Thesis Proposal

On the Expansion of Graphs

Pedro Paredes

November 2021

Abstract

A popular way of analyzing a graph is through properties of its associated matrices, such as the adjacency matrix or the Laplacian matrix. This type of *spectral analysis* has produced several insights with practical applications in diverse areas, including internet search, clustering and segmentation of data and many more. From a theoretical perspective, *spectral graph theory* is such a fundamental tool that its applications span virtually the whole field of theoretical computer science.

One of the many successes of this area is the notion of *graph expansion*. A graph is expanding if it is simultaneously sparse and highly connected (meaning that we need to remove a lot of edges to disconnect a large part of the graph.) Since being defined in the '70s, *expander graphs* have spawned a lot of research with many applications in mathematics, computer science and even physics.

In my thesis work so far I have focused on answering the following fundamental questions:

- How can we construct explicit (i.e. deterministically and efficiently) expanding graphs?
- What is the expansion of random graphs drawn from different distributions?
- How can we leverage expansion in other domains, such as coding theory or refutation of constraint satisfaction problems?

Contents

1 Introduction

1.1 Expansion and Regular Graphs

Consider an undirected n-vertex multigraph (self loops and multiple edges are allowed) $G = (V(G), E(G))$, $|V(G)| = n$ and for $v \in V(G)$ let's denote by $N(v)$ the set of neighbors of v. We say that G is a *d-regular graph* if all vertices have degree exactly d, meaning that for all $v \in V(G)$ we have $|N(v)| = d$. For sets of vertices $S, T \subseteq V$ we denote by $E(S,T)$ the set of edges that have one endpoint in S and one endpoint in T, formally $E(S,T) = \{(u,v) | u \in S, v \in T, (u,v) \in E(G)\}$. We also denote by $\overline{S} = V(G) \setminus S$ the complement of S. The *edge boundary* of a set S, denoted ∂S, is defined as the set of edges with one endpoint in S and one endpoint outside of S, or formally $\partial S = E(S, \overline{S})$.

Definition 1.1 (Edge Expansion Ratio)**.** The *edge expansion ratio* of G, denoted $h(G)$, is defined as:

$$h(G) = \min_{\substack{S \in V(G) \\ |S| \leqslant \frac{n}{2}}} \frac{|\partial S|}{|S|}.$$

Note that a disconnected graph has edge expansion ratio of 0, since if we take S to be the smallest connected component of the graph (which must contain at most half the vertices) the boundary of such set is empty. It is also easy to see that if a graph has maximum degree Δ then the edge expansion ratio is at most Δ, since for a set of vertices S the maximum number of edges with one endpoint in S is at most $\Delta \cdot |S|$.

We can study the edge expansion ratio of any graph, but as we will see later, it is especially interesting to look at the case of sparse graphs. To do so we will consider d-regular graphs, since if we think of d as a constant but n going to infinity, then the resulting family of graphs is sparse. We choose to fix the degree of all vertices because on one hand this will introduce extra constraints to the problems we study (and thus, it will only make them harder to solve), but on the other hand it is nicer to analyze the regular case. Additionally, there are many theoretical applications where fixing the degree is actually important. So this motivates the following definition:

Definition 1.2 (Family of Edge Expander Graphs)**.** An infinite sequence of d-regular graphs $\{G_i\}_{i \in \mathbb{N}}$ of vertex set size increasing with i is said to be a *family of edge expander graphs* if there is a constant $\varepsilon > 0$ such that $h(G_i) \geqslant \varepsilon$ for all i.

This definition is motivated by our initial informal description of expanders as "sparse and highly connected". The sparseness comes from our use of d-regular graphs. As for being highly connected, notice that if we want to disconnect a set S of vertices from the rest of the graph we need to remove at least $\varepsilon|S|$ edges.

Let's now consider a different way of characterizing expansion, through spectral properties of graphs. The adjacency matrix A_G of G is the matrix with rows and columns indexed by the vertices of G, where for $u, v \in V(G)$, $(A_G)_{uv}$ is equal to the number of occurrences of the edge $\{u, v\}$ in $E(G)$. Given a vector $f : V(G) \to \mathbb{R}$, we have that $(A_G f)_v = \sum_{v \sim u} A_{vu} f_u$, where $\sim$ denotes adjacency between vertices. Since we are assuming that G is undirected, A_G is a real symmetric matrix and thus the spectral theorem tells us that there are n real *eigenvalues* with corresponding orthogonal *eigenvectors*. We order the eigenvalues and denote them by $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$.

The largest eigenvalue λ_1 is known as the *trivial eigenvalue* and it is always equal to d, since the vector $\phi_1 = \mathbf{1}/\sqrt{n} = (1/\sqrt{n}, \ldots, 1/\sqrt{n})$ satisfies $A_G\phi_1 = d\phi_1$. It is also known that the smallest eigenvalue λ_n satisfies $\lambda_1 \geqslant -\lambda_n$ (this follows from the Perron-Frobenius theorem).

Definition 1.3 (Spectral Expansion)**.** The *spectral expansion* of G, denoted $\lambda(G)$, is defined as:

$$\lambda(G) = \max\{\lambda_2, |\lambda_n|\}.$$

And, as we did before, we can define a family of spectral expander graphs.

Definition 1.4 (Family of Spectral Expander Graphs)**.** An infinite sequence of d-regular graphs $\{G_i\}_{i\in\mathbb{N}}$ of vertex set size increasing with i is said to be a *family of spectral expander graphs* if there is a constant $\delta > 0$ such that $h(G_i) \leqslant (1-\delta)d$ for all i.

The aforementioned properties of A_G imply that $\lambda(G)$ is a real number between 0 and d. If the graph G is disconnected then we can show that $\lambda_2 = d$, which means $\lambda(G) = d$. Indeed, consider two connected components C_1 and C_2 and let v_1 be the vector with ones on the elements corresponding to vertices in C_1 and v_2 be the vector with ones on the elements corresponding to vertices in C_2. These two vectors are orthogonal but both satisfy $A_G v_i = dv_i$. Conversely, if G is a complete graph then all eigenvalues except λ_1 are -1, so $\lambda(G) = 1$. This suggests a similar behavior to the edge expansion ratio, where if a graph is disconnected then $\lambda(G)$ is large (and $h(G)$ is small) and if a graph is highly connected then $\lambda(G)$ is small (and $h(G)$ is large), hence why $\lambda(G)$ is known as spectral expansion. This connection can be made quantitative through what is known as *Cheeger's Inequality*, which was originally proved by Dodziuk [Dod84] and independently by Alon and Milman [AM85].

Theorem 1.5 (Cheeger's Inequality)**.**

$$\frac{d-\lambda_2}{2} \leqslant h(G) \leqslant \sqrt{2d(d-\lambda_2)}.$$

Another way to interpret how $\lambda(G)$ governs the expansion of a graph is through the *Expander Mixing Lemma*, which was first proved by Alon and Chung [AC88].

Lemma 1.6 (Expander Mixing Lemma)**.** *For all $S, T \subseteq V$':*

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leqslant \lambda(G)\sqrt{|S||T|}.$$

We can interpret this lemma in two ways. First, by considering $T = \overline{S}$ we recover another connection between $\lambda(G)$ and $h(G)$. Second, the quantity $d|S||T|/n$ is the expected number of edges between S and T in a random graph of density d/n. So this lemma tells us that in a spectral expanding graph all pairs of sets of vertices have a number of crossing edges close to what is expected in a random graph. This property motivates calling expander graphs *pseudorandom* and indeed the Expander Mixing Lemma finds many applications in the theory of pseudorandomness.

A natural question that follows from the above is: how small can $\lambda(G)$ be? This fundamentally asks what is the optimal spectral expander. The answer is given by the well-known *Alon-Boppana bound*, which was shown in a series of works [Alo86, Nil91, Fri93], that says:

Theorem 1.7 (Alon-Boppana Bound)**.**

$$\lambda_2 \geqslant 2\sqrt{d-1} - O\left(\frac{1}{\log^2 n}\right).$$

This shows that $2\sqrt{d-1}$ is essentially a lower bound to the spectral expansion and hence it leads to the following definition of optimal spectral expanders.

Definition 1.8 (Ramanujan Graphs)**.** A d-regular (multi)graph G is called *(two-sided) Ramanujan* whenever $\lambda(G) \leqslant 2\sqrt{d-1}$. When we merely have $\lambda_2 \leqslant 2\sqrt{d-1}$, we call G *one-sided Ramanujan*.

Now the question of *explicit constructions* of such graphs arises. By explicit we mean that there is a deterministic and efficient algorithm to generate such a graph. However, we can define efficiency in different ways.

