4.20. Notice that this covering map is *not* exactly of the form $p : G \to H$ where $V(G) = V(H) \times S$: the two lift coordinates s_1 and s_2 are 'split'. But it is *equivalent* to such a covering map up to a natural isomorphism of the vertex set of $G_1 \otimes G_2$ – namely, the one that permutes the factors of $V(H_1) \times S_1 \times V(H_2) \times S_2$ to get to $V(H_1) \times V(H_2) \times S_1 \times S_2$. This will happen again in our next proofs.

Proposition 4.19 seems to be a fairly general statement, and it's worth considering several special cases. For example, it's easy to check that we obtain a well-known result about Cayley/Schreier graphs as a special case when the coverings p_1, p_2 are of bouquets, as in Examples 3.2, 3.5:

Corollary 4.21. *We have* $\mathrm{Cay}(\mathcal{G}_1, S_1) \otimes \mathrm{Cay}(\mathcal{G}_2, S_2) = \mathrm{Cay}(\mathcal{G}_1 \times \mathcal{G}_2, S_1 \times S_2)$*, and more generally* $\mathrm{Sch}(\mathcal{G}_1, A_1, S_1) \otimes \mathrm{Sch}(\mathcal{G}_2, A_2, S_2) = \mathrm{Sch}(\mathcal{G}_1 \times \mathcal{G}_2, A_1 \times A_2, S_1 \times S_2)$ *where the action of* $\mathcal{G}_1 \times \mathcal{G}_2$ *on* $A_1 \times A_2$ *is the product action* $(g_1, g_2)(a_1, a_2) = (g_1 a_1, g_2 a_2)$.

Another special case is obtained by using a trivial covering for p_2:

Corollary 4.22. *If* $p : G \to H$ *is a labeled covering of* S*-regular digraphs, and* K *is any digraph, there is an induced covering map* $q : G \otimes K \to H \otimes K$.

Then making the graph K from the latter Corollary a bouquet we recover another familiar operation:

Definition 4.23. For a digraph G with a two-way labeling and a number d, define the **edge duplicated graph** dG to be the two-way labeled digraph obtained from G by duplicating every edge d times, so that the d copies of an edge $u \xrightarrow{i \quad j} v$ are labeled as $u \xrightarrow{(i,k) \quad (j,k)} v$ for k ranging over $\{1, \ldots, d\}$.

The effect on the adjacency matrix of G is multiplication by d: $A_{dG} = dA_G$, hence $\lambda(dG) = \lambda(G)$. It's easy to see that edge duplication is compatible with covering:

Corollary 4.24. *If* $p : G \to H$ *is a labeled covering of regular digraphs, and* B_d *is the bouquet of* d *loops where the head and tail of the* i*-th loop is labeled by* i*, we have a labeled covering* $q : G \otimes B_d = dG \to dH = H \otimes B_d$.

4.4. The backward-forward square and undirecting

Here we define two natural graph operations that allow us to translate results about directed expanders to results about undirected ones in a way compatible with covering maps. Given G, our first operation is given by simply superimposing G with the graph obtained from G by reversing all edges, following Ben-Aroya and Ta-Shma [**BATS11**]; this has a natural structure of an undirected digraph. Our second operation is like the square, but instead of two forward steps we do a *backward step followed by a forward step*; the motivation is that the adjacency matrix will be $A_G^T A_G$, which is symmetric and naturally related to $\lambda(G)$ by Proposition 2.18. Thus the effect on expansion is like squaring, with the additional benefit that we get undirected graphs! We will use this *backward-forward square* to give a directed analogue of the Alon-Boppana Theorem 2.24, and to get undirected expanding towers from directed ones.

4.4.1. Definition and expansion properties.

Definition 4.25. For a D-regular digraph G, the **undirection** of G is the $D \times \{-1, 1\}$-regular undirected digraph $G^\dagger$ with an opposite pair of edges $u \xrightarrow{(i,1)\quad(j,1)} v, v \xrightarrow{(j,-1)\quad(i,-1)} u \in E(G^\dagger)$ for every edge $u \xrightarrow{i\quad j} v \in E(G)$. The **backward-forward square** of G, denoted G^TG, is the D^2-regular digraph with vertex set $V(G)$, and rotation map

$$\mathrm{Rot}_{G^TG}[v, (i', j)] = [w, (j', i)]$$

whenever we have the following edges:

$$u \xrightarrow{i\quad i'} v \in E(G),\ u \xrightarrow{j\quad j'} w \in E(G).$$

As promised, we have[2]

Proposition 4.26. *For any D-regular two-way labeled digraph G, $G^\dagger$ is an* undirected $D \times \{-1, 1\}$-*regular digraph that inherits an* undirected *two-way labeling, has adjacency matrix $A_G + A_G^T$, and $\lambda(G^\dagger) \leq \lambda(G)$. Similarly, G^TG is an* undirected D^2*-regular digraph that inherits an* undirected *two-way labeling, has adjacency matrix $A_G^T A_G$, and $\lambda(G^TG) = \lambda(G)^2$.*

Proof. For the undirection, everything is obvious except spectral expansion; for this observe that since $G^\dagger$ is $2|D|$-regular, $W_{G^\dagger} = 1/2(W_G + W_G^T)$. Then for any $x \perp u_G$, we have $\|W_{G^\dagger}x\| \leq 1/2(\|W_Gx\| + \|W_G^Tx\|) \leq 1/2(\lambda(G) + \lambda(G)) = \lambda(G)$, as singular values are invariant under transposition. Next, by the definition of the backward-forward square, for an edge $v \xrightarrow{(i',j)\quad(j',i)} w \in E(G^TG)$, we also have an edge $w \xrightarrow{(j',i)\quad(i',j)} v$, and it's natural to pair these two to give G^TG the structure of an undirected digraph. As the labels of the two edges at both v and w match, and moreover any loop this is an undirected two-way labeling. Next, we count

$$(A_{G^TG})_{vw} = \sum_{u \in V(G)} (A_G)_{uv}(A_G)_{uw} = \sum_{u \in V(G)} (A_G^T)_{vu}(A_G)_{uw} = (A_G^TA_G)_{vw}$$

By regularity, this means $W_{G^TG} = W_G^TW_G$. As we saw in **??**, $\lambda(G)$ is the second singular value of W_G, which is exactly the square root of the second eigenvalue of $W_G^TW_G$, and we're done. □

Corollary 4.27 (Lower bounds on $\lambda(G)$ for directed graphs). *Given a family of d-regular digraphs $G_1, G_2, \ldots$ with $|V(G_n)| \to \infty$, $\lambda(G_n) \geq \sqrt{2}\sqrt{d-1}/d - o_n(1)$.*

To see this, just apply Theorem 2.24 to $G_1^TG_1, G_2^TG_2, \ldots$, or $G_1^\dagger, G_2^\dagger, \ldots$

4.4.2. Lifting properties.

Proposition 4.28. *Suppose $p : G \to H$ is a labeled S-covering of D-regular digraphs. Then there are natural labeled covering maps $q : G^TG \to H^TH, r : G^\dagger \to H^\dagger$ of* undirected *digraphs.*

Proof. Let's have an edge $v \xrightarrow{(i',j)\quad(j',i)} w \in E(H^TH)$ coming from the two edges

$$u \xrightarrow{i\quad i'} v \in E(H),\ u \xrightarrow{j\quad j'} w \in E(H)$$

For any $s \in S$, these two define edges in the lift:

$$(u, s) \xrightarrow{i\quad i'} (v, \pi_{u,i}s) \in E(G),\ (u, s) \xrightarrow{j\quad j'} (w, \pi_{u,j}s) \in E(G)$$

[2]It transpired after submission of this thesis that compatibility with lifts fails for the backward-forwards square because we weren't careful enough with loops; it turns out that our correspondence between undirected graphs and digraphs has to allocate pairs of opposite edges for loops as well! After this change, the proposition still works for undirecting under a slight change in the definition of the rotation map.

which in turn mean we have the edge $(v, \pi_{u,i}s) \xrightarrow{(i',j)\quad(j',i)} (w, \pi_{u,j}s) \in E(G^TG)$. Relabeling S according to $\pi_{u,i}^{-1}$, this gives

$$\forall s \in S : (v, s) \xrightarrow{(i',j)\quad(j',i)} \left(w, \pi_{u,j}\pi_{u,i}^{-1}s\right) \in E(G^TG)$$

and hence G^TG is the lift of H^TH where the (i', j)-th edge out of (v, s) is assigned the permutation $\pi_{u,j}\pi_{u,i}^{-1}$. The permutation assigned to the reverse edge $w \xrightarrow{(j',i)\quad(i',j)} v$ is then $\pi_{u,i}\pi_{u,j}^{-1} = (\pi_{u,j}\pi_{u,i}^{-1})^{-1}$; thus, pairs of opposite edges in H^TH lift to pairs of opposite edges in G^TG, as we wanted. The verification for the undirection follows an analogous idea. □

4.5. Zig-zag product and generalized zig-zag product

The zig-zag product of Reingold, Vadhan and Wigderson [**RVW02**] marks a turning point in the work on explicit constructions of expanders, as it demonstrated how to construct good expander families by an elementary and intuitive combinatorial argument.

4.5.1. Definition and expansion properties.

Definition 4.29. For two-way labeled regular digraphs G and H with G a $V(H)$-regular digraph and H a D-regular digraph, the **zig-zag product** $G ⓩ H$ is the D^2-regular graph with vertex set $V(G) \times V(H)$ and rotation map

$$\mathrm{Rot}_{G ⓩ H}[(v, k), (i, j)] = [(w, l), (j', i')]$$

whenever we have the following edges:

$$k \xrightarrow{i\quad i'} k' \in E(H), \quad v \xrightarrow{k'\quad l'} w \in E(G), \quad l' \xrightarrow{j\quad j'} l \in E(H)$$

This seems very complicated! Here's an intuitive idea: let's think of the set $V(G) \times V(H)$ as a version of $V(G)$ where every vertex was blown up to a *cloud* in bijection with $V(H)$. Starting at the $k \in V(H)$-th vertex of the cloud of $v \in V(G)$, a single step under the label (i, j) in the zig-zag product can be thought of as:

- a step *within* the v-cloud following label i, arriving at the k'-th vertex in the cloud;
- a step *between* clouds, guided by k' interpreted as an edge label in G, to the w cloud. The in-label l' of the $v \to w$ edge tells us at which vertex of the w cloud we land;
- a step *within* the w-cloud following label j.

Example 4.30. It will be convenient to keep some (half-)trivial examples in mind. Consider the zig-zag product $B_S ⓩ K$ of a bouquet of circles B_S on one vertex $*$ with any $|S|$-regular digraph K, and suppose that B_S is consistently labeled. We can ignore the $*$ and think of it as a graph on the set $V(H)$. To determine $\mathrm{Rot}_{B_S ⓩ K}[k, (i, j)]$, we look at the edges

$$k \xrightarrow{i\quad i'} k' \in E(K), \ * \xrightarrow{k'\quad k'} * \in E(B_S), \ k' \xrightarrow{j\quad j'} l \in E(K)$$

and conclude that the result is $[l, (j', i')]$, hence $B_S ⓩ K = K^2$.

The amazing thing about the zig-zag product is that it essentially inherits spectral expansion from both G and H, but degree only from H! This is the what makes the zig-zag product so successful in the spectral setting. Amazingly, the proof of the following Theorem uses only basic linear algebra!

Theorem 4.31 (Vadhan [**Vad12**]; Reingold-Vadhan-Wigderson [**RVW02**]). *If G is an (n, m, λ_G)-digraph and H is an (m, d, λ_H)-digraph, then for* any *two-way labeling of G and H, $G ⓩ H$ is an $(nm, d^2, \lambda_G + 2\lambda_H)$-digraph; furthermore, if G and H are undirected, $G ⓩ H$ is an undirected $(nm, d^2, \lambda_G + \lambda_H)$-digraph.*

This was used by Reingold, Vadhan and Wigderson in [**RVW02**] to give an elementary, combinatorial fully-explicit construction of expanders by an iterative process. The considerations behind this construction will be important for us later on, when we make constructions of expanding towers based on these ideas.

Example 4.32 (Fully explicit expanders from the zig-zag product). Intuitively, we want to start with some good expander, and perform a sequence of operations (one of them being the zig-zag product) that gives us back a bigger graph with bounded expansion and the same degree.

One idea is to start with H being a (d^4, d, λ)-digraph, and inductively define

$$G_{n+1} = G_n^2 ⓩ H,\ G_1 = H^2$$

Then it's easy to see that G_n has d^{4n} vertices, and as long as λ is a small enough constant (which is achievable by, say, brute-force search), $(G_n)_{n\in\mathbb{N}}$ will be an expander family of d^2-regular graphs. However, here we only get mild explicitness; the reason is that to evaluate the rotation map of G_{n+1}, we need to make two calls to the rotation map of H, but also *two* calls to the rotation map of G_n. Since the depth of the recursion is n, this leads to exponentially many in $n = O(\log(d^{4n}))$ queries at the bottom!

To remedy this, Reingold, Vadhan and Wigderson used the following trick to make the recursion shallower: for H a (d^8, d, λ)-digraph, let $G_1 = H^2, G_2 = H \otimes H$, and then

$$G_{n+1} = \left(G_{\lceil \frac{n}{2} \rceil} \otimes G_{\lfloor \frac{n}{2} \rfloor}\right)^2 ⓩ H$$

Then G_n will be a d^2-regular digraph on d^{8n} vertices with bounded expansion if λ is small. But the time $T(n)$ to compute a rotation map in G_n is now about $T(n) \approx 4T(n/2) + c$, because we need two rotations from $G_{\lceil \frac{n}{2} \rceil}$, two rotations from $G_{\lfloor \frac{n}{2} \rfloor}$, and two rotations from H. The recursion solves to a polynomial in $n = O(\log(d^{8n}))$.

We remark that constructions based on the zig-zag product can achieve $\lambda = O(d^{3/4}/d)$ (and $O(d^{2/3}/d)$ with some extra work), which is better than constant, but still not as good as Ramanujan graphs.

4.5.2. Relationship to the semidirect product. Alon, Lubotzky and Wigderson [**ALW01**] found that, somewhat surprisingly, the zigzag product of Cayley graphs is a Cayley graph of the semidirect product with a suitable choice of generators:

Fact 4.33 (Zig-zag product and semidirect product). *For groups $\mathcal{G}$ and $\mathcal{H}$ with $\mathcal{H}$ acting on $\mathcal{G}$, $\mathrm{Cay}(\mathcal{G}, S)ⓩ \mathrm{Cay}(\mathcal{H}, T)$ is a Cayley graph $\mathrm{Cay}(\mathcal{G} \rtimes \mathcal{H}, U)$ of the semidirect product when the generating sets S and T are chosen suitably; for example, when S is a single T-orbit.*

This is suspiciously similar to the wreath products from Chapter 3. It is natural to ask if this can be used as a basis for a construction of expanding towers, and indeed, we shall see in Subsection 5.1.1 how this idea was used by Rozenman, Shalev and Wigderson to construct expanding towers via the relationship between coverings and the wreath product!

Another reason this is intriguing is that it feels very similar to Corollary 4.21; so there are reasons to believe that Fact 4.33 can be a special instance of a much more general phenomenon. Thus, an immediate question for future work is the following:

Question 4.34. How do we generalize Fact 4.33 in the same way that Proposition 4.19 generalizes Corollary 4.21?

4.5.3. Lifting properties. It turns out that there is a simpler relationship between zig-zag products and coverings that is somewhat surprising: given a labeled covering $G \to H$, we get a labeled covering $Gⓩ K \to Hⓩ K$. Intuitively, one reason for that is that every edge in $Hⓩ K$ comes from a unique edge in H (the edge between clouds). Using the permutation on this edge induced by the covering map $G \to H$, we can define a lift of $Hⓩ K$; this lift turns out to be naturally isomorphic to $Gⓩ K$!

Proposition 4.35. *Suppose $p : G \to H$ is a labeled S-covering of D-regular two-way labeled digraphs, and K is a two-way labeled digraph with vertex set D. Then there is a natural labeled covering map $q : G ⓩ K \to H ⓩ K$. Moreover, if p is a covering of undirected digraphs and K is undirected, q is also a covering of undirected digraphs.*

Proof. First observe that the degrees make sense: both G and H have labels in bijection with D, which is exactly the vertex set of K. Next, let's have an edge $(v,k) \xrightarrow{(i,j)\quad(j',i')} (w,l) \in E(H ⓩ K)$ coming from the three edges

$$k \xrightarrow{i\quad i'} k' \in E(K), \quad v \xrightarrow{k'\quad l'} w \in E(H), \quad l' \xrightarrow{j\quad j'} l \in E(K)$$

For every $s \in S$, the edge $v \xrightarrow{k'\quad l'} w \in E(H)$ gives rise to an edge $(v,s) \xrightarrow{k'\quad l'} (w, \pi_{v,k'}s) \in E(G)$. Substituting this for the middle edge in the above triple gives us a new triple which means we have an edge

$$[(v,s),k] \xrightarrow{(i,j)\quad(j',i')} [(w,\pi_{v,k'}s),l] \in E(G ⓩ K)$$

Notice that, since k' and thus $\pi_{v,k'}$ is determined uniquely by $[(v,k),(i,j)]$, the above encodes exactly the rotation map of the lift of $H ⓩ K$ where the permutation on the (i,j)-th edge out of (v,k) is $\pi_{v,k'}$. In the undirected case, the opposite edge lifts via $\pi_{w,l'} = \pi_{v,k'}^{-1}$ since the covering is undirected, hence q is also a covering of undirected graphs. Once again, keep in mind Remark 4.20 that the lift coordinate doesn't come last! □

This feels somewhat mysterious, even after we've seen the proof. It's worth contemplating it some more. The key reason it works is that, in the way an edge in the zig-zag product $H ⓩ K$ is defined using two edges from K and one edge from H, there is certain independence between the labels on the edges of H and the names of vertices of H. The latter labels are the important thing, since they determine the 'jump' we take in K; the niceness of lifting comes exactly from being able to lift the middle edge to a lift G of H, which changes the *names* of the vertices of H by adding a lift coordinate, but *preserves* the labels k', l' on the edge.

4.5.4. The generalized zig-zag product of Ben-Aroya and Ta-Shma. It is natural to ask what the limits of the idea behind the zig-zag product are. Ben-Aroya and Ta-Shma gave a partial answer in [**BATS11**], which achieves fully explicit expanders with $\lambda(G_n) = d^{-1/2+o(1)}$. This is pretty close to Ramanujan! The product is more involved, and in this section we state its definition and expansion properties, and show that it also respects coverings!

We say that a two-way labeled D-regular digraph G is **locally invertible** if its rotation map is of the form $\mathrm{Rot}_G(v,i) = (w, \pi(i))$ for a *fixed* permutation $\pi : D \to D$; for example, a consistently labeled digraph is locally invertible with $\pi = \mathrm{id}$. Later on, we will need the following easy fact:

Fact 4.36. *If G_1, G_2 are locally invertible, then so are $G_1^k, G_1 \otimes G_2, G_1^\dagger$; moreover, for a labeled covering $(G; l_G) \to (H; l_H)$ and H locally invertible with respect to l_H, G is locally invertible with respect to l_G.*

Having defined local invertibility, we can define the *generalized zig-zag product*:

Definition 4.37 (Generalized zig-zag product). Let G be a D_1-regular *locally invertible* digraph on vertex set V_1, and let $\overline{H} = (H_1, \dots, H_k)$ be a sequence of D_2-regular *undirected locally invertible* digraphs, each on vertex set V_2, where $V_2 = D_1^{4k}$. Let $\pi_i : V_2 \to D_1$ be the projection to the i-th coordinate. Then the zig-zag product $G ⓩ \overline{H}$ is a D_2^k-regular graph on vertex set $V_1 \times V_2$ defined by the following rotation map:

$$\left(v_0^{(1)}, v_0^{(2)}\right) \xrightarrow{(i_1,\dots,i_k)\quad(i_k',\dots,i_1')} \left(v_{2k-1}^{(1)}, v_{2k-1}^{(2)}\right) \in E(G ⓩ \overline{H})$$

whenever we have the following sequence of edges, for $j = 1, 2, \dots, 2k-1$:

$$v_{j-1}^{(1)} = v_j^{(1)} \text{ and } v_{j-1}^{(2)} \xrightarrow{i_t \quad i'_t} v_j^{(2)} \in E(H_t) \text{ whenever } j = 1 \pmod 2 \text{ where } t = (j+1)/2$$
$$v_{j-1}^{(1)} \xrightarrow{\pi_1\left(v_{j-1}^{(2)}\right) \quad \pi_1\left(v_j^{(2)}\right)} v_j^{(1)} \in E(G) \text{ whenever } j = 0 \pmod 2, \text{ and}$$
$$v_j^{(2)} \text{ is additionally determined by } \pi_i(v_j^{(2)}) = \pi_i(v_{j-1}^{(2)}) \text{ for all } 1 < i \leq 4k$$

As Ben-Aroya and Ta-Shma show, $G\textcircled{z}\overline{H}$ will also be locally invertible – but it is possibly a directed graph, since H_k might be different from H_1! Guaranteeing expansion is not that straightforward anymore: it relies on a probabilistic argument for the existence of a *good* $\overline{H}$. Fortunately, it can be shown that a good $\overline{H}$ exists for *all* D_1-regular locally invertible graphs G! This was noticed by the anonymous referee of [**BATS11**], and will be important for us in Subsection 5.1.5[3] With this, we have

Theorem 4.38 (Theorem 2 and Theorem 7 from Ben-Aroya and Ta-Shma [**BATS11**]). *Suppose G is a locally invertible (V_1, D_1, λ_1)-digraph, and $\overline{H} = (H_1, \dots, H_k)$ a sequence of undirected $(V_2 = D_1^{4k}, D_2, \lambda_2)$-digraphs that is ε-good with respect to every D_1-regular graph and satisfies $\lambda_2 \leq 1/2$. Then $G\textcircled{z}\overline{H}$ is an $(V_1 \times V_2, D_2^k, \lambda_2^{k-1} + 2(\varepsilon + \lambda_1) + \lambda_2^k)$-digraph. Moreover, for large enough D_1 and D_2, ε-good $\overline{H}$ exist with $\varepsilon = D_2^{-k}$ and $\lambda_2 = 2\sqrt{|D_2| - 1}/|D_2| + \varepsilon$.*

Finally, we arrive at the lifting property for the generalized zig-zag product; the philosophy behind why it works turns out to be the same as for the ordinary zig-zag product.