Definition 1.9 (Explicit Constructions)**.** We define the following three notions of explicitness:

- An algorithm is *weakly explicit* if given integers n and d, it generates an n-vertex d-regular Ramanujan graph in time polynomial in n.
- An algorithm is *strongly explicit* if given integers n and d, it generates a representation A of an n-vertex d-regular Ramanujan graph such that: when given as input a vertex $v \in \{1, \ldots, n\}$ and a neighbor $i \in \{1, \ldots, d\}$, there is an algorithm that computes the ith neighbor of v in $\text{polylog}(n)$ time.
- An algorithm is *probabilistically strongly explicit* if given integers n and d and a seed $s \in \{0,1\}^{O(\log n)}$, it generates a representation A of an n-vertex d-regular graph that is Ramanujan with high probability over the choice of seed s and such that: when given as input a vertex $v \in \{1, \ldots, n\}$ and a neighbor $i \in \{1, \ldots, d\}$, there is an algorithm that computes the ith neighbor of v in $\text{polylog}(n)$ time.

Our discussion so far justifies the first fundamental question that this thesis is centered around:

Question 1.10. How can we construct an explicit Ramanujan graph with n vertices and degree d, for all degrees d and high enough n?

Let's review what was known about this before this thesis. Margulis [Mar73] was the first to provide an explicit expander family; a slight variant of it, which is 8-regular, was shown [GG81] to have $\lambda \leqslant 5\sqrt{2} \approx 7.1$ (see [HLW06]).

Using the resolution of the Ramanujan–Petersson conjectures in various number-theoretic settings, it is possible to construct d-regular expander families that meet the bound $\lambda(G) \leqslant 2\sqrt{d-1}$ for some values of d. The case when $d-1$ is an odd prime is due to Ihara [Iha66] (implicitly) and to Lubotzky–Phillips–Sarnak [LPS88] and Margulis [Mar88] (independently); the $d-1=2$ case is by Chiu [Chi92]; and, the general prime power case is due to Morgenstern [Mor94]. For extensions to general d where the eigenvalue bound depends on the number of distinct prime divisors of $d-1$, see [Piz90, Cla06]. We summarize these result in the following theorem.

Theorem 1.11. *([Mor94].) For any $d \geqslant 3$ with $d-1$ a prime power, there is a strongly explicit family of d-regular Ramanujan graphs.*

For all other values of d — e.g., for $d = 7$ — it is unknown if infinite families of d-regular Ramanujan graphs exist. A natural question then is whether, for every d, one can achieve explicit graph families that are "ε-near-Ramanujan". In their work introducing the *zig-zag product*, Reingold–Vadhan–Wigderson [RVW02] asked whether explicit families could at least reach a bound of $O(\sqrt{d})$; towards this, their work gave strongly explicit families with $\lambda(G) \leqslant O(d^{2/3})$. By extending their approach, Ben-Aroya and Ta-Shma reached $d^{1/2+o(1)}$:

Theorem 1.12. *([RVW02, BT11].) There are strongly explicit families of d-regular multigraphs G satisfying the bound $\lambda(G) \leqslant \sqrt{d} \cdot 2^{O(\sqrt{\log d})}$.*

Bilu and Linial [BL06] got even closer to $O(\sqrt{d})$, using a new approach based on random *lifts* (which we will define later.) Their graph families are not strongly explicit, although Bilu–Linial showed that they are at least probabilistically strongly explicit.

Theorem 1.13. *([BL06].) There are probabilistically strongly explicit families of d-regular multigraphs G satisfying the bound $\lambda(G) \leqslant \sqrt{d} \cdot O(\log^{1.5} d)$.*

Cioabă and Murty [CM08] described the following idea (cf. [dlHM06]): take a prime (or prime power) $q < d - 1$, form a $(q+1)$-regular Ramanujan graph, and then add in $d - q - 1$ arbitrary perfect matchings. It is shown in [CM08] that each perfect matching increases $\lambda(G)$ by at most 1. Hence:

Theorem 1.14. *([CM08].) For any $d \geqslant 3$, there is a strongly explicit family of d-regular multigraphs with $\lambda(G) \leqslant 2\sqrt{d-1} + gap(d)$, where $gap(d)$ denotes the least value g such that $d - 1 - g$ is a prime (power). One can bound $gap(d)$ by $O(\log^2 d)$ under Cramér's conjecture, by $O(\sqrt{d} \log d)$ under the Riemann Hypothesis, or by $O(d^{.525})$ unconditionally.*

Finally, Marcus–Spielman–Srivastava [MSS15a, MSS15b] introduced the *Interlacing Polynomials Method* and used it to show that *one-sided bipartite* Ramanujan graphs exist for all $d \geqslant 3$ and all even n. Their proof was merely existential, but Cohen [Coh16] was able to make it explicit (though not strongly so):

Theorem 1.15. *([MSS15a, MSS15b, Coh16].) For any $d \geqslant 3$, there is an weakly explicit family of one-sided bipartite, d-regular, Ramanujan multigraphs.*

This summarizes the story of explicit constructions of spectral expanders and Ramanujan graphs. A natural follow up question is to ask how is expansion distributed over random graphs of different distributions. This is exactly what this thesis' second fundamental question asks.

Question 1.16. What is the spectral expansion of random graphs drawn from different distributions?

The most well-known result of this nature is related to the behavior of uniformly random regular graphs. Alon [Alo86] conjectured that a random n-vertex d-regular graph $\boldsymbol{G}$ has $\lambda(\boldsymbol{G}) \leqslant 2\sqrt{d-1} + o_n(1)$ with high probability, and this was proven two decades later by Friedman [Fri08] and later a simpler proof was given by Bordenave [Bor19].

Theorem 1.17. *([Fri08].) Fix any $d \geqslant 3$ and $\varepsilon > 0$ and let $\boldsymbol{G}$ be a uniformly random d-regular graph. Then*

$$\mathbf{Pr}\left[\lambda(\boldsymbol{G}) \leqslant 2\sqrt{d-1} + \varepsilon\right] \geqslant 1 - o_n(1).$$

In fact [Bor19], $\boldsymbol{G}$ achieves the subconstant $\varepsilon = \widetilde{O}(1/\log^2 n)$ with probability at least $1 - 1/n^{.99}$.

Given all of the above, the final fundamental question is:

Question 1.18. How can we leverage expansion in other domains, such as coding theory or refutation of constraint satisfaction problems?

It would be impossible to summarize all of the applications of expander graphs. We recommend the surveys of Hoory-Linial-Wigderson [HLW06] and Kowalski [Kow19] for a comprehensive list of applications and connections of Ramanujan graphs and expanders to computer science and mathematics.

1.2 Overview of Completed Work

Throughout this thesis we will attempt to answer the three fundamental questions in different ways. Here is a summary of our contributions so far:

- To answer Question 1.10, we devise an explicit construction of nearly optimal expanding regular graphs of all degrees. We also show how to use this result to obtain nearly optimal expanding graphs with high girth (i.e. that do not contain small cycles).
- To answer Question 1.16, we analyze the expansion of several types of different random graph distributions based on graphs products, like random additive lifts and random abelian lifts.
- To answer Question 1.18, we show how to analyze the SDP value of a family of random constraint satisfaction problems (CSPs) and also show how to construct explicit nearly linear distance quantum low density parity check (LDPC) error correcting codes in polynomial time.

All of these results are related and were developed over a series of four papers. We devote Section 3 to [MOP20a], Section 4 to [MOP20b], Section 5 to [Par21] and finally Section 6 to [JMO+22]. For each of these we will first introduce some motivation and background, then summarize the results of the paper and end with mentioning follow-up open problems. But before we do so, we will introduce some notation and general background on Section 2, which will be useful for the remaining sections. We will end this thesis document by mentioning some extra related open problems on Section 7.

2 Background

2.1 Random Models of Regular Graphs

Definition 2.1 (Excess)**.** Given a multigraph $H = (V, E)$, its *excess* is $\mathrm{exc}(H) = |E| - |V|$.

We can think of excess as the minimum number of edges we can remove from our graph to obtain a tree.

Definition 2.2 (A/uni/bi-cyclic)**.** A connected multigraph H with $\mathrm{exc}(H) = -1, 0, 1$ (respectively) is said to be *acyclic*, *unicyclic*, *bicyclic* (respectively). In either of the first two cases, we call H *bicycle-free* (or *at most unicyclic*).

Definition 2.3 (Bicycle-free at radius r)**.** We say a multigraph is *bicycle-free at radius r* if the distance-r neighborhood of every vertex is bicycle-free. Another way to say this is that a breadth-first search of depth r, started at any vertex, encounters at most one "back-edge".

The first regulargraph model we define is the following.

Definition 2.4 (Graph lift)**.** Fix a *base* graph $\underline{G} = (\underline{V}, \underline{E})$. Then for $n \in \mathbb{N}^+$, an *n-lift of $\underline{G}$* is graph G defined by a collection of permutations $\pi_{uv} \in \mathrm{Sym}(n)$, one for each edge $(u,v) \in \vec{\underline{E}}$, under the constraint that $\pi_{uv} = \pi_{vu}^{-1}$. The vertex set of G is $\underline{V} \times [n]$, and the edges of G are given by all pairs $(u,i),(v,j)$ satisfying $(u,v) \in \underline{E}$ and $\pi_{uv}(i) = j$. When the permutations π_{uv} are independent and uniformly random, we call the associated graph $\boldsymbol{G}$ a *(uniformly) random n-lift of $\underline{G}$*.