Proposition 4.39. *Suppose $p : K \to G$ is a labeled S-covering of D_1-regular locally invertible graphs, G has vertex set V_1, and $\overline{H} = (H_1, \dots, H_k)$ is a sequence of D_2-regular locally invertible undirected digraphs, each on vertex set $V_2 = D_1^{4k}$. Then there is a natural labeled covering map $q : K\textcircled{z}\overline{H} \to G\textcircled{z}\overline{H}$.*

Proof. First, clearly the zig-zag products can be taken, and both result in D_2^k-regular graphs. Next, suppose we have an edge $\left(v_0^{(1)}, v_0^{(2)}\right) \xrightarrow{(i_1,\dots,i_k) \quad (i'_k,\dots,i'_1)} \left(v_{2k-1}^{(1)}, v_{2k-1}^{(2)}\right) \in E(G\textcircled{z}\overline{H})$ arising from edges in G and $\overline{H}$ as in the definition above. Then the edges in G give rise to edges in the lift:

$$\forall s \in S, j \equiv 0 \pmod 2 : (v_{j-1}^{(1)}, s) \xrightarrow{\pi_1\left(v_{j-1}^{(2)}\right) \quad \pi_1\left(v_j^{(2)}\right)} \left(v_j^{(1)}, \pi_{v_{j-1}^{(1)}, \pi_1\left(v_{j-1}^{(2)}\right)} s\right) \in E(K)$$

and in particular, letting $\mu_{j-1} = \pi_{v_{j-1}^{(1)}, \pi_1\left(v_{j-1}^{(2)}\right)}$ whenever j is even and choosing the values for s inductively, we have (with the convention $\mu_{-1} = \mathrm{id}$)

$$\forall s \in S, j \equiv 0 \pmod 2 : (v_{j-1}^{(1)}, \mu_{j-3} \dots \mu_1 s) \xrightarrow{\pi_1\left(v_{j-1}^{(2)}\right) \quad \pi_1\left(v_j^{(2)}\right)} \left(v_j^{(1)}, \mu_{j-1}\mu_{j-3} \dots \mu_1 s\right) \in E(K)$$

Combining these edges with the edges from $\overline{H}$, we get the existence of an edge

$$\forall s \in S : (v_0^{(1)}, s, v_0^{(2)}) \xrightarrow{(i_1,\dots,i_k) \quad (i'_k,\dots,i'_1)} (v_{2k-1}^{(1)}, \mu_{2k-1} \dots \mu_1 s, v_{2k-1}^{(2)}) \in E(K\textcircled{z}\overline{H})$$

As usual, since the permutations μ_i are completely determined by $v_0^{(1)}, v_0^{(2)}$ and $(i_1, \dots, i_t)$, this encodes the rotation map of a cover of $G\textcircled{z}\overline{H}$ such that the covering map respects the labels. □

4.6. Derandomized squaring

4.6.1. Definition and expansion properties. The derandomized square is a close cousin of the zig-zag product, and is also a sort of derandomized graph product: for a d-regular digraph G, the derandomized square of G has degree linear in d, but spectral expansion only slightly worse than the expansion of G^2 (hence the name)!

[3] Thus, I'd like to thank the anonymous referee, whoever they are! :)

Definition 4.40. For two-way labeled digraphs G and H with G a $V(H)$-regular graph and H a T-regular graph, the **derandomized square** $G Ⓢ H$ of G with respect to H is the $V(H) \times D$-regular graph with vertex set $V(G)$ and rotation map

$$\mathrm{Rot}_{G Ⓢ H}[v, (k, i)] = [w, (k', i')]$$

when we have the following edges:

$$v \xrightarrow{k \quad l} u \in E(G),\ l \xrightarrow{i \quad i'} l' \in E(H),\ u \xrightarrow{l' \quad k'} w \in E(G)$$

As with the zig-zag product, this is somewhat complicated. The intuition is that we first take a step in G freely, but the next step is *restricted* by the small graph H. And here is the promised spectral expansion bound:

Theorem 4.41 (Rozenman and Vadhan, [**RV05**]). *If G is an (n, m, λ)-digraph and H is an (m, d, μ)-digraph, then for any choice of two-way labelings, $G Ⓢ H$ is a $(n, md, \lambda^2 + \mu)$-digraph.*

4.6.2. Lifting properties. The derandomized square enjoys a lifting property analogous to the one for the zig-zag product; it is similarly somewhat mysterious, but it works for the same reason the zig-zag one worked. The proof is very similar, so it's deferred to the appendix: see Proposition A.2.

Proposition 4.42. *Suppose $p : G \to H$ is a labeled S-covering of T-regular two-way labeled digraphs, and K is a two-way labeled digraph on vertex set T. Then there is a natural labeled covering map $q : G Ⓢ K \to H Ⓢ K$.*

4.7. Categories?

In this section, which can be skipped in a first reading, we remark that a simple way to state most of the results in this chapter is via *category theory*. The language of categories allows us to formulate and think about the results in this chapter in a clearer way, and points us to possible generalizations.

Category theory is a sort of metamathematics that studies common patters in mathematical structures; for example, algebraic topology – which is where category theory originated – is based on common patterns in the world of topological spaces and groups. Category theory provides us, via *functors* and *natural transformations*, with a way to *translate* the world of topological spaces to that of groups in a highly consistent manner. The benefit is that the world of algebra seems to be easier to understand than that of topology, and this approach has been very successful in giving us topological - and sometimes algebraic - insights. Beyond that, category theory helps us generalize various concepts in mathematics, and give a common perspective on many of them; we refer the interested reader to the classical book by Mac Lane [**ML71**]; here we only scratch the surface.

Definition 4.43. A **category** C is a collection[4] of *objects* $\mathrm{ob}\, C$ and a collection of *morphisms* $\hom C$, such that every morphism $f \in \hom C$ has a **source** $X \in \mathrm{ob}\, C$ and **target** $Y \in \mathrm{ob}\, C$, denoted as $f : X \to Y$. Moreover, every object X has a designated **identity morphism** id_X, and for any two morphisms $f : X \to Y, g : Y \to Z$, there is a composite morphism $g \circ f : X \to Z$. Furthermore, we require that:

- For any $f : X \to Y$, $f\, \mathrm{id}_X = f = \mathrm{id}_Y f$;
- For any $f : X \to Y, g : Y \to Z, h : Z \to T$, we have $h \circ (g \circ f) = (h \circ g) \circ f$.

Example 4.44. Topological spaces with morphisms being continuous maps form the category Spaces; groups with morphisms being group homomorphisms form Groups; sets with morphisms being total functions form Sets, ...

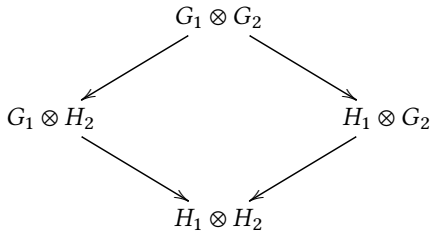
[4] We run into set-theoretic issues if we use 'set' instead of collection, because we want to talk about e.g. the category of sets, which cannot be a set because of Russell's paradox. But don't worry, because "...the whole concept of a category is essentially an auxiliary one; our basic concepts are essentially those of a functor and of a natural transformation . ...The idea of a category is required only by the precept that every function should have a definite class as domain and a definite class as range, for the categories are provided as the domains and ranges of functors."[**EM45**]

This will be the important example for us:

Example 4.45. The collection of all (not necessarily finite) S-regular *two-way labeled* digraphs for S a finite set can be given the structure of a category $\textsc{Graphs}_S$ by taking the morphisms to be labeled covering maps; as we've seen, they compose nicely, and the identity is just the identity covering map.

We stress that in this section, all our digraphs will be objects of such categories, and thus carry implicit two-way labelings! Also, the condition of a labeled covering is very strong: if $p : G \to H$ is a labeled covering of weakly connected digraphs, it's easy to see that knowing the image of one vertex of G in H forces the rest of the covering.

Interesting statements about categories are often represented by *commutative diagrams*, which are diagrams of objects and morphisms such that, whenever there are two different ways to follow the morphisms from one object to another, the composite morphisms are equal. For example, suppose we have morphisms $p_1 : G_1 \to H_1$ in $\textsc{Graphs}_S$ and $p_2 : G_2 \to H_2$ in $\textsc{Graphs}_T$. Then, by applying Proposition 4.19 several times and using the identity coverings, it can be seen that we get a commutative diagram



in $\textsc{Graphs}_{S\times T}$.

Almost all of the results from this chapter can be stated in terms of *functors* between some two categories $\textsc{Graphs}_S$ and $\textsc{Graphs}_T$. A functor can be thought of as a way to translate commutative diagrams from one category to another:

Definition 4.46. A **functor** $F : \mathcal{C} \to \mathcal{D}$ between two categories consists of an object $FX \in \operatorname{ob}\mathcal{D}$ for each object $X \in \operatorname{ob}\mathcal{C}$, and a morphism $Ff : FX \to FY$ for each morphism $f : X \to Y$ in $\mathcal{C}$, such that

- $F\operatorname{id}_X = \operatorname{id} FX$ for every object X in $\mathcal{C}$;
- whenever we have $f : X \to Y, g : Y \to Z$ in $\mathcal{C}$, $F(g \circ f) = Fg \circ Ff$.

So, for example, the following requires a closer look at the proof of Proposition 4.35, but no new ideas; we defer the proof to Proposition A.1.

Proposition 4.47. *Given a D-regular graph K on vertex set S, define the following correspondence between objects and morphisms of $\textsc{Graphs}_S$ to objects and morphisms of $\textsc{Graphs}_{T\times T}$:*

$$G \mapsto G ⓩ K, \quad (p : G \to H) \mapsto (q : G ⓩ K \to H ⓩ K) \text{ given by Proposition 4.35}$$

Then this defines a functor $\textsc{Graphs}_S \to \textsc{Graphs}_{T\times T}$.

Somewhat related to this line of reasoning, a categorical approach to graphs was taken by Cooper, Dotterer, and Prassidis in [**CDP06**] to vastly generalize the zig-zag product (though its expansion properties don't generalize), and show (like we did in Proposition 4.35 for the ordinary zig-zag product) that it preserves covering maps – though they didn't explicitly describe this property as a functor.

It would be interesting to see if the formalism of categories can help us come up with more general statements than the ones in this chapter! For example, it would be interesting to see if we can say something nice about the *limit* (in the categorical sense) of a tower of labeled coverings, which is intuitively the 'smallest' graph that covers all graphs in the tower compatibly with the covering maps in the tower.

CHAPTER 5

Applications

In this chapter, we bring together the theory developed in Chapters 3 and 4, and apply it in several contexts.

5.1. A technique for elementary explicit constructions of expanding towers

In the world of elementary explicit constructions of expander towers, there have been two major results, by Bilu and Linial [**BL06**] and Rozenman, Shalev and Wigderson [**RSW06**]. The first paper showed that any simple, undirected d-regular graph has a 2-lift where all new eigenvalues are bounded by $O(\log^{3/2}/d^{1/2})$; the construction is only mildly explicit - the 2-lift can be computed in time polynomial in the size of the base graph.

In the second paper, Rozenman, Shalev and Wigderson gave an elementary, iterative explicit construction of Cayley expanders for iterated wreath products of alternating groups $\wr_i \mathrm{Alt}(n)$ for n large enough. The key ingredient for expansion was the group-theoretic interpretation of the zig-zag product (Fact 4.33); the key ingredient for explicitness was an algorithmic version of the fact that every element of $\wr_i \mathrm{Alt}(d)$ is a commutator [**Nik04**], which allows efficient computation in iterated wreath products.