A simple observation is that if $\underline{G}$ is a d-regular graph, then any graph lift of $\underline{G}$ is a d-regular graph on $|V(\underline{G})|n$ vertices. An important case of the lift model is the one of *2-lifts*. An equivalent way of defining a 2-lift is by considering an edge-signing $w : \underline{E} \to \{\pm 1\}$ of $\underline{G}$. This edge-signing uniquely defines a 2-lift of $\underline{G}$, which we can describe in the following way:

$$V = \underline{V} \times \{\pm 1\}, \qquad E = \Big\{\{(u,\sigma),(v,\sigma \cdot w(u,v))\} : (u,v) \in \underline{E}, \sigma \in \{\pm 1\}\Big\}.$$

The following was first observed by Bilu and Linial [BL06]:

Lemma 2.5. *Let $\underline{G}$ be a d-regular graph, $w : \underline{E} \to \{\pm 1\}$ an edge-signing and $\widetilde{\underline{G}}$ the signed version of $\underline{G}$ (meaning the graph such that its adjacency matrix has nonzero entries $w(u,v)$ when $\{u,v\} \in \underline{G}$). Then the corresponding 2-lift G satisfies:*

$$\mathrm{Spec}(A_G) = \mathrm{Spec}(A_{\underline{G}}) \cup \mathrm{Spec}(A_{\widetilde{\underline{G}}}).$$

We can now define our second regular graph model.

Definition 2.6 (Configuration model)**.** Given integers $n > d > 0$ with nd even, the *configuration model* produces a random n-vertex, d-regular undirected multigraph (with loops) $\boldsymbol{G}$. This multigraph is induced by a uniformly random matching $\boldsymbol{M}$ on the set of "half-edges", $[n] \times [d] \cong [nd]$ (where $(v,i) \in [n] \times [d]$ is thought of as half of the ith edge emanating from vertex v). We identify $\boldsymbol{M}$ with a symmetric matrix in $\{0,1\}^{nd \times nd}$ having 1's precisely in the entries corresponding to matched pairs $\{(v,i),(v',i')\}$. We may think of $\boldsymbol{M}$ being generated as follows: First a uniformly random permutation $\boldsymbol{\pi} \in S_{nd}$ is chosen; then we set $\boldsymbol{M}_{\boldsymbol{\pi}(j),\boldsymbol{\pi}(j+1)} = \boldsymbol{M}_{\boldsymbol{\pi}(j+1),\boldsymbol{\pi}(j)} = 1$ for each odd $j \in [nd]$.

Given $\boldsymbol{M}$, the multigraph $\boldsymbol{G}$ is formed by "attaching" the matched half-edges. More formally, the (v,v')-entry of $\boldsymbol{G}$'s adjacency matrix $\boldsymbol{A}$ is the sum, over all $i,i' \in [d]$, of $\boldsymbol{M}_{(v,i),(v',i')}$. Hence

$$\boldsymbol{A}_{v,v'} = \sum_{i,i'=1}^{d} \sum_{\substack{\text{odd} \\ j \in [nd]}} (1[\boldsymbol{\pi}(j) = (v,i)] \cdot 1[\boldsymbol{\pi}(j+1) = (v',i')] + 1[\boldsymbol{\pi}(j) = (v',i')] \cdot 1[\boldsymbol{\pi}(j+1) = (v,i)]).$$

Note that $\boldsymbol{A}_{v,v}$ will always be even; a self-loop is considered to contribute degree 2.

It is well known that a graph $\boldsymbol{G}$ drawn from the configuration model is simple [Wor99] — i.e., has no cycles of length 1 or 2 — with probability $\Omega_d(1)$, this continues to hold for *pseudorandom*

d-regular graphs (to be defined later.) We also record the well known fact that for $\boldsymbol{G}$ drawn from the configuration model, when $\boldsymbol{G}$ is conditioned on being simple, its conditional distribution is uniformly random among all d-regular graphs.

It is easy to see that any n-vertex, d-regular graph that is bicycle-free at radius r must have $r \lesssim \log_{d-1} n$ (this also holds in the configuration model.) On the other hand, it can be shown (see, for example, [Bor19]) that a random d-regular graph achieves this bound up to a constant factor.

2.2 The Trace Method and Non-Backtracking Walks

A common tool to bound the largest eigenvalue of a symmetric matrix is the Füredi-Komlós Trace Method [FK81]. Let H be a $n \times n$ symmetric real matrix and denote its eigenvalues by $\lambda_1 \geqslant \ldots \geqslant \lambda_n$. Then, for any integer k, it is a standard fact that $\sum_{i=1}^{n} \lambda_i^k = \operatorname{tr}(H^k)$. If k is an even integer, we have that $\lambda_1^k \leqslant \operatorname{tr}(H^k)$. Suppose we can bound the any element of the diagonal of H^k by $a(k)$. The idea of the Trace Method is to take $k \gg \log n$ to conclude that $\lambda_1 \leqslant n^{1/k} a(k)^{1/k} = (1 + o_n(1)) a(k)^{1/k}$.

Using the Trace Method to analyze eigenvalues of graphs involves counting closed walks in them, since powers of the adjacency matrix correspond to walks and the elements in the diagonal correspond to walks that start and end at the same vertex. To do so, it is common to instead count *non-backtracking* walks, since these are much easier to count. Hence, we define the *non-backtracking matrix*.

Definition 2.7 (Non-backtracking matrix [Has89])**.** Let $G = (V, E)$ be a multigraph with adjacency matrix A. Let $\vec{E}$ denote the (multi)set of all directed edges formed by replacing each undirected edge in E with two opposing directed edges. Then G's *non-backtracking* matrix B has rows and columns indexed by $\vec{E}$, with

$$B_{(u_1,v_1),(u_2,v_2)} = \begin{cases} A_{u_2,v_2} & \text{if } v_1 = u_2 \text{ and } v_2 \neq u_1, \\ 0 & \text{otherwise.} \end{cases}$$

Ultimately, we need to map between eigenvalues of this matrix B and the adjacency matrix A. In a number-theoretic context, Ihara [Iha66] implicitly showed how to do so when the graph G is regular. Serre [Ser77] and several others suggested the translation to graph theory, and Bass [Bas92] (following [Has89]) explicitly established:

Theorem 2.8. *(Ihara–Bass formula.) Let G be a d-regular (multi)graph and write $q = d - 1$. Then*

$$\det(\mathbb{1} - zB) = (1 - z^2)^{\operatorname{exc}(G)-1} \det((1 + qz^2)\mathbb{1} - zA),$$

where $\mathbb{1}$ denotes the identity matrix (of appropriate dimension).

This theorem has been given many proofs, and it can be generalized to irregular graphs, edge-weighted graphs, and infinite graphs. We can use this formula to convert result about the spectrum of B into results about A. For our purposes we will only use this lemma to analyze eigenvalues of the form $\lambda = 2\sqrt{d-1} + \epsilon$ (the Ramanujan bound), so the following corollary (appearing in [Bor19]) will be useful:

Corollary 2.9. *Let $G = (V, E)$ be a d-regular graph ($d \geqslant 3$) with adjacency matrix A and non-backtracking matrix B. If A has an eigenvalue of magnitude $2\sqrt{d-1} + \varepsilon$ (for $\varepsilon \geqslant 0$) then B has an eigenvalue of magnitude $\sqrt{d-1} + \sqrt{\varepsilon}\sqrt{\sqrt{q} + \varepsilon/4} + \varepsilon/2$ (which is $\sqrt{d-1} + \Theta(d^{1/4}\sqrt{\varepsilon})$ for fixed d and $\varepsilon \to 0$).*

2.3 Standard Derandomization Tools

Here we briefly introduce two derandomization tools we will refer to later.

Definition 2.10 ((δ, k)-wise uniform bits)**.** Let $\delta \in [0,1]$ and $k \in \mathbb{N}^+$. A sequence of Boolean random variables $\boldsymbol{y} = (\boldsymbol{y}_1, \dots, \boldsymbol{y}_n) \in \{\pm 1\}^n$ is said to be (δ, k)*-wise uniform*[1] if, for every $S \subseteq [n]$ with $0 < |S| \leqslant k$, it holds that $|\mathbf{E}[\prod_{i \in S} \boldsymbol{y}_i]| \leqslant \delta$. When $\delta = 0$, we simply say that the sequence is *(truly) k-wise uniform*; indeed, in this case the bits are individually uniformly distributed and are k-wise independent.

Definition 2.11 ((δ, k)-wise uniform permutations)**.** Let $\delta \in [0,1]$ and $k \in \mathbb{N}^+$. Let $[n]_k$ denote the set of all sequences of k distinct indices from $[n]$. A random permutation $\boldsymbol{\pi} \in S_n$ is said to be (δ, k)*-wise uniform* if, for every sequence $(i_1, \dots, i_k) \in [n]_k$, the distribution of $(\boldsymbol{\pi}(i_1), \dots, \boldsymbol{\pi}(i_k))$ is δ-close in total variation distance from the uniform distribution on $[n]_k$. When $\delta = 0$, we simply say that the permutation is *(truly) k-wise uniform*.

3 2-Lifts and Explicit Near-Ramanujan Graphs

3.1 Overview

In this section we describe the results of [MOP20a], which was joint work with Sidhanth Mohanty and Ryan O'Donnell. In this paper we show how to construct near-Ramanujan graphs in a probabillistically strongly explicit way. More formally, the main theorem says the following:

Theorem 3.1 ([MOP20a])**.** *There is a deterministic polynomial-time (in the input length) algorithm with the following properties:*

- *It takes as input N, $d \geqslant 3$, and $\varepsilon > 0$ written as binary strings.*
- *It also takes as input a "seed" $s \in \{0,1\}^{O(\log N)}$ (the $O(\cdot)$ hides a factor of $O(d^{1/4}\log(d)/\sqrt{\varepsilon})$).*
- *It outputs a Boolean circuit C that implements the "adjacency list" of a d-regular graph G on $N' \sim N$ vertices in $\mathrm{polylog}(N)$ time. (This means that on input $u \in [N']$ and $i \in [d]$, both expressed in binary, $C(u,i)$ outputs the $v \in [N']$ that is the ith neighbor of u in G.)*
- *With high probability over the choice of seed s, the resulting graph G satisfies the bound $\lambda(G) \leqslant 2\sqrt{d-1} + \varepsilon$.*

Our proof has two parts. First, we weakly derandomize Bordenave's proof of Theorem 1.17 to produce a small d-regular near Ramanujan graph, using standard derandomization tools. Additionally, we show how to make this small graph be bicycle-free at a large enough radius. Then, we show that a random 2-lift of a graph that is bicycle-free at such a radius is also near-Ramanujan, which we also derandomize. Finally, by iterating this procedure we are able to obtain a near-Ramanujan graph of the desired size.

[1] Frequently called (δ, k)-wise *independent* in the literature.

3.2 2-Lifting a Base Graph

Let $G = (V, E)$ be an n-vertex d-regular graph, and let $\widetilde{G}$ be the edge-signed version of it associated to edge-signing $w : E \to \{\pm 1\}$. Recall that this edge-signing is in a sense equivalent to the "2-lift" $G_2 = (V_2, E_2)$ of G defined by

$$V_2 = V \times \{\pm 1\}, \qquad E_2 = \Big\{ \{(u,\sigma),(v,\sigma \cdot w(u,v))\} : (u,v) \in E \Big\}.$$

This G_2 is a $2n$-vertex d-regular graph, and the equivalence is that G_2's eigenvalues are precisely the multiset-union of G's eigenvalues and $\widetilde{G}$'s eigenvalues. (The latter refers to the eigenvalues of $\widetilde{G}$'s signed adjacency matrix, whose nonzero entries are $w(u,v)$ for each $\{u,v\} \in E$.) In particular, if all the eigenvalues of G and $\widetilde{G}$ have magnitude at most $2\sqrt{d-1} + \varepsilon$ (excluding G's trivial eigenvalue of d), then the same is true of G_2 (excluding *its* trivial eigenvalue.) So this motivates the main technical theorem.

Theorem 3.2. *Let $G = (V, E)$ be an arbitrary d-regular n-vertex graph, where $d \leqslant \mathrm{polylog} n$. Assume that G is bicycle-free at radius $r \gg (\log\log n)^2$. Then for $\boldsymbol{G}$ a uniformly random edge-signing of G, except with probability at most n^{-100} the non-backtracking matrix $\boldsymbol{B}$ of $\boldsymbol{G}$ satisfies the spectral radius bound*

$$\rho(\boldsymbol{B}) \leqslant \sqrt{d-1} \cdot \left(1 + O\left(\frac{(\log\log n)^2}{r}\right)\right),$$

and hence (by a version of Corollary 2.9) the signed adjacency matrix $\boldsymbol{A}$ of $\boldsymbol{G}$ satisfies the bound

$$\rho(\boldsymbol{A}) \leqslant 2\sqrt{d-1} \cdot \left(1 + O\left(\frac{(\log\log n)^4}{r^2}\right)\right).$$

Furthermore, let $C = C(n)$ satisfy $1 \leqslant C \leqslant \mathrm{polylog} n$ and suppose we merely assume that the random edge-signs are (δ, k)-wise uniform for $\delta \leqslant n^{-O(C \log d)}$ and $k \geqslant 2C \log n$. Then the above bounds continue hold, with an additional additive $O(\sqrt{d}/C)$ in the $\rho(\boldsymbol{B})$ bound and $O(\sqrt{d}/C^2)$ in the $\rho(\boldsymbol{A})$ bound.

Thus Theorem 3.2 can provide us with a (derandomizable) way of doubling the number of vertices in an ε-near-Ramanujan graph. It is not hard to see that if G is r-bicycle-free then G_2 will also be r-bicycle-free, thus we can apply this theorem repeatedly once we have an appropriate base graph.

3.3 Generating a Base Graph

Given the result of last section, our base graph should be some d-regular ε-near-Ramanujan graph H on a smaller number of vertices, n, which is $O((\log\log N)^2)$-bicycle-free. Thanks to Friedman/Bordenave, we know that a *random* d-regular n-vertex graph is (with high probability) near-Ramanujan (see Theorem 1.17), and it's not hard to show it's $\Theta(\log n)$-bicycle-free. Thus we could get started with H being a random d-regular graph on, say, $n = 2^{\sqrt{\log N}}$ vertices, or even something smaller like $n = \mathrm{quasipoly}(\log\log N)$.

Of course, to get a construction which is overall explicit, we need to derandomize the Friedman/Bordenave analysis for this base graph H. The advantage is we now have $\mathrm{poly}(N)$ time to spend on constructing a graph with $n \ll N$ vertices. A trivial exponential-time derandomization won't work, but nor do we need a polynomial-time derandomization; a quasipolynomial-time derandomization is more than sufficient. So we prove the following lemma:

Theorem 3.3. *Fix $3 \leqslant d \leqslant C^{-1}\sqrt{\log n}$ and let $\varepsilon \leqslant 1$ and k satisfy*

$$\varepsilon \geqslant C^3 \cdot \left(\frac{\log\log n}{\log_{d-1} n}\right)^2, \qquad k \geqslant C\log(n)/\sqrt{\varepsilon}.$$

Let $\boldsymbol{G}$ be chosen as a d-regular k-wise uniform random n-lift of K_{d+1}. Then except with probability at most $1/n^{.99}$, the following hold:

- *$\boldsymbol{G}$ is bicycle-free at radius $c\log_{d-1} n$;*
- *$\lambda(\boldsymbol{G}) \leqslant 2\sqrt{d-1}\cdot(1+\varepsilon)$.*

Finally, by known derandomization results, these statements remains true for n-lifts over (δ, k)-wise uniform permutations, $\delta \leqslant 1/n^{8k+1}$.

3.4 Near-Ramanujan Graphs

Recall we want to show there is a deterministic algorithm that on input $N, d \geqslant 3$ and $\varepsilon > 0$, outputs in $\mathrm{poly}(N)$-time a d-regular graph G on $N' \sim N$ vertices with $\lambda(G) \leqslant 2\sqrt{d-1}+\varepsilon$. Here is a brief outline of how to prove Theorem 3.1:

1. Using Theorem 3.3 we construct a d-regular simple graph G_0 on some "small" number of vertices $n_0 = n_0(N)$, which is bicycle-free at radius $\Omega(\log n_0)$ and has $\lambda(G_0) \leqslant 2\sqrt{d-1}+\epsilon$. The quantity n_0 should satisfy

$$2^{\omega((\log\log N)^2)} \leqslant n_0 \leqslant 2^{O(\sqrt{\log N})},$$

   the left inequality so that G_0 is sufficiently bicycle-free for Step 2 below, and the right inequality so that G_0 is constructible in deterministic $\mathrm{poly}(N)$ time.

2. Next we repeatedly use Theorem 3.2 (roughly $\log(N/n_0) \sim \log N$ times) to double the number of vertices in our construction from Step 1, while keeping $\lambda \leqslant 2\sqrt{d-1}+\epsilon$ and also retaining that the graph is bicycle-free at radius $\Omega(\log n_0)$. Importantly, since Theorem 3.2 is a high-probability result, we will be able to reuse the seed for each of the $\log N$ pseudorandom edge-signings.

3.5 Future Directions and Open Problems

There are many open problems and possible future directions related to this area, we summarize a few.