In the same paper, they gave an elementary iterative fully-explicit construction of an expanding tower of Schreier graphs for iterated wreath products $(\wr_{i=1}^{n} K)_{n\in\mathbb{N}}$ given a Schreier graph of K with $\lambda < 1/4$. The expansion is constant, but can be brought down to $O(d^{3/4}/d)$ with the appropriate base case. Again, the key step for expansion is the zig-zag product, and explicitness relies on the commutator property. It is interesting that they arrived at the wreath product not from the direction of lifts, as we did!

Abstractly, the proof works by starting with a base graph $G = K^4$, and then performing the sequence of operations $G \mapsto tG \mapsto (tG)ⓩK \mapsto ((tG)ⓩK)^2$ for appropriate t (recall the notation from Corollary 4.24). The latter graph turns out to be a lift of G (*what did just happen?!*), and then everything is repeated with this lift.

This feels very magical, precisely because we somehow get that lift out of 'nothing'. Perhaps part of the mystery is that there are two general ideas that heavily interact behind the scenes - one is that the voltage groups of towers are iterated wreath products (Proposition 3.28), and the other is the generalization of the construction that we will describe later (Proposition 5.2), which makes no explicit reference to the group structure (but the structure is implicitly still there). It seems that separating these two ideas is part of what allows us to give a simpler account of the construction and generalize it.

5.1.1. The Rosenman-Shalev-Wigderson expanding tower. But first, let's describe the construction. Keep in mind that in the original it uses *undirected Schreier graphs*, but of course everything can be translated to undirected Schreier digraphs as we discussed in Subsection 2.3.1. Here's the statement, and a sketch of the proof:

Theorem 5.1 (Rosenman-Shalev-Wigderson [**RSW06**]). *Let E_n be the set of leaves at distance n from the root in the infinite rooted tree T_d were every node has d children, $K_1 \subset \mathrm{Sym}(E_1)$ and $K_n = \wr_{i=1}^{n} K_1$. If there is a generating set Q_1 of K_1 with $\lambda(K_1, E_1, Q_1) \leq 1/4$ and $|Q_1| \leq d^{1/4}/2$, there exist generating sets $Q_n \subset K_n$ such that $|Q_n| = |Q|^4$, $\lambda(K_n, E_n, Q_n) \leq 1/4$, and Q_n can be computed in time* $\mathrm{polylog}(|E_n|)$.

Proof sketch. Assume $|Q|^4$ divides d - this makes the proof much simpler to explain, but is not essential. We will proceed by induction; the first graph is $G_1 = \mathrm{Sch}(K_1, E_1, Q^4)$. Now assume we have $G_n = \mathrm{Sch}(K_n, E_n, Q_n)$ with $\lambda(G_n) \leq 1/4$. Then we perform the following sequence of operations on G_n:

(1) Let $\underline{x}$ be an element of $Q_n^{E_1}$ where each element of Q_n appears exactly $d/|Q|^4$ times. Using the inclusions $K \hookrightarrow K_{n+1}$ and $K_n^d \hookrightarrow K_{n+1}$ (remember Example 3.26), define the set $U_{n+1} = \left\{ y\underline{x}z \;\middle|\; y, z \in Q \right\} \subset K_{n+1}$. Let $\widetilde{Q}_n$ be the multiset obtained by the list of elements of $\underline{x}$; then we can consider $G'_n = \mathrm{Sch}(K_n, E_n, \widetilde{Q}_n)$, which is just G_n with every edge duplicated $d/|Q|^4$ times.
(2) Since $\underline{x}$ gives us a map from elements of E_1 to elements of $\widetilde{Q}_n$, which in turn are the labels of edges of G'_n, we have a well-defined zig-zag product $G''_n = G'_n ⓩ \mathrm{Sch}(K_1, E_1, Q)$. It turns out that $G''_n = \mathrm{Sch}(K_{n+1}, E_{n+1}, U_{n+1})$, because of our choice of U_{n+1} and by analogy with Fact 4.33; the proof is a simple application of the definition of the zig-zag product.
(3) Let $G_{n+1} = (G''_n)^2$., i.e. $Q_{n+1} = U_{n+1}^2$. It turns out that G_{n+1} is a cover of G_n. This follows because the set Q_{n+1} is *consistent* with the set Q_n, in the sense that the restriction homomorphism $K_{n+1} \to K_n$ maps Q_{n+1} to Q_n as multisets. The intuition behind that is that we can associate a word of length 4 in Q to every generator in Q_n. For $Q_1 = Q^4$, this is done in the obvious way; for higher Q_n, this can be shown by induction, using the fact that $Q_{n+1} = U_{n+1}^2 = \left\{ y\underline{x}zy'\underline{x}z' \;\middle|\; y, z, y', z' \in Q \right\}$, so that we can associate $y\underline{x}zy'\underline{x}z'$ to $yzy'z' \in Q^4$; as a sanity check, one easily sees that since $\underline{x}$ is embedded in the n bottom levels of the tree with leaves E_{n+1}, it doesn't affect multiplication on the first level, so the restriction homomorphism to the first level sends $y\underline{x}zy'\underline{x}z'$ to $yzy'z'$.

    The explicitness comes from the algorithmic version of the *commutator property*, which guarantees that we can compute efficiently in wreath products, so that if we can compute (the constant-size set) Q_n efficiently, we can find neighbors in G_n efficiently, and also compute Q_{n+1} recursively from Q_n; for the details, see [**RSW06**]. Notice that the naive approach of computing neighbors recursively won't work, because to compute a neighbor in G_n, we have to call the neighbor algorithm on G_{n-1} *twice*, since $\underline{x}$ appears twice in $y\underline{x}zy'\underline{x}z'$. This will make the running time exponential in n. This is essentially the same problem we encountered in Example 4.32 with the first construction of expanders from the zig-zag product that was based on squaring!

□

5.1.2. A generalization. How much can we abstract about the above construction of an expanding tower? Ignoring explicitness for now, the broad idea behind it is to start with a graph G_0, and apply some operations that have a nice effect on expansion to get to a graph G_1 that miraculously turns out to be a cover of G_0; we then repeat the process with the new graph G_1. But how does the miracle happen?

Here's an idea: what if we start with G_0 being a very simple graph - like a bouquet of circles - then, as we saw in Subsection 4.1.1, many graphs will cover G_0, so we have a higher chance of success; in the undirected case, any even degree graph suffices by Example 4.11! Now suppose we have our sequence of operations α such that $\alpha(G_0)$ covers G_0. The other main idea we need is exactly the theory developed in Chapter 4: if every individual operation in α is one of the operations we proved are compatible with covering maps, the covering $\alpha(G_0) \to G_0$ will imply a covering $\alpha(\alpha(G_0)) \to \alpha(G_0)$ - so letting $G_2 = \alpha(G_1)$, this is exactly a covering $G_2 \to G_1$! This is the essence of the magic.

Since the operations that are interesting for expansion depend on the rotation maps, we have to worry about that too; but it turns out that we can inductively define the labels in a way that makes the above idea work. The point is, when we get a covering $\alpha(G_n) \to \alpha(G_{n-1}) = G_n$, to discard the labels on $\alpha(G_n)$ that come from α and the labels on G_n, and adopt the labels that are induced from the labels on G_n, and the covering $\alpha(G_n) \to G_n$. The interplay between the labels is somewhat subtle, so pay close attention! Finally, when we compose several operations, we have to keep in mind the implicit re-orderings of the factors in the vertex sets of our graphs induced by these operations, as explained in Remark 4.20.

Proposition 5.2. *Suppose α is a sequence of operations on two-way labeled digraphs, where each operation is of the following form:*

- $G \mapsto G^k$ *or* $G \mapsto G^{\otimes k}$ *for some* k*;*
- $G \mapsto G \otimes H$ *or* $G \mapsto G \textcircled{z} H$ *or* $G \mapsto G \textcircled{s} H$ *for some digraph* H*;*
- $G \mapsto G^T G$ *or* $G \mapsto G^\dagger$*.*
- $G \mapsto G \textcircled{z} \overline{H}$ *whenever the generalized zig-zag product is defined.*

such that whenever G is an $|S|$-regular digraph, $\alpha(G)$ is also an $|S|$-regular digraph. Moreover, suppose that for some two-way labeling l_0 of $G_0 := B_S$, the result of $\alpha(G_0; l_0)$ satisfies any of the conditions in Proposition 4.10. Then there is a sequence of graphs $G_0, G_1, \ldots$ and two-way labelings $l_0, l_1, \ldots$ such that for all $n \geq 0$, $G_{n+1} = \alpha(G_n; l_n)$, and there is a labeled covering map $(G_{n+1}; l_{n+1}) \to (G_n; l_n)$.

Proof. We will define the sequence inductively; the base case comes by letting $G_1 = \alpha(G_0; l_0)$, since by Proposition 4.10 $\alpha(G_0)$ covers G_0. Note that in general there is no reason for this covering map to be 'compatible' in any way with the labels l_0 and the labels inherited by G_1 from α and l_0! Now set l_1 to be the labels induced on G_1 from the covering $G_1 \to (G_0; l_0)$. This completes the base case.

For the step, assume that we have a labeling l_{n-1} such that $G_n = \alpha(G_{n-1}; l_{n-1})$, and that we have a labeled covering map $p_n : (G_n; l_n) \to (G_{n-1}; l_{n-1})$. Since each individual operation of α preserves the labeled covering as we proved in Chapter 4, we get a covering $p_{n+1} : \alpha(G_n; l_n) \to \alpha(G_{n-1}; l_{n-1}) = G_n$; now let $G_{n+1} = \alpha(G_n; l_n)$, and let l_{n+1} be induced from the covering $G_{n+1} \to G_n$ we just found, when G_n is given labels l_n. □

This gives a mildly explicit construction of expanding towers - we can simply simulate the inductive proof, and build up all the graphs up to G_n. *However*, observe that we keep changing the labels and don't stick with the ones inherited from the operation α.

5.1.3. Rosenman-Shalev-Wigderson revisited. Going back to the Rozenman-Shalev-Wigderson construction, we can now spot an implicit bouquet of $|Q|^4$ circles G_0 as the bottom graph, and get a much clearer idea of what's going on. As we saw in the proof outline 5.1, the sequence of operations here is

$$G_n \mapsto \frac{d}{|Q|^4} G_n \mapsto \left(\left(\frac{d}{|Q|^4} G_n\right) \textcircled{z} \mathrm{Sch}(K_1, E_1, Q)\right) \mapsto \left(\left(\frac{d}{|Q|^4} G_n\right) \textcircled{z} \mathrm{Sch}(K_1, E_1, Q)\right)^2 = G_{n+1}$$

All operations respect coverings. Duplicating edges is not quite one of our operations, but let's implicitly interpret it as a tensor product with a consistently labeled bouquet of circles (recall Example 4.24). It remains to establish the base case. Give a two-way labeling of the bouquet $G_0 = B_{Q^4}$ that is consistent, i.e. every loop has the same label at the tail and the head. Then $\frac{d}{|Q|^4} G_0$ is also consistently labeled, so as we saw in Example 4.30, $\left(\frac{d}{|Q|^4} G_0\right) \textcircled{z} \mathrm{Sch}(K_1, E_1, Q) = (\mathrm{Sch}(K_1, E_1, Q))^2 = \mathrm{Sch}(K_1, E_1, Q^2)$. The square is $\mathrm{Sch}(K_1, E_1, Q^4)$, which is exactly G_1; since G_1 is a Schreier graph, the base case of Proposition 5.2 holds! Thus, we were able to show expansion and covering without explicit reference to the wreath product structure, and only using the fact that our first graph is a Schreier graph.