Open Question 3.4. Can we build on these results to obtain near-Ramanujan graphs with other combinatorial properties (e.g. high girth)?

For a lot of applications of expander graphs it is important that the expander also has extra combinatorial properties. An example of such a property is high girth, which has implications in the decodability of some families of error correcting codes. We will see more about this in Section 5.

Open Question 3.5. Can we obtain a combinatorial strongly explicit construction of near-Ramanujan graphs?

The zig-zag product of Reingold-Vadhan-Wigderson [RVW02] is the only known *combinatorial* construction of strongly explicit expander graphs. It would be interesting to find other strongly explicit constructions with better expansion, perhaps based on the results of this section.

Open Question 3.6. Are there explicit Ramanujan graphs of all degrees d?

The "Holy Grail" of expander graphs would be to find an explicit construction of Ramanujan graphs for all degrees d. Even the existence of such graphs is open (even though we know how to construct one-sided Ramanujan graphs of all degrees).

4 Additive Lifts and Two-Eigenvalue Graphs

4.1 Overview

In this section we describe the results of [MOP20b], which was joint work with Sidhanth Mohanty and Ryan O'Donnell. In this paper we determine the SDP value of large random instances of certain kinds of constraint satisfaction problems, "two-eigenvalue 2CSPs".

Refutation of constraint satisfaction problems (CSPs) is a fundamental problem in complexity theory. Given a CSP formula, refutation is the task of providing a proof that no assignment achieves some larger value. In the theory of algorithms and complexity, the most difficult instances of a given CSPs are arguably random (sparse) instances. Indeed, the assumed intractability of random CSPs underlies, for example, various cryptographic proposals for one-way functions [Gol00, JP00].

Given, say, a random Max-Cut instance of average degree d, its optimum value is (whp) concentrated around $\frac{1}{2} + f(d)$, where f is a certain function of d. However, the most efficient algorithms we know can only find (whp) cuts of value approximately $\frac{1}{2} + .83f(d)$ the optimal one. This suggests an "information-computation" gap. One way to study this is through the behavior of semidefinite programming (SDP) relaxations, which are the most popular and successful approaches to refuting CSPs. Given an instance of a CSP, we call the exact threshold result for when the natural SDP algorithm is able to certify unsatisfiability the *SDP value of the instance*.

We precisely determined the SDP value of large random instances of certain kinds of constraint satisfaction problems, which are known as "two-eigenvalue 2CSPs". Briefly, these are CSPs where each clause can be described by a graph where each vertex represents a variable and each edge is an XOR constraint between two variables, and such that the spectrum of the adjacency matrix of the graph only contains two distinct eigenvalues. This includes multiple famous CSPs families like the NAE-3SAT, the SORT_4 and the $\mathrm{Forrelation}_k$ CSPs. Formally, we prove the following theorem.

Theorem 4.1. *For random c-constraint-regular instances of a CSP with 2 distinct eigenvalues λ_1 and λ_2, the SDP value is in the range*

$$\frac{\lambda_1 + \lambda_2 + 2\sqrt{(c-1)(-\lambda_1\lambda_2)}}{c(-\lambda_1\lambda_2)} \pm \varepsilon$$

with high probability, for any $\varepsilon > 0$.

To establish this result we had to analyze the spectral expansion of a distribution of graphs that generalizes uniformly random regular graphs. To do so we generalized well known concepts like the nonbacktracking operator, the Ihara-Bass Formula, and the Friedman/Bordenave proof of Alon's Conjecture.

4.2 Preliminaries

All of the CSPs we studied (Max-Cut, NAE-3SAT, Sort_4, $\mathsf{Forrelation}_k$, etc.) will effectively reduce to 2XOR *optimization problems* — equivalently, the problem maximizing a homogeneous degree-2 polynomial with ± 1 coefficients over the Boolean hypercube.

Definition 4.2. (Optimization of 2XOR instances) Let $G = (V, E)$ be an undirected graph (possibly with parallel edges), with edge-signing $\mathrm{wt} : E \to \{\pm 1\}$. We call the pair $\mathcal{I} = (G, \mathrm{wt})$ an *instance*. The associated 2XOR *optimization problem* is to determine the *(true) optimum value*

$$\mathrm{OPT}(\mathcal{I}) = \max_{x:V\to\{\pm 1\}} \operatorname*{avg}_{e=\{u,v\}\in E} \{\mathrm{wt}(e)x_u x_v\} \in [-1, +1].$$

The special case in which $\mathrm{wt} \equiv -1$ is referred to as the Max-Cut problem on G, as in this case $\frac{1}{2} + \frac{1}{2}\mathrm{OPT}(\mathcal{I}) = \mathsf{Max\text{-}Cut}(G)$, the maximum fraction of edges that can be cut by a bipartition of V.

Determining $\mathrm{OPT}(\mathcal{I})$ is NP-hard in the worst case, leading to the study of computationally tractable approximations/relaxations. Two such approximations are the *eigenvalue bound* and the *SDP bound*, which we now recall.

Definition 4.3. (Adjacency matrix/operator) The *adjacency matrix* A of a finite weighted graph (G, wt) has rows and columns indexed by V; the entry $A[u, v]$ equals the sum of $\mathrm{wt}(e)$ over all edges with endpoints $\{u, v\}$. In case G is infinite we can more generally define the adjacency operator A on $\ell_2(V)$ as follows:

$$\text{for } F \in \ell_2(V), \quad AF(u) = \sum_{e=(u,v)\in E} \mathrm{wt}(e)F(v).$$

Definition 4.4. (Eigenvalue bound) The *eigenvalue bound* $\mathrm{EIG}(\mathcal{I})$ for 2XOR instance $\mathcal{I}$ with adjacency matrix A is $\frac{n}{2|E|}\lambda_{\max}(A)$, where $\lambda_{\max}$ denotes the maximum eigenvalue. We have $\mathrm{OPT}(\mathcal{I}) \leqslant \mathrm{EIG}(\mathcal{I})$ always, as the eigenvalue bound captures the relaxation of 2XOR optimization where we allow any $x : V \to \mathbb{R}$ satisfying $\|x\|^2 = n$.

The *SDP value* provides an even tighter upper bound on $\mathrm{OPT}(\mathcal{I})$, and is still efficiently computable.

Definition 4.5. (SDP bound) The *SDP bound* $\mathrm{SDP}(\mathcal{I})$ for 2XOR instance $\mathcal{I}$ is

$$\mathrm{SDP}(\mathcal{I}) = \max_{\vec{x}:V\to S^{m-1}} \operatorname*{avg}_{e=\{u,v\}\in E} \{\mathrm{wt}(e)\langle \vec{x}_u, \vec{x}_v\rangle\} \in [-1, +1],$$

where S^{m-1} refers to the set of unit vectors in $\mathbb{R}^m$ and the maximum is also over m (though $m = n$ is sufficient). The following holds for all $\mathcal{I}$:

$$\mathrm{OPT}(\mathcal{I}) \leqslant \mathrm{SDP}(\mathcal{I}) \leqslant \mathrm{EIG}(\mathcal{I}).$$

The left inequality is obvious. One way to see the right inequality is to use the fact, based on SDP duality, that $\mathrm{SDP}(\mathcal{I})$ is also equal to the minimum value of the eigenvalue bound applied to $A + Y$, where A is the weighted adjacency matrix of $\mathcal{I}$ and Y ranges over all matrices of trace 0. Additionally, we have the following equivalent definition for the SDP bound for 2XOR instances:

$$\mathrm{SDP}(\mathcal{I}) = \max_{X \succeq 0, X_{ii}=1} \langle A, X \rangle.$$

4.3 Instance Graphs, Additive Lifts and Nomadic Walks

Definition 4.6 (2-eigenvalue graphs)**.** We call an undirected, edge-weighted simple graph $\mathcal{I}$ a 2-*eigenvalue graph* if there are two real numbers λ_1 and λ_2 such that each eigenvalue of $\mathcal{I}$'s (signed) adjacency matrix A is equal to either λ_1 or λ_2.

Definition 4.7 (Constraint graphs)**.** An *r-ary, c-atom constraint graph* is any n-fold lift $\mathcal{H}$ of the complete bipartite graph $K_{r,c}$. Each vertex on the c-regular side is called a *variable vertex*, and is typically depicted by a circle. The variable vertices are partitioned into r *variable groups* each of size n, called the 1*st variable group*, the 2*nd variable group*, etc. Each vertex on the r-regular side is called a *constraint* (or *atom*) *vertex*, and is typically depicted by a square. Again, the constraint vertices are partitioned into c *constraint* (or *atom*) groups of size n, called the 1*st constraint/atom group*, 2*nd constraint/atom group*, etc. When $n = 1$, we call $\mathcal{H}$ a *base constraint graph*. We also allow "$n = \infty$": this means we take the infinite (r, c)-biregular tree and partition its variable vertices into r groups and its constraint variables into c groups in such a way that every variable vertex in the ith group has exactly one neighbor from each of the c constraint groups, and similarly every constraint vertex in the jth group has exactly one neighbor from each of the r variable groups.