But iterated wreath products will be implicit in any expanding tower based on Proposition 5.2. Indeed, this happens because

- Any lift of a bouquet with permutation voltages in $\mathcal{G}$ is a Schreier graph of $\mathcal{G}$;
- All our operations transform a covering map with voltages in some permutation group $\mathcal{G}$ to another covering map with voltages in either $\mathcal{G}$, or some direct power $\mathcal{G}^d$ in the case of the tensor power; but as we saw in Example 3.27, $\mathcal{G}^d \subset \wr_{i=1}^d \mathcal{G}$;
- The top of a tower of lifts with voltages in groups $\wr_i \mathcal{G}$ is a lift of the base graph with voltages in some $\wr_i \mathcal{G}$, by Proposition 3.28. Since our base graph is a bouquet, this means that the top graph will be a Schreier graph of $\wr_i \mathcal{G}$.

5.1.4. Adding the tensor trick. It is desirable to give a fully explicit construction along the lines of Rozenman-Shalev-Wigderson where the use of the commutator property is avoided. Intuitively, the trouble with the naive approach of recursively computing the action of the generating set comes from the fact that we use squaring, which is similar to when we tried to make fully explicit expanders with the zig-zag product in Example 4.32. So we want to use some form of the tensor trick; but it doesn't seem to be of the form of Proposition 5.2.

Fortunately, it turns out that our technique is applicable to the tensor trick construction as well! To make the base case work, we switch around the order of squaring and zig-zagging, but otherwise everything is very similar.

Proposition 5.3 (Fully explicit towers without the commutator property). *Let $G_0 = B_S$ with $|S| = |D^4|$, and H be a two-way labeled (D^8, D, λ) digraph which satisfies any of the conditions of Proposition 4.10. Then there is a sequence of graphs $G_0, G_1, \ldots$ and two-way labelings $l_0, l_1, \ldots$ such that for all $0 < k$,*

$$G_k = \left(\left(\left(G_{\lceil \frac{k-1}{2} \rceil}; l_{\lceil \frac{k-1}{2} \rceil}\right) \otimes \left(G_{\lfloor \frac{k-1}{2} \rfloor}; l_{\lfloor \frac{k-1}{2} \rfloor}\right)\right) ⓩ H\right)^2$$

and there is a labeled covering map $(G_k; l_k) \to (G_{k-1}; l_{k-1})$. Moreover, the graphs form a fully explicit family of expanders.

Proof. We split the proof in three parts: proving the covering relations, proving expansion, and proving explicitness.

Covering. We proceed by induction on the length of the sequence of graphs and labelings constructed so far. For the base case $n = 1$, let l_0 be a labeling of G_0 which is consistent, so that the head and tail of every loop get the same label. Then, $(G_0; l_0) \otimes (G_0; l_0)$ inherits a consistent labeling as well, and we define $G_1 = ((G_0; l_0) \otimes (G_0; l_0) ⓩ H)^2 = (H^2)^2 = H^4$, from Example 4.30. By assumption, H is a Schreier graph, hence H^4 is also a Schreier graph, thus there is a covering map $G_1 \to G_0$ we can compute in constant time. Finally let l_1 be the labeling induced from that covering map and l_0. This completes the base case!

Now for the inductive step: suppose we have a sequence of digraphs $G_0, G_1, \ldots, G_n$ and two-way labelings $l_0, \ldots, l_n$ with the wanted properties. We have two analogous cases, so we only deal with $n = 2k$. Here $\lceil \frac{n+1-1}{2} \rceil = \lfloor \frac{n+1-1}{2} \rfloor = k$. From the labeled covering map $(G_k; l_k) \to (G_{k-1}; l_{k-1})$ and the identity covering map $(G_k; l_k) \to (G_k; l_k)$, it successively follows that we have labeled covering maps

$$(G_k; l_k) \otimes (G_k; l_k) \to (G_k; l_k) \otimes (G_{k-1}; l_{k-1})$$
$$((G_k; l_k) \otimes (G_k; l_k)) ⓩ H \to ((G_k; l_k) \otimes (G_{k-1}; l_{k-1})) ⓩ H$$
$$(((G_k; l_k) \otimes (G_k; l_k)) ⓩ H)^2 \to (((G_k; l_k) \otimes (G_{k-1}; l_{k-1})) ⓩ H)^2 = G_n$$

We now let $G_{n+1} = (((G_k; l_k) \otimes (G_k; l_k)) ⓩ H)^2$, and l_{n+1} be the labeling induced by the covering map $G_{n+1} \to G_n$ when G_n is given labels l_n.

Expansion. One can show by induction that G_n is an (D^{8n}, D^4)-digraph. By the properties of our operations, $\lambda(G_k) \leq (\max\{\lambda(G_1), \ldots, \lambda(G_{k-1})\} + \lambda)^2$ and $\lambda(G_1) = \lambda^4, \lambda(G_0) = 0$. We can show by induction that $\lambda(G_k) \leq \lambda^2 + c\lambda^3$ for some appropriately chosen c as long as λ is a small constant. Hence, if we start with a Ramanujan, even-degree, undirected H (which is known to exist, and can be found by brute-force search), we get a family of t-regular graphs with $\lambda(G_n) \leq O(t^{-1/4})$.

Explicitness. We reason inductively. We start by computing a covering map $H^4 \to G_0$ if we're not given a Schreier structure on H; this can be done in time constant in n, say by brute-force search. Next, let t_{n+1} be the labeling by elements of D^4 on G_{n+1} induced from the operations

$$G_{n+1} = \left(\left(\left(G_{\lceil \frac{n}{2} \rceil}; l_{\lceil \frac{n}{2} \rceil}\right) \otimes \left(G_{\lfloor \frac{n}{2} \rfloor}; l_{\lfloor \frac{n}{2} \rfloor}\right)\right) ⓩ H\right)^2$$

Observe that, inductively assuming an algorithm for computing rotations with respect to $l_0, l_1, \ldots, l_n$, we can easily compute rotations *under* t_{n+1}. The complication is that we need the rotation under l_{n+1}! The key is that we can go 'all the way down' with the D^4 labels, and then come back 'all the way up'

with the S labels. Without loss of generality, when $n = 2k$ is even, we have the tower of labeled covering maps $(G_{n+1}; l_{n+1}) \to (G_n; l_n) \to \ldots \to (G_1; l_1)$; by the Covering portion of the proof, ignoring labels, this tower is the same as the tower of labeled coverings

$$\begin{aligned}(((G_k; l_k) \otimes (G_k; l_k)) \circledcirc H)^2 &\to (((G_k; l_k) \otimes (G_{k-1}; l_{k-1})) \circledcirc H)^2 \\ \to (((G_{k-1}; l_{k-1}) \otimes (G_{k-1}; l_{k-1})) \circledcirc H)^2 &\to (((G_{k-1}; l_{k-1}) \otimes (G_{k-2}; l_{k-2})) \circledcirc H)^2 \\ &\to \ldots \to (((G_0; l_0) \otimes (G_0; l_0)) \circledcirc H)^2 = G_1\end{aligned}$$

Suppose we want to compute $\mathrm{Rot}_{(G_{n+1}; l_{n+1})}(u, s)$, that is, determine s' and v in the edge $u \xrightarrow{s \quad s'} v \in E(G_{n+1}; l_{n+1})$ given $u \in V(G_{n+1})$ and $s \in S$. Let $p : G_{n+1} \to G_1$ be the composed covering map; then we have an edge $p(u) \xrightarrow{s \quad s'} p(v) \in E(G_1; l_1)$. This same edge has some labeling

$$p(u) \xrightarrow{(d_1, d_2, d_3, d_4) \quad (d'_1, d'_2, d'_3, d'_4)} p(v) \in E(G_1; t_1)$$

which comes from the choice of covering map $G_1 \to G_0$ we made in the base case. Lifting back, this means there is an edge $u \xrightarrow{(d_1, d_2, d_3, d_4) \quad (d'_1, d'_2, d'_3, d'_4)} v \in E(G_{n+1}; t_{n+1})$, so we've reduced the problem to computing a single rotation in $(G_{n+1}; t_{n+1})$.

How much time does it take to run the above computation? Given u, we know what $p(u)$ is by keeping track of how our operations change the vertex sets of our graphs. The vertex set of G_n is $V(H)^n$, and one of these n coordinates is a lift coordinate for the covering map $G_n \to G_{n-1}$. Let f_n be the index of the lift coordinate; we will show how to compute it inductively. Clearly $f_1 = 1$, and if $n = 2k$ is even, as we saw above, the covering $G_{n+1} \to G_n$ comes from tensoring the coverings $G_k \to G_k$ and $G_k \to G_{k-1}$, and then zig-zagging with H. The resulting vertex set is $V(G_k) \times V(G_k) \times V(H)$, and the lift coordinate is the f_k-th factor of the *second* copy of $V(G_k) = V(H)^k$. The case $n = 2k - 1$ is analogous, and we get the recursion

$$f_{n+1} = \begin{cases} k + f_k, & \text{if } n = 2k \\ f_k, & \text{if } n = 2k - 1 \end{cases}$$

Following this, f_n can be computed in polynomial (in fact polylogarithmic) time in n. To get to $p(u)$, we peel the lift coordinates one by one, which again takes some polynomial $O(n^c)$ in total, for example $O(n^3)$ is easily seen to work. When we get to $p(u)$, we look up $\mathrm{Rot}_{G_1}(p(u), s)$ and recover s'. Getting to (d_1, d_2, d_3, d_4) can be done in constant time by consulting the correspondence between the labelings l_1 and t_1, since G_1 is a constant-size graph. Then it remains to apply the rotation map for $(G_{n+1}; t_{n+1})$ to get v, by accessing the rotation maps for $\left(G_{\lceil \frac{k-1}{2} \rceil}; l_{\lceil \frac{k-1}{2} \rceil}\right)$ and $\left(G_{\lfloor \frac{k-1}{2} \rfloor}; l_{\lfloor \frac{k-1}{2} \rfloor}\right)$ twice each (roughly $4T(n/2)$ time), and the rotation map of H four times (constant time). Overall, the running time to compute a rotation of $(G_{n+1}; l_{n+1})$ is $T(n+1) \approx 4T(n/2) + O(n^c) + C$ for some constants c, C, which by standard bounds means $T(n) = \mathrm{poly}(n)$, and we have full explicitness. □

5.1.5. Adding the generalized zig-zag product. Ben-Aroya and Ta-Shma use their generalized zig-zag product (Subsection 4.5.4) to give a fully explicit construction of *almost Ramanujan* expanders that is analogous to the construction using the zig-zag product, but can achieve $\lambda(G) = O(d^{1/2+\delta}/d)$ for any $\delta > 0$; it turns out that it can also be made compatible with lifts in the spirit of Proposition 5.3:

Proposition 5.4 (Fully explicit almost Ramanujan towers). *Let D_2 be a set of even size, $D = D_2^k \times \{-1, 1\}$ and $G_0 = B_D$. Let $\overline{H} = (H_1, \ldots, H_k)$ be a sequence of undirected locally invertible $(D^{16k}, D_2, \lambda_2)$-digraphs that is ε-good with respect to all D^4-regular locally invertible graphs for $\varepsilon = |D_2|^{-k}$ and $\lambda_2 = 2\sqrt{|D_2| - 1}/|D_2| + \varepsilon$ (which exists by Theorem 4.38). Then there is a sequence of undirected (D^{16kt}, D, λ)-digraphs $G_0, G_1, \ldots$ for $\lambda = 2\lambda_2^{k-1}$ and two-way labelings $l_0, l_1, \ldots$ such that for all $0 < k$,*

$$G_k = \left(\left(\left(G_{\lceil \frac{k-1}{2} \rceil}; l_{\lceil \frac{k-1}{2} \rceil}\right) \otimes \left(G_{\lfloor \frac{k-1}{2} \rfloor}; l_{\lfloor \frac{k-1}{2} \rfloor}\right)\right)^2 \circledcirc \overline{H}\right)^{\dagger}$$

and there is a labeled covering map $(G_k, l_k) \to (G_{k-1}, l_{k-1})$. Moreover, the labels l_k make G_k into a consistently labeled digraph, and the graphs form a fully explicit expander family.