Definition 4.8 (Instance graphs)**.** Let $\mathcal{A} = (A_1, \ldots, A_c)$ be a sequence of *atoms*, meaning edge-weighted undirected graphs on a common vertex set $[r]$. (In this paper, the edge-weights will usually be ± 1.) We also think of each atom as a collection of "2XOR-constraints" on variable set r. Now given an r-ary, c-atom constraint graph $\mathcal{H}$, we can combine it with the atom specification $\mathcal{A}$ to form the *instance graph* $\mathcal{I} := \mathcal{A}(\mathcal{H})$. This edge-weighted undirected graph $\mathcal{I}$ has as its vertex set all the variable vertices of $\mathcal{H}$. The edges of $\mathcal{I}$ are formed as follows: We iterate through each $j \in [c]$ and each constraint vertex f in the jth constraint group of $\mathcal{H}$. Given f, with variables neighbors $v_1, \ldots, v_r$ in $\mathcal{H}$, we place a copy of atom A_j onto these vertices in $\mathcal{I}$. ($\mathcal{I}$ may end up with parallel edges.) We refer to the graph obtained by placing a copy of A_j on vertices $v_1, \ldots, v_r$ as A_f, and for any edge e in $\mathcal{I}$ that came from placing A_j, we define $\mathrm{Atom}(e) := A_f$. We use $v \sim A_f$ to denote that v is one of $v_1, \ldots, v_r$. For $u, v \in \{v_1, \ldots, v_r\}$, $A_f(u, v)$ denotes the edge in A_f between u and v. And finally, denote the set $\{A_f : f \text{ constraint vertex in } \mathcal{H}\}$ with $\mathrm{Atoms}(\mathcal{I})$.

Remark 4.9. We treat atoms as edge-weighted, undirected, complete graphs. Thus, for a constraint vertex f in constraint-graph $\mathcal{H}$, if there is an edge between vertices u and v, and an edge between vertices v and w in the atom A_f, then there is an edge between u and w in A_f.

Definition 4.10 (Random additive lifts)**.** In the context of r-ary, c-atom constraint graphs, a *random n-lifted constraint graph* simply means a usual random n-lift $\mathcal{H}$ of the base constraint graph. Given atoms $\mathcal{A} = (A_1, \ldots, A_c)$, the resulting instance graph $\mathcal{I} = \mathcal{A}(\mathcal{H})$ is called a *random additive lift* of $\mathcal{A}$.

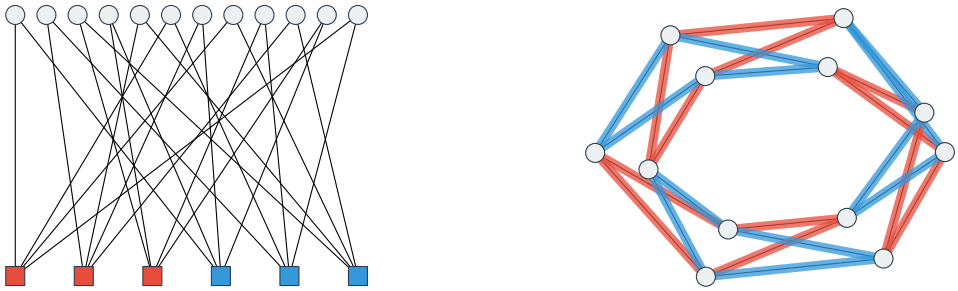

Figure 1: The figure on the left shows an example of a 4-ary, 2-atom 3-fold lift constraint graph, with the left bipartition color coded by constraint/atom groups. The figure on the right is the corresponding instance graph on (C_4, C_4), two four-cycle graphs, where each atom is color coded to match the figure on the left.

Definition 4.11 (Additive products)**.** If instead $\mathcal{H}$ is the "∞-lift" of $K_{r,c}$, the resulting infinite instance graph $\mathcal{I} = \mathcal{A}(\mathcal{H})$ is called the *additive product* of $A_1, \ldots, A_c$, denoted $A_1 \dotplus A_2 \dotplus \cdots \dotplus A_c$.

We will also extend Definition 4.8 to allow random additive lifts with *negations*. Eventually we will define a general notion of "1-wise uniform negations", but let us begin with two special cases. In the "constraint negation" model, we assign to each constraint vertex f in $\mathcal{H}$ (from group j) an independent uniformly random sign ξ^f. Then, when the instance graph $\mathcal{I}$ is formed from $\mathcal{H}$, each edge engendered by the constraint f has its weight multiplied by ξ^f. (Thus the edges in this copy of the atom A_j are either all left alone or they are simultaneously negated, with equal probability.) In the "variable negation" model, for each group-j constraint vertex f, adjacent to variable vertices $v_1, \ldots, v_r$, we assign independent and uniformly random signs $(\xi_i^f)_{i \in [r]}$ to the variables. Then when the copy of A_j is added into $\mathcal{I}$, the $\{i, i'\}$-edge has its weight multiplied by $\xi_i^f \xi_{i'}^f$. This corresponds to the constraint being applied to random *literals*, rather than variables.

Notice that in both of these negation models, every time a copy of atom A_j is placed into $\mathcal{I}$, its edges are multiplied by a collection of random signs $(\xi_{ij}^f)_{i,j \in [r]}$ which are "1-wise uniform". This is the only property we will require of a negation model.

Definition 4.12 (Random additive lifts with negations)**.** A random additive lift *with* 1*-wise uniform negations* is a variant of Definition 4.8 where, for each constraint vertex f there are associated random signs $\xi_i^{(f)} \in \{\pm 1\}$, where $i \in [r]$. For each fixed f, the random variables $\xi_i^{(f)}$ are required to be ± 1 with probability $1/2$ each, but they may be arbitrarily correlated; across different f's, the collections $(\xi_i^{(f)})_{i \in [r]}$ must be independent. When the instance graph $\mathcal{I}$ is formed as $\mathcal{A}(\mathcal{H})$, and a copy of A_j placed into $\mathcal{I}$ thanks to constraint vertex f, each new edge $\{i, i'\}$ has its weight $A_j[i, i']$ multiplied by $\xi_{ii'}^{(f)} := \xi_i^{(f)} \xi_{i'}^{(f)}$.

Remark 4.13. For a given constraint-vertex f of an instance graph $\mathcal{I}$ obtained via a random additive lift with negations, the matrix $\mathrm{Adj}(A_f)$ has the same spectrum as $\mathrm{Adj}(\overline{A_f})$ where $\overline{A_f}$ denotes the subgraph prior to applying random negations, since there is a sign diagonal matrix D such that $\mathrm{Adj}(\overline{A_f}) = D \cdot \mathrm{Adj}(A_f) \cdot D^\dagger$.

Definition 4.14 (Nomadic walks)**.** Let $\mathcal{H}$ be a constraint graph, $\mathcal{A} = (A_1, \ldots, A_c)$ a sequence of atoms, and $\mathcal{I} = \mathcal{A}(\mathcal{H})$ the associated instance graph. For initial simplicity, assume the atoms are unweighted (i.e., all edge weights are $+1$). A *nomadic walk* in $\mathcal{I}$ is a walk where consecutive steps are prohibited from "being in the same atom". Note that if $r = 2$ and the atoms are single edges, a nomadic walk in $\mathcal{I}$ is equivalent to a nonbacktracking walk.

To make the definition completely precise requires "remembering" the constraint graph structure $\mathcal{H}$. Each step along an edge of $\mathcal{I}$ corresponds to taking two consecutive steps in $\mathcal{H}$ (starting and ending at a variable vertex.) The walk in $\mathcal{I}$ is said to be nomadic precisely when the associated walk in $\mathcal{H}$ is nonbacktracking.

Finally, in the general case when the atoms A_j have weights, each *walk* in $\mathcal{I}$ gets a weight equal to the product of the edge-weights used along the walk.

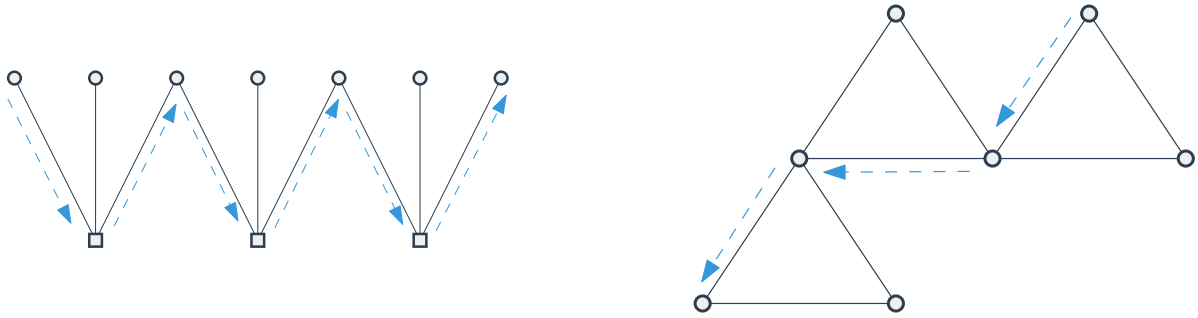

Figure 2: The figure on the left shows a nonbacktracking walk on a subset of a 3-ary constraint graph and the one on the right the same nomadic walk on the corresponding instance graph.

Definition 4.15 (Nomadic walk operator)**.** In the setting of the previous definition, the *nomadic walk operator* B for $\mathcal{I}$ is defined as follows. Each edge $e = \{u, v\}$ in $\mathcal{I}$ is regarded as two opposing directed edges $\vec{e} = (u, v)$ and $\vec{e}^{-1} = (v, u)$, each having the same edge-weight as e; i.e., $\mathrm{wt}(\vec{e}) = \mathrm{wt}(\vec{e}^{-1}) = \mathrm{wt}(e)$. Let $\vec{E}$ denote the collection of all directed edges. Now B is defined to be the following linear operator on $\ell_2(\vec{E})$:

$$\text{for } F \in \ell_2(\vec{E}), \quad BF(\vec{e}) = \sum_{\vec{e}'} \mathrm{wt}(\vec{e}')F(\vec{e}'),$$

where the sum is over all directed edges $\vec{e}'$ such that the pair $(\vec{e}, \vec{e}')$ forms a nomadic walk of length-2. In the finite-graph case we also think of B as a matrix; the entry $B[\vec{e}, \vec{e}'] = \mathrm{wt}(\vec{e}')$ whenever $(\vec{e}, \vec{e}')$ is a length-2 nomadic walk. Again, in the case where $r = 2$ and all atoms are single edges, the nomadic walk operator B coincides with the nonbacktracking walk operator.

4.4 Spectrum of Random Additive Lifts

The utility of the nomadic walk operator is twofold for us. First, for two-eigenvalue CSPs we can relate the eigenvalues of the usual adjacency operator to those of the nomadic walk operator through the following generalization of the Ihara–Bass Formula:

Theorem 4.16. *Let $\mathcal{A}$ be a sequence of atoms such that every atom has the same pair of exactly two distinct eigenvalues, λ_1 and λ_2, and let $\mathcal{H}$ be a constraint graph on variable set V. Let $\mathcal{I} = \mathcal{A}(\mathcal{H})$ be the corresponding instance graph with vertex set V and denote by A and B the adjacency matrix and nomadic walk matrix respectively of $\mathcal{I}$.*

Let $L(t) := \mathbb{1} - At + (\lambda_1 + \lambda_2)t\mathbb{1} + (c-1)(-\lambda_1\lambda_2)t^2$. Then we have:

$$(1+\lambda_1 t)^{|V|\frac{c\lambda_2}{\lambda_2-\lambda_1}-1}(1+\lambda_2 t)^{|V|\frac{c\lambda_1}{\lambda_1-\lambda_2}-1}\det L(t) = \det(\mathbb{1} - Bt).$$

The second utility of nomadic walks is that they provide the key simplification needed to make closed-walk counting in non-tree-like CSPs tractable. Because of this, we are able to establish the following modification of Bordenave's proof of Friedman's Theorem:

Theorem 4.17. *Let $\mathcal{A} = (A_1, \dots, A_c)$ be a sequence of r-vertex atoms with edges weights ± 1. Let $|\mathcal{I}_1|$ denote the instance graph $\mathcal{A}(K_{r,c})$ associated to the base constraint graph when the edge-signs are deleted (i.e., converted to $+1$), and let $|B_1|$ denote the associated nomadic walk matrix. Also, let $\boldsymbol{\mathcal{H}}_n$ denote a random n-lifted constraint graph and $\boldsymbol{\mathcal{I}}_n = \mathcal{A}(\boldsymbol{\mathcal{H}}_n)$ an associated instance graph with 1-wise uniform negations $(\boldsymbol{\xi}^f_{ii'})$. Finally, let $\boldsymbol{B}_n$ denote the nomadic walk matrix for $\boldsymbol{\mathcal{I}}_n$. Then for every constant $\varepsilon > 0$,*

$$\mathbf{Pr}[\rho(\boldsymbol{B}_n) \geqslant \sqrt{\rho(|B_1|)} + \varepsilon] \leqslant \delta,$$

where $\delta = \delta(n)$ is $o_{n\to\infty}(1)$.

And we can use our version of Ihara–Bass, Theorem 4.16, to conclude bounds on the spectrum of the adjacency matrix A from this theorem.

Theorem 4.18. *Let $\boldsymbol{\mathcal{I}}_n$ be a random additive n-lift of $\mathcal{A}$ with adjacency matrix $A_{\boldsymbol{\mathcal{I}}_n}$, and let $\epsilon > 0$. Then:*

$$\mathbf{Pr}\left[\rho(A_{\boldsymbol{\mathcal{I}}_n}) \in [\lambda_1 + \lambda_2 - 2\sqrt{(c-1)(-\lambda_1\lambda_2)} - \varepsilon, \lambda_1 + \lambda_2 + 2\sqrt{(c-1)(-\lambda_1\lambda_2)} + \varepsilon\right] = 1 - o_n(1)$$

Yet another advantage of using nomadic walks instead of closed walks is that in Theorem 4.18 we are able to bound the left and right spectral edge of $A_{\boldsymbol{\mathcal{I}}_n}$ by *different* values, whereas counting closed walks would, at best, only give an upper bound on $|\lambda|_{\max}(A_{\boldsymbol{\mathcal{I}}_n})$.

4.5 Additive Products and CSPs

The previous section gives us an upper bound on the SDP value for 2-eigenvalue CSPs, we complement that with a lower bound via the construction of an SDP solution that nearly matches the upper bound. In particular, we prove the following:

Theorem 4.19. *For every $\varepsilon > 0$, for large enough n, there are $|V(\boldsymbol{\mathcal{I}}_n)| \times |V(\boldsymbol{\mathcal{I}}_n)|$ positive semidefinite matrices M_+ and M_- with all-ones diagonals such that*

$$\langle A_{\boldsymbol{\mathcal{I}}_n}, M_+\rangle \geqslant (\lambda_1 + \lambda_2 + 2\sqrt{(c-1)(-\lambda_1\lambda_2)} - \varepsilon)n$$
$$\langle A_{\boldsymbol{\mathcal{I}}_n}, M_-\rangle \leqslant (\lambda_1 + \lambda_2 - 2\sqrt{(c-1)(-\lambda_1\lambda_2)} + \varepsilon)n.$$

with probability $1 - o_n(1)$.

This is proven using what is known as the "Gaussian Wave" idea, which allows one to convert approximate eigenvectors of the infinite graph defined as the additive product of the atoms to matching SDP solutions on random finite graphs $\mathcal{I}$. Finally, we can use this theorem to prove the final result regarding the SDP value.

Theorem 4.20. *Let $\mathcal{A} = (A_1, \ldots, A_c)$ be a sequence of r-vertex atoms with edge weights ± 1. Let $\boldsymbol{\mathcal{H}}_n$ denote a random n-lifted constraint graph and $\boldsymbol{\mathcal{I}}_n = \mathcal{A}(\boldsymbol{\mathcal{H}}_n)$ an associated instance graph with 1-wise uniform negations $(\boldsymbol{\xi}^f_{ii'})$. Let $\boldsymbol{A}_n$ be the adjacency matrix of $\boldsymbol{\mathcal{I}}_n$. Then, with probability $1 - o_n(1)$,*

$$\max_{X \succeq 0, X_{ii}=1} \langle \boldsymbol{A}_n, X \rangle = (\lambda_1 + \lambda_2 + 2\sqrt{(c-1)(-\lambda_1\lambda_2)} \pm \varepsilon)n$$

$$\min_{X \succeq 0, X_{ii}=1} \langle \boldsymbol{A}_n, X \rangle = (\lambda_1 + \lambda_2 - 2\sqrt{(c-1)(-\lambda_1\lambda_2)} \pm \varepsilon)n.$$

This implies Theorem 4.1.

5 Girth and Ramanujan Graphs

5.1 Overview

In this section we describe the results of [Par21]. In this paper we described a new method to remove short cycles on regular graphs while maintaining spectral bounds (the nontrivial eigenvalues of the adjacency matrix), as long as the graphs have certain combinatorial properties. These combinatorial properties are related to the number and distance between short cycles and are known to happen with high probability in uniformly random regular graphs.

Using this method we were able to show two results involving high girth spectral expander graphs: there exists an explicit distribution of d-regular $\Theta(n)$-vertex graphs where with high probability its samples have girth $\Omega(\log_{d-1} n)$ and are ε-near-Ramanujan; there is a a deterministic $\text{poly}(n)$-time algorithm that outputs a d-regular graph on $\Theta(n)$-vertices that is ε-near-Ramanujan and has girth $\Omega(\sqrt{\log n})$.