PROOF. As before, we let l_0 be the consistent two-way labeling of $G_0 = B_D$. Let $G_1 = (((G_0; l_0) \otimes (G_0; l_0))^2 \textcircled{z} \overline{H})^\dagger$; the application of the generalized zig-zag is possible, since the big graph is a consistently labeled B_{D^4}. Since G_1 is an even degree undirected graph, following Example 4.11 there is an undirected Schreier graph structure on it; using this structure, we get a covering map $G_1 \to G_0$ which induces labels l_1 on G_1. As $(G_0; l_0)$ is consistently labeled, this is also true of G_1. This completes the base case!

The inductive step is analogous to the covering step in Proposition 5.3, since all the operations we're using respect coverings, as shown in Chapter 4. Here are the modifications:

- we have to be careful that we apply the generalized zig-zag product to locally invertible graphs. But by induction, both $\left(G_{\lceil \frac{k-1}{2} \rceil}; l_{\lceil \frac{k-1}{2} \rceil}\right)$ and $\left(G_{\lfloor \frac{k-1}{2} \rfloor}; l_{\lfloor \frac{k-1}{2} \rfloor}\right)$ are consistently labeled, and since consistent labeling is a special case of local invertibility, Fact 4.36 tells us that the square of their tensor product is also locally invertible.
- We have to show the next labeling we get is consistent. As before, we get to a covering map $G_{n+1} \to G_n$ and we induce labels l_{n+1} on G_{n+1} from the labels l_n from G_n. By induction l_n gives a consistent labeling, hence Fact 4.36 tells us that so does l_{n+1}.

For expansion, the analysis of Ben-Aroya and Ta-Shma applies here to give bounds on expansion; the only difference is that we have different base cases, so it suffices to show that $\lambda(G_1), \lambda(G_2) \leq \lambda$, after which their induction applies to give us $\lambda(G_n) \leq \lambda$. Using Theorem 4.38 and the effect of the other operations on expansion, we have $\lambda(G_1) \leq \lambda_2^{k-1} + 2/|D_2|^k + \lambda_2^k \leq \lambda$ as long as the H_i have diameter > 2 (recall Section 2.6) and $\lambda_2 \leq 1/2$, in which case we can use the bound $\lambda_2 \geq 1/\sqrt{|D_2|}$. Then $\lambda(G_2) \leq \lambda_2^{k-1} + 2/|D_2|^k + 2\lambda(G_1)^2 + \lambda_2^k \leq \lambda$ by using analogous bounds.

Finally, full explicitness follows in analogy with the Explicitness portion of the proof of Proposition 5.3. The difference is that the running time will be a polynomial of degree depending on k, as we take many steps in the big graph in the generalized zig-zag product.[1] □

5.1.6. Making the [RSW06] tower denser. The towers produced by Rozenman, Shalev and Wigderson are of quite large degree (that is, $|V(G_{n+1})|$ is much larger than $|V(G_n)|$); this is because we require that $d > |Q|^4$. Here we sketch a way to make the tower denser, ignoring explicitness.

Suppose we start our construction with a Schreier graph $\mathrm{Sch}(\wr_i \mathbb{Z}/2\mathbb{Z}; E_1; Q^4)$ that is itself of a wreath product. Then, by Proposition 3.28 and Example Example 3.5 it follows that our expanders will be Schreier graphs of groups $\wr_j \wr_i \mathbb{Z}/2\mathbb{Z}$; by associativity, this is just an iterated wreath product $\wr_i \mathbb{Z}/2\mathbb{Z}$. By Proposition 3.28 and by the consistency of the generators, this means that we in fact have a tower of 2-lifts!

This is of course provided that we have a base case $\mathrm{Sch}(\wr_{i=1}^n \mathbb{Z}/2\mathbb{Z}; E_1; Q)$ for n a large constant which is a good expander with $|Q|^4 < |E_1|$. As we know from Example 3.27, the direct product $(\mathbb{Z}/2\mathbb{Z})^n$ lives inside the wreath product, and it's easy to see that the problem of finding such an expanding Schreier graph reduces to the problem of finding an expanding Cayley graph for $(\mathbb{Z}/2\mathbb{Z})^n$, at which point classical results by Alon and Roichman [**AR94**] give probabilistic constructions. In the next section, we show in a different way that in the *bipartite* setting, such Schreier expanders (and in fact much better ones) exist.

5.2. Bipartite Ramanujan Schreier graphs for iterated wreath products of $\mathbb{Z}/2\mathbb{Z}$

In 2013, Marcus, Spielman and Srivastava published a breakthrough paper [**MSS13**] that showed the existence of *bipartite* Ramanujan expanders of all degrees $d > 2$, following an approach proposed by

[1] We remark that, upon a closer look at the proof, the goodness of $\overline{H}$ with respect to *all* D^4 locally-invertible graphs is not necessary! The reason is that the graphs we apply the zig-zag product to, also being a tower of lifts, have the same local inversion function, and it is in fact with respect to the local inversion function that goodness is measured; see the paper by Ben-Aroya and Ta-Shma [**BATS11**]. This means we have a lot more freedom to choose $\overline{H}$, and thus a lot more freedom to choose G_1.

Bilu and Linial [**BL06**] of taking successive two-lifts. Bipartite expanders are a relaxation of undirected expanders where we care about the largest in absolute value eigenvalue, *ignoring the largest and the smallest eigenvalues*; the reason is that in a d-regular bipartite graph, the smallest eigenvalue of W_G is -1. Such expander families are still interesting, since for some applications (as we saw in Subsection 2.1.1), bipartite expanders suffice.

In this section, we sketch the main points of the construction, and remark that it generalizes to multigraphs in a straightforward way, which we can use to show existence of bipartite Ramanujan Schreier graphs of iterated wreath products of $\mathbb{Z}/2$. The plan of attack is the following: we want to show that for every bipartite Ramanujan graph there is a 2-lift that is also Ramanujan. Since lifts of bipartite graphs are bipartite, we can repeat the argument. So we need to show a good 2-lift exists, which means that a good signing matrix (as in Example 3.19) exists. It turns out that:

- if we average the characteristic polynomials of the signing matrices corresponding to all possible 2-lifts, we get a nice real-rooted polynomial, called the *matching polynomial*, which has all roots bounded in absolute value by $2\sqrt{d-1}$.
- These characteristic polynomials satisfy a special property, called *interlacing*, that guarantees that (this is the magic moment of the paper) the largest root of some of them is at most the largest root of their average!

Since for a bipartite graph the eigenvalues are symmetric about 0, this automatically takes care of the negative eigenvalues as well. The generalization to multigraphs has three main steps:

- the signing matrix generalizes, as we saw in Example 3.19;
- the bound on the roots of the average characteristic polynomial was in fact originally proved in the generality of multigraphs;
- the interlacing property generalizes as well, since it comes from a 'linear' argument, which is compatible with our signing matrix.

5.2.1. Interlacing families. The basis of the result is a new probabilistic argument for bounding roots of polynomials. A polynomial f is said to **interlace** a polynomial g if both are real-rooted, $\deg f = \deg g + 1$, and if the roots of f are $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ and the roots of g are $\beta_1, \ldots, \beta_n$, we have

$$\alpha_1 \leq \beta_1 \leq \alpha_2 \leq \ldots \leq \alpha_n \leq \beta_n \leq \alpha_{n+1}$$

We say that polynomials $f_1, \ldots, f_m$ have a **common interlacing** if there is a polynomial g that interlaces each of them. Here's the prototype of the probabilistic result:

Fact 5.5 (Interlacing families: prototype). *Suppose $f_1, \ldots, f_m$ are polynomials with positive leading coefficients that have a common interlacing. Then there exists some i such that the largest root of $f_\emptyset = \sum_{i=1}^m f_i$ is $\geq$ the largest root of f_i.*

This is an elementary exercise; drawing some pictures of the polynomials will help you see how easy the proof is! From this innocent-looking statement, we can inductively generalize to the following:

Definition 5.6 (Interlacing families). Let $S_1, \ldots, S_m$ be finite sets, and let us have, for every $(s_1, \ldots, s_m) \in S_1, \ldots, S_m$, a polynomial $f_{s_1,\ldots,s_m}$ with positive leading coefficient. For $1 \leq k \leq m$, define the partial sums

$$f_{s_1,\ldots,s_k} = \sum_{s_{k+1} \in S_{k+1}, \ldots, s_m \in S_m} f_{s_1,\ldots,s_k,s_{k+1},\ldots,s_m}$$

and let $f_\emptyset = \sum_{s_1,\ldots,s_m} f_{s_1,\ldots,s_m}$. We say that $\left\{ f_{s_1,\ldots,s_m} \;\middle|\; (s_1, \ldots, s_m) \in S_1 \times \ldots \times S_m \right\}$ form an **interlacing family** if $\left\{ f_{s_1,\ldots,s_k,t} \;\middle|\; t \in S_{k+1} \right\}$ have a common interlacing for all $0 \leq k < m$ and all $s_1, \ldots, s_k$.

Of course, the common interlacing property forces the polynomials to have real roots and the same degree. The main fact about interlacing families easily follows from the prototype 5.5 by induction:

FACT 5.7. *For $\{f_{s_1,\dots,s_m}\}$ an interlacing family as above, there exist $s_1, \dots, s_m$ such that the largest root of $f_{s_1,\dots,s_m}$ is at most the largest root of $f_\emptyset$.*

So we came up with that strange, special condition which guarantees us a sort of probabilistic method for roots of polynomials. But so what? The key is that – and this is still being used to produce new results – many natural families of combinatorial polynomials are interlacing families!

5.2.2. The matching polynomial. For an undirected graph G, define the **matching polynomial** to be $\mu_G(x) = \sum_{i \geq 0} x^{n-2i}(-1)^i m_i$ where m_i is the number of matchings in G that consist of i edges, and $m_0 = 1$. If there are multiple edges between two vertices, only one of them can be included in a matching, but it matters for the count *which* one, so that for example in the graph

there are 6 matchings of 2 edges, and 5 matchings of one edge. This corresponds to counting matchings in simple *weighted* graphs, where a matching on edges with weights $w_1, \dots, w_i$ contributes $w_1 \dots w_i$ to the count. It is in this context that the matching polynomial was studied by Heilmann and Lieb [**HL04**]. The MSS paper used the specialization of this to simple graphs, but it is true more generally. The proof is just a careful reading of Heilman and Lieb, so we defer it to Proposition A.3:

PROPOSITION 5.8 (FROM THEOREMS 4.2 AND 4.3 IN [**HL04**]). *For a multigraph G with maximum degree at most d, all roots of $\mu_G(x)$ are real and have absolute value $\leq 2\sqrt{d-1}$.*

5.2.3. The expected characteristic polynomial of the signing. It turns out that the average of the characteristic polynomials of the signing matrices (as defined in Example 3.19) for all 2-lifts of a multigraph is the matching polynomial of the multigraph; again, this is very similar to the corresponding proof for simple graphs, so we defer it to Proposition A.4:

PROPOSITION 5.9 (FROM THEOREM 3.6 IN [**MSS13**]). *Let us be given a multigraph G, and let s be the random variable which gives a uniformly random signing: that is, every edge gets independently 2-lifted by the identity permutation or the transposition $(1\ 2)$ with uniform probability. Let A_s be the singing matrix (also a random variable); then $\mathbf{E}_s[\det(xI - A_s)] = \mu_G(x)$.*

5.2.4. Putting it all together. At this point, Marcus, Spielman, and Srivastava finish the problem by showing that, when we take $m = |E(G)|$ and $S_1 = \dots = S_m = \{1, -1\}$, the polynomials $f_s = \det(xI - A_s)$ as s ranges over all signings $\{1, -1\}^m$ are an interlacing family. From Fact 5.7, this means that there is some signing $s' = (s_1, \dots, s_m)$ such that the largest root of $f_{s'}$ is at most the largest root of $\mathbf{E}_s[\det(xI - A_s)]$; from 5.9, this equals the largest root of $\mu_G(x)$; and from Proposition 5.8, this is at most $2\sqrt{d-1}$.

We have generalized all the steps to multigraphs, except for the interlacing property. In the paper, this follows in roughly two steps: first, interlacing is characterized by the real-rootedness of certain families of polynomials; then, the theory of *real stable polynomials* is used to show these polynomials indeed have real roots. The key steps are the following:

FACT 5.10 ([**MSS13**], THEOREM 5.2). *If for any reals $p_1, \dots, p_m \in [0, 1]$, the polynomial*

$$R(x) = \sum_{s \in \{\pm 1\}^m} \left(\prod_{i : s_i = 1} p_i \right) \left(\prod_{i : s_i = -1} (1 - p_i) \right) \det(xI - A_s)$$

is real rooted, the polynomials $\{f_s\}_{s \in \{\pm 1\}^m}$ form an interlacing family.

FACT 5.11 ([**MSS13**], THEOREM 6.6.). *Let $a_1, \dots, a_m$ and $b_1, \dots, b_m$ be vectors in $\mathbb{R}^n$, and let $p_1, \dots, p_m$ be reals in $[0, 1]$, and D a positive semidefinite matrix. Then every univariate polynomial of the form*

$$P(x) = \sum_{S \subset [m]} \left(\prod_{i \in S} p_i \right) \left(\prod_{i \notin S} 1 - p_i \right) \det \left(xI + D + \sum_{i \in S} a_i a_i^T + \sum_{i \notin S} b_i b_i^T \right)$$

is real-rooted.

The point is that we can get the above determinant to be $\det(xI + dI - A_s)$, by picking $a_i = e_u - e_v$ and $b_i = e_u + e_v$ whenever i is an edge between u and v, where e_u, e_v are characteristic vectors of the vertices u and v respectively. But this works just as well for multigraphs! This real-rootedness suffices, since then the roots of $P(x)$ will be the roots of $R(x)$ shifted by d, so real-rootedness of $P(x)$ implies real-rootedness of $R(x)$. This completes the generalization.

5.2.5. Bipartite Ramanujan Schreier graphs for $\wr_i \mathbb{Z}/2\mathbb{Z}$. Let $G_0 = B_d$ be the bouquet of $d \geq 3$ loops, and take the bipartite double cover G_0 (Example 2.11) of B_d. Then make it into an undirected multigraph of degree d; this is our base case. It's immediate that the spectrum of G_1 is $\{-d, d\}$, so it's a bipartite Ramanujan graph. By what we just proved, there exists a tower of 2-lifts $G_1, G_2, G_3, \ldots$ over G_1 that form a family of Bipartite Ramanujan expanders. Since G_1 is itself a 2-lift of B_S, we have a tower of 2-lifts over B_S, which by Proposition 3.28 means that G_n is a lift of B_S with permutation voltages in $\wr_{i=1}^n \mathbb{Z}/2\mathbb{Z}$, which by Example 3.5 means that G_n is a Schreier graph of $\wr_{i=1}^n \mathbb{Z}/2\mathbb{Z}$.

5.3. Translation results for classical constructions

In the 'classical' constructions based on a group $\mathcal{G}$ with property (T), which is a certain condition on the unitary representations of $\mathcal{G}$, the way one usually constructs expanders was by considering a 'nice' Cayley graph of $\mathcal{G}$ with a finite generating set, and then 'projecting' it to a Cayley graph of a quotient by a finite index subgroup $\mathcal{H}_n$ of $\mathcal{G}$; as we vary the index $[\mathcal{G} : \mathcal{H}_n]$, we get graphs of increasing sizes with uniformly bounded spectral expansion. If we pick the subgroups the right way, we get an expanding tower! Here, we follow Lubotzky [**Lub12**] to outline this idea:

Fact 5.12 (Proposition 2.2, [**Lub12**]). *Let $\mathcal{G}$ be a group with property (T) generated by a finite symmetric set S, and let $N = \left\{\mathcal{N} \;\middle|\; \mathcal{N} \text{ is a normal subgroup of } \mathcal{G} \text{ with } [\mathcal{G} : \mathcal{N}] < \infty\right\}$. Then there exists $\lambda < 1$ such that $\lambda(\mathrm{Cay}(\mathcal{G}/\mathcal{N}, S)) < \lambda$ for all $\mathcal{N}$.*

It's easy to see that if $\mathcal{N}_2 \subset \mathcal{N}_1$, $\mathrm{Cay}(\mathcal{G}/\mathcal{N}_2, S)$ covers $\mathrm{Cay}(\mathcal{G}/\mathcal{N}_1, S)$ by the natural mapping given by labels from S; usually, it's not hard to find an infinite sequence $\ldots \subset \mathcal{N}_2 \subset \mathcal{N}_1$ of normal subgroups; then we get an expanding tower! At this point, many of the results from Chapter 4 can be applied to this tower to translate it to another expanding tower, over a different base graph! For example, since the tower of Cayley graphs is over the bouquet B_S which is labeled consistently with the generators S, when we zig-zag the entire tower with some S-regular graph H, we get a new tower over H^2. This can tell us more about which graphs have good lifts!

5.4. Conclusions and future work

The main insight we seem to have gained from the theory developed in this thesis is that, if we take the approach of explicit constructions of expanders by iteratively applying graph operations like powering, tensoring and zig-zag products, imposing the additional condition that our expander families form towers comes almost 'for free' – for example, in the undirected setting, if we start with an even-degree bouquet of circles.

Along the way, we explored many beautiful properties of coverings, and it feels like there is a lot more to be understood. As we saw, somewhat surprisingly, explicitly working with multigraphs and voltage assignments can be beneficial to our understanding of coverings and expansion! It is also interesting what the most general form of a construction along the lines of Propositions 5.2, 5.3 and 5.4 is, what the categorical framework can give us, what translation results between towers we can give, and to see whether the parallel between the worlds of Cayley/Schreier graphs on the one hand, and ordinary/relative voltage assignments on the other, can be extended further.

List of some notation

G, H, K	Usually a graph/digraph
S, T, V, D, E	Usually a set
d, n, m	Usually a natural number
$\mathcal{G}, \mathcal{H}, \ldots$	A group
$\Gamma(S)$	The set of vertices with a neighbor in $S \subset V(G)$ for a graph G
$\mathrm{poly}(n)$	Polynomial time: number of steps bounded by Cn^k for some constants C, k
$\mathrm{polylog}(n)$	Polylogarithmic time: number of steps bounded by $C(\log n)^k$ for some constants C, k.
$o(f(n)), o_n(f)$	A function $g : \mathbb{N} \to \mathbb{N}$ such that $\lim_{n\to\infty} g(n)/f(n) = 0$
$O(f(n)), O_n(f)$	A function $g : \mathbb{N} \to \mathbb{N}$ such that $g(n) \leq f(n)$ for some constant C
$\bigvee_{i=1}^{n} b_i$	The logical disjunction of $b_1, \ldots, b_n$
$\mathrm{Cay}(\mathcal{G}, S)$	The Cayley graph of the group $\mathcal{G}$ with respect to the multiset $S \subset \mathcal{G}$
$\mathbf{E}_X[f(X)]$	The expectation of the function $f(X)$ with respect to the random variable X
$\mathbf{Pr}_X[E(X)]$	The probability of the event $E(X)$ with respect to the random variable X
$\|v\|$	The l_2 norm of the vector v
$\|v\|_1$	The l_1 norm of the vector v
e^-	The *tail*, i.e. the source vertex, of the edge e
e^+	The *head*, i.e. the targe vertex, of the edge e
B_S	A digraph: the bouquet of loops in bijection with a set S.
B_d	A digraph: the bouquet of loops in bijection with $\{1, \ldots, d\}$
$\mathcal{G}/\mathcal{H}$	The left cosets of $\mathcal{H}$ in $\mathcal{G}$.
$\mathrm{GL}(\mathcal{V})$	The group of invertible linear operators on the vector space $\mathcal{V}$
$\mathrm{U}(\mathcal{V})$	The group of unitary linear operators on the complex vector space $\mathcal{V}$.
$\mathcal{V}^\perp$	The orthogonal complement of a vector space $\mathcal{V}$.
$\mathrm{Sym}(S), \mathrm{Sym}(n)$	The symmetric group on the set S / on n elements.
$\mathrm{Alt}(S), \mathrm{Alt}(n)$	The alternating group on the set S / on n elements.
u_G	The uniform probability distribution on the set $V(G)$ for a digraph G.

Bibliography

[AKK+08] Sanjeev Arora, Subhash A Khot, Alexandra Kolla, David Steurer, Madhur Tulsiani, and Nisheeth K Vishnoi. Unique games on expanding constraint graphs are easy. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 21–28. ACM, 2008.

[AKM13] Naman Agarwal, Alexandra Kolla, and Vivek Madan. Small lifts of expander graphs are expanding. *arXiv preprint arXiv:1311.3268*, 2013.

[AKS83] Miklós Ajtai, János Komlós, and Endre Szemerédi. An 0 (n log n) sorting network. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 1–9. ACM, 1983.

[AL06] Alon Amit and Nathan Linial. Random lifts of graphs: edge expansion. *Combinatorics, Probability and Computing*, 15(03):317–332, 2006.

[ALM] Alon Amit, Nathan Linial, and journal=Random Structures & Algorithms volume=20 number=1 pages=1–22 year=2002 publisher=Wiley Online Library Matousek, Jir. Random lifts of graphs: independence and chromatic number.

[ALMR01] Alon Amit, Nathan Linial, Jir Matousek, and Eyal Rozenman. Random lifts of graphs. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*, pages 883–894. Society for Industrial and Applied Mathematics, 2001.

[ALW01] Noga Alon, Alexander Lubotzky, and Avi Wigderson. Semi-direct product in groups and zig-zag product in graphs: connections and applications. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 630–637. IEEE, 2001.

[AR94] Noga Alon and Yuval Roichman. Random cayley graphs and expanders. *Random Structures & Algorithms*, 5(2):271–284, 1994.

[Art] Michael Artin. Algebra.

[BATS11] Avraham Ben-Aroya and Amnon Ta-Shma. A combinatorial construction of almost-ramanujan graphs using the zig-zag product. *SIAM Journal on Computing*, 40(2):267–290, 2011.

[BL06] Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap*. *Combinatorica*, 26(5):495–519, 2006.

[CDP06] Samuel Cooper, Dominic Dotterrer, and Stratos Prassidis. Properties of the generalized zig-zag product of graphs. *arXiv preprint math/0607352*, 2006.

[Din07] Irit Dinur. The pcp theorem by gap amplification. *Journal of the ACM (JACM)*, 54(3):12, 2007.

[EM45] Samuel Eilenberg and Saunders MacLane. General theory of natural equivalences. *Transactions of the American Mathematical Society*, pages 231–294, 1945.

[F+03] Joel Friedman et al. Relative expanders or weakly relatively ramanujan graphs. *Duke Mathematical Journal*, 118(1):19–35, 2003.

[FT05] Joel Friedman and Jean-Pierre Tillich. Generalized alon–boppana theorems and error-correcting codes. *SIAM Journal on Discrete Mathematics*, 19(3):700–718, 2005.

[Gro77] Jonathan L Gross. Every connected regular graph of even degree is a schreier coset graph. *Journal of Combinatorial Theory, Series B*, 22(3):227–232, 1977.

[GT87] Jonathan L Gross and Thomas W Tucker. *Topological graph theory*. Courier Dover Publications, 1987.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, 2002.

[HL04] Ole J Heilmann and Elliott H Lieb. Theory of monomer-dimer systems. In *Statistical Mechanics*, pages 45–87. Springer, 2004.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.

[KB67] AN Kolmogorov and Ya M Barzdin. About realization of sets in 3-dimensional space. *Problems in Cybernetics*, 8(261-268):259–260, 1967.

[LP10] Nati Linial and Doron Puder. Word maps and spectra of random graph lifts. *Random Structures & Algorithms*, 37(1):100–135, 2010.

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[LR05] Nathan Linial and Eyal Rozenman. Random lifts of graphs: perfect matchings. *Combinatorica*, 25(4):407–424, 2005.

[Lub94] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125. Springer, 1994.

[Lub12] Alexander Lubotzky. Expander graphs in pure and applied mathematics. *Bulletin of the American Mathematical Society*, 49(1):113–162, 2012.

[McL03] Colin McLarty. *The rising sea: Grothendieck on simplicity and generality*. na, 2003.

[ML71] Saunders Mac Lane. Category theory for the working mathematician, 1971.

[Mot95] Rajeev Motwani. *Randomized algorithms*. Cambridge university press, 1995.

[MS95] Hirobumi Mizuno and Iwao Sato. Characteristic polynomials of some graph coverings. *Discrete mathematics*, 142(1):295–298, 1995.

[MSS13] Adam Marcus, Daniel A Spielman, and Nikhil Srivastava. Interlacing families i: Bipartite ramanujan graphs of all degrees. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 529–537. IEEE, 2013.

[Nik04] Nikolay Nikolov. On the commutator width of perfect groups. *Bulletin of the London Mathematical Society*, 36(01):30–36, 2004.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[Pin73] Mark S Pinsker. On the complexity of a concentrator. In *7th International Telegraffic Conference*, volume 4, pages 1–318. Citeseer, 1973.

[Pud12] Doron Puder. Expansion of random graphs: New proofs, new results. *arXiv preprint arXiv:1212.5216*, 2012.

[PV05] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on*, pages 285–294. IEEE, 2005.

[Rei08] Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM (JACM)*, 55(4):17, 2008.

[RSW06] Eyal Rozenman, Aner Shalev, and Avi Wigderson. Iterative construction of cayley expander graphs. *Theory OF Computing*, 2(1):91–120, 2006.

[RV05] Eyal Rozenman and Salil Vadhan. Derandomized squaring of graphs. In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques*, pages 436–447. Springer, 2005.

[RVW02] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Annals of Mathematics*, pages 157–187, 2002.

[Ser77] Jean-Pierre Serre. Linear representations of finite groups. *New York*, 1977.

[Vad12] Salil P Vadhan. *Pseudorandomness*. Now, 2012.

[Val76] Leslie G Valiant. Graph-theoretic properties in computational complexity. *Journal of Computer and System Sciences*, 13(3):278–285, 1976.

APPENDIX A

Deferred proofs

PROPOSITION A.1. *Given a T-regular graph K on vertex set S, define the following mapping from objects and morphisms of $\textsc{Graphs}_S$ to objects and morphisms of $\textsc{Graphs}_{T\times T}$:*

$$G \mapsto G\textcircled{z}K, \quad (p : G \to H) \mapsto (q : G\textcircled{z}K \to H\textcircled{z}K) \text{ given by Proposition 4.35}$$

Then this defines a functor $\textsc{Graphs}_S \to \textsc{Graphs}_{T\times T}$.

PROOF. Clearly, the identity covering map is carried to itself by Proposition 4.35; so it remains to show that our supposed functor respects composition. Suppose we have an S-covering $p : G \to H$ and a R-covering $q : L \to G$, where permutations on the edges e of H induced by p are denoted by π, and permutations on the edges of G induced by q are denoted by μ. As before, we start with three edges of the following form:

$$k \xrightarrow{i \quad i'} k' \in E(K), \quad v \xrightarrow{k' \quad l'} w \in E(H), \quad l' \xrightarrow{j \quad j'} l \in E(K)$$

Then the covering p induces the edge $(v, s) \xrightarrow{k' \quad l'} (w, \pi_{v,k'}s) \in E(G)$. From this, the covering q induces the edge $(v, s, r) \xrightarrow{k' \quad l'} (w, \pi_{v,k'}s, \mu_{(v,s),k'}r) \in E(L)$.

Now consider the image of $p \circ q$ under our mapping; that is, the covering map $L\textcircled{z}K \to H\textcircled{z}K$ which Proposition 4.35 gives us from $p \circ q$. As we saw in the proof of the proposition, the permutation it induces on the edge $(v, k) \xrightarrow{(i,j) \quad (j',i')} (w, l) \in E(H\textcircled{z}K)$ is the permutation on $S \times R$ that $p \circ q$ induces on the k'-th edge out of v; as we just saw, this is exactly the permutation $(s, r) \mapsto (\pi_{v,k'}s, \mu_{(v,s),k'}r)$.

So we want to show that the permutation assigned on $(v, k) \xrightarrow{(i,j) \quad e \quad (j',i')} (w, l) \in E(H\textcircled{z}K)$ by composing the lifts we get from p and q individually is the same. Using the same observation as in the previous paragraph, p induces $\pi_{v,k'}$; this gets us to the edge $[(v, s), k] \xrightarrow{(i,j) \quad (j',i')} [(w, \pi_{v,k'}s), l] \in E(H\textcircled{z}K)$. Then, q induces the permutation $\mu_{(v,s),k'}$ on this edge. The end result is that the edge e is lifted by $(s, r) \mapsto (\pi_{v,k'}s, \mu_{(v,s),l'})$. Hence, the two lifts of $H\textcircled{z}K$ are the same! □

PROPOSITION A.2. *Suppose $p : G \to H$ is a labeled S-covering of T-regular two-way labeled digraphs, and K is a two-way labeled digraph on vertex set T. Then there is a natural labeled covering map $q : G\textcircled{s}K \to H\textcircled{s}K$.*

PROOF. Let's have an edge $v \xrightarrow{(k,i) \quad (k',i')} w \in E(H\textcircled{s}K)$ coming from the three edges

$$v \xrightarrow{k \quad l} u \in E(H), \; l \xrightarrow{i \quad i'} l' \in E(K), \; u \xrightarrow{l' \quad k'} w \in E(H)$$

Then for every $s \in S$ we have the lifts of the first edge $(v, s) \xrightarrow{k \quad l} (u, \pi_{v,k}s) \in E(G)$ and third edge $(u, \pi_{v,k}s) \xrightarrow{l' \quad k'} (w, \pi_{u,l'}\pi_{v,k}s) \in E(G)$. But this means that we have an edge

$$(v, s) \xrightarrow{(k,i) \quad (k',i')} (w, \pi_{u,l'}\pi_{v,k}s) \in E(G\textcircled{s}K)$$

The permutation $\pi_{u,l'}\pi_{v,k}$ is determined uniquely by $[(v, s), (k, i)]$, hence the above encodes the rotation map of the lift of $H\textcircled{s}K$ where the permutation on the (k, i)-th edge out of v is $\pi_{u,l'}\pi_{v,k}$. □

Proposition A.3. *For a multigraph G with maximum degree at most d, all roots of $\mu_G(x)$ are real and have absolute value $\leq 2\sqrt{d-1}$.*

Proof. We follow Heilmann and Lieb [**HL04**] closely, and translate their terminology in our language. They work with weighted simple graphs, so given a multigraph G, interpret it as a weighted simple graph where the weight of the edge (u, v) is the number of edges between u and v.

Let $W(u, v)$ be the weight on the edge between u and v; $W(u, v) \geq 0$ always, and is positive whenever there is an edge between u and v. A **dimer arrangement** $\mathcal{D}$ is a matching on G; the **weight** of a dimer arrangement is

$$W(\mathcal{D}) = \prod_{(i,j)\in\mathcal{D}} W(i, j)$$

which is the same as the contribution of the corresponding matching. Then the d-**dimer partition function** is

$$Z_d = \sum_{|\mathcal{D}|=d} W(\mathcal{D}),$$

i.e. the sum of the weights of all dimers on d edges, with the convention $Z_0 = 1$. This is exactly m_d for G. Using this, Heilmann and Lieb define the polynomial (equations (2.5a) and (2.7) in [**HL04**])

$$Q(G; x) = i^{-N} \sum_{d=0}^{\lfloor N/2 \rfloor} Z_d (xi)^{N-2d} = \sum_{d=0}^{\lfloor N/2 \rfloor} (-1)^d Z_d x^{N-2d}$$

which is exactly $\mu_G(x)$. Now, for every vertex u, define

$$W_u = \sum_{v\neq u} W(v, u) - \min\{W(v, u) \;\big|\; v \in G, W(v, u) > 0\}$$

and let $B_1' = \max W_u$, $B_1'' = \frac{1}{4} \max W(u, v)$, $B_1 = \max\{B_1', B_1''\}$. Then Theorems 4.2 and 4.3 from [**HL04**] tells us that $Q(G; x)$ is real-rooted, with all roots having absolute value at most $2\sqrt{B_1}$.

To finish the proof, we need to show that $B_1 \leq d - 1$. By construction of G, $\sum_{v\neq u} W(v, u) \leq d$ for every u, and $\min\{W(v, u) \;\big|\; v \in G, W(v, u) > 0\} \geq 1$ because our edge weights are integers; thus $B_1' \leq d - 1$. Moreover, $B_1'' \leq d/4$, so $B_1 \leq d - 1$, and we're done. □

Proposition A.4.

Proof. We get to

$$\mathbf{E}_s \left[\det(xI - A_s)\right] = \sum_{k=0}^{n} x^{n-k} \sum_{S\subset V(G), |S|=k} \sum_{\pi\in \mathrm{Sym}(S)} \mathbf{E}_s \left[(-1)^{|\pi|} \prod_{i\in S} (A_s)_{i,\pi(i)}\right]$$

by linearity of expectation, exactly as in the original proof. Here π is a permutation whose fixed points are precisely $V(G) - S$. But now, $(A_s)_{i,\pi(i)}$ is a sum of $A_{i,\pi(i)}$ independent uniformly random signs. By elementary probability this implies

$$\mathbf{E}_s \left[s_{i,\pi(i)}\right] = 0 \text{ and } \mathbf{E}_s \left[s_{i,\pi(i)}^2\right] = A_{i,\pi(i)}$$

Consequently, by independence the only terms that survive the expectation are the permutations on S in which all orbits are of size 2. The contribution of such a term is then the product of the $A_{i,\pi(i)}$, which is precisely the number of matchings using the edges $\{(i, \pi(i))\}_{i\in S}$ - so we get the matching polynomial again. □