Prior to this work, Alon-Ganguly-Srivastava [AGS19] showed that for a given d such that $d-1$ is prime and $\alpha \in (0, 1/6)$, there is a construction of infinite families of graphs with girth at least $(1 - o_n(1))(2/3)\alpha \log_{d-1} n$ and λ at most $(3/\sqrt{2})\sqrt{d-1}$ with many eigenvalues localized on small sets of size $O(n^\alpha)$. Their motivation came from the theory of quantum ergodicity in graphs, which relates high-girth expanding graphs to delocalized eigenvectors. See [AGS19] for more on this. Our main result was based on some of the techniques of this work.

One other motivation to search for graphs with simultaneous good spectral expansion and high girth is its application to the theory of error-correcting codes, particularly for *Low Density Parity Check* or *LDPC* codes. The connection with high girth regular graphs was first pointed out by Margulis in [Mar82]. The property of high-girth is desirable since the decoding of such codes relies on an iterative algorithm whose performance is worse in the presence of short cycles. Additionally, using graphs with good spectral properties to generate these codes heuristically seems to lead to good performance, as pointed out by several works [RV00, LR00, MS02].

5.2 Spectral Preserving Cycle Removal

Before stating our main result we will first introduce one definition.

Definition 5.1 ((r,τ)-graph)**.** Let r and τ be a positive integers. Then, we call a graph G a (r,τ)-graph if it satisfies the following conditions:

- G is bicycle-free at radius at least r;
- The number of cycles of length at most r is at most τ.

Now, our main result is the following short cycle removal theorem:

Theorem 5.2. *There exists a deterministic polynomial-time algorithm* Fix *that, given as input a d-regular n-vertex (r,τ)-graph G satisfying $r \leqslant (2/3)\log_{d-1}(n/\tau) - 5$ outputs a graph* $\mathrm{Fix}(G)$ *satisfying*

- $\mathrm{Fix}(G)$ *is a d-regular graph with $n + O(\tau \cdot (d-1)^{r/2+1})$ vertices;*
- $\lambda(\mathrm{Fix}(G)) \leqslant \max\{\lambda(G), 2\sqrt{d-1}\} + O_d(1/r)$*;*
- $\mathrm{Fix}(G)$ *has girth at least r.*

The key fact in our proof of this statement is a theorem proved by Kahale [Kah95], originally used to construct Ramanujan graphs with better expansion of sublinear sized subsets.

The preconditions of this theorem are not arbitrary. Even though random uniformly n-vertex d-regular graphs have constant girth with high probability, they are bicycle-free at radius $\Omega(\log_{d-1} n)$ and the number of cycles of length at most $c\log_{d-1} n$ (for small enough c) is $o(n)$ with high probability. Recall that from Theorem 1.17 we also know that being near-Ramanujan is also a property that occurs with high probability in random regular graphs. So a statement like the above can be used to produce distributions over regular graphs that have high girth and are near-Ramanujan with high probability. With this in mind, we introduce the following definition:

Definition 5.3. ((Λ, g)-good graphs). We call a graph G a (Λ, g)-good graph if $\lambda(G) \leqslant \Lambda$ and $\mathrm{girth}(G) \geqslant g$.

Let $\mu_d(n)$ be a distribution over d-regular graphs with $\sim n$ vertices. We say $\mu_d(n)$ is (Λ, g)-good if $G \sim \mu_d(n)$ is (Λ, g)-good with probability at least $1 - o_n(1)$.

Additionally, we call the distribution explicit if sampling an element is doable in polynomial time.

We can prove the following using Theorem 5.2:

Theorem 5.4. *Given $d \geqslant 3$ and n, let G be a uniformly random d-regular n-vertex graph. For any $c < 1/4$ and $\epsilon > 0$,* $\mathrm{Fix}(G)$ *is a $(2\sqrt{d-1}+\epsilon, c\log_{d-1} n)$-good explicit distribution.*

A simple path counting argument known as the "Moore bound" shows that this girth is upper bounded by $(1 + o_n(1))2\log_{d-1} n$, so this distribution has optimal girth up to a constant. Based on our proof of the above and using some classic results about the number of d-regular n-vertex graphs, we can show a lower bound on the number of $(2\sqrt{d-1}+\epsilon,\ c\log_{d-1} n)$-good graphs in some range.

Corollary 5.5. *Let $d \geqslant 3, n$ be integers and $\epsilon > 0, c > 1/4$ reals. The number of d-regular graphs with number of vertices in $[n, n + O(n^{3/8})]$, which are $(2\sqrt{d-1}+\epsilon,\ c\log_{d-1} n)$-good, is at least*

$$\Omega\left(\left(\frac{d^d n^d}{e^d (d!)^2}\right)^{n/2}\right).$$

Finally, we showed a slightly stronger version of result of [MOP20a] by plugging our short cycle removal theorem into its main construction.

Theorem 5.6. *Given any integer n and constants $d \geqslant 3$, $\epsilon > 0$ and c, there is a deterministic polynomial-time (in n) algorithm that constructs a d-regular N-vertex graph with the following properties:*

- $N = n(1 + o_n(1))$;
- $\lambda(G) \leqslant 2\sqrt{d-1} + \epsilon$;
- *G has girth at least $c\sqrt{\log n}$.*

The running time from the theorem above has an exponential dependency on d, ϵ and c.

5.3 Future Directions and Open Problems

There are many open problems and possible future directions related to this area, we summarize a few.

Open Question 5.7. Can we improve Theorem 5.6 to obtain high girth?

Something like this could be proved by showing that when 2-lifting a graph with large enough girth, with sufficiently high probability the girth of the resulting graph increases. This would boost the girth of the graph generated by the first step of the construction of [MOP20a] during the repeated 2-lift step. However, it is unclear if this can be done. Alternatively, one could show that bicycle-freeness increases with good probability as we 2-lift, but this is also unclear.

A different strategy would be to find a different way to derandomize Theorem 1.17 such that the we can generate a starter graph of larger size. However, it is unclear if this strategy could work since the tool used to derandomize this, namely (δ, k)-wise uniform permutations, cannot be improved to derandomize this to the required extent.

Open Question 5.8. Can we obtain Theorem 5.4 for higher values of c; for example, can we build a distribution that is $(2\sqrt{d-1} + \epsilon, .99 \log_{d-1} n)$-good?

One promising strategy would be to show that the graphs produced by the distribution described in [LS19], which were shown to have girth at least $.99 \log_{d-1} n$ with high probability, are also near-Ramanujan with high probability. Numerical calculations seem to indicate that the answer is positive, as pointed out in one of the open problems given in [LS19].

6 Abelian Lifts and Quantum LDPC Codes

6.1 Primer on Coding Theory

An *error correcting code* $\mathcal{C}$ of *code length* n over an *alphabet* Σ is a subset of Σ^n. Elements of $\mathcal{C}$ are known as *codewords*. We usually represent the cardinality of the code $|\Sigma|$ by q. The *dimension* of the code is given by $\log_q |\mathcal{C}|$, which we usually denote by k or $\dim \mathcal{C}$. An alternate way of defining an error correcting code is as an injective map $\Sigma^k \to \Sigma^n$.

A *linear code* is a code for which any linear combination of codewords is also a codeword. Consider a finite field $\mathbb{F}_q$ and an n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Formally, a linear $[n,k]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$. We can associate to $\mathcal{C}$ a full-rank $n \times k$ matrix G, called the *generator matrix*, such that $\mathcal{C}$ is the row space of G. Using the map definition of codes, this is equivalent to saying that the injective map $\mathbb{F}_q^k \to \mathbb{F}_q^n$ that defines the code is given by $x \mapsto Gx$. Additionally, we can associate a $(n-k) \times n$ matrix H, called the *parity check matrix*, such that $\mathcal{C}$ is the kernel of H, which means that for $x \in \mathcal{C}$ we have $Hx = 0$. It is not hard to see that $GH^T = 0$.

The *dual code* of a code $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is a $[n, n-k]_q$ linear code defined as $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n | \forall y \in \mathcal{C}, \langle x, y \rangle = 0\}$. It is easy to see that the generator matrix for $\mathcal{C}$ is H and the parity check matrix is G.

The *Hamming distance* between two vectors $x, y \in \mathbb{F}_q^n$, denoted by $d(x,y)$, is the number of positions at which the corresponding symbols are different. The *distance of a code* $\mathcal{C}$ is the minimum Hamming distance between distinct codewords, formally $d(\mathcal{C}) = \min\{d(x,y) | x \neq y; x, y \in \mathcal{C}\}$.

A *low density parity check (LDPC) code* is a linear code whose parity check matrix has row and column weights bounded by a constant w. They were first introduced by Gallager [Gal62] in the '60s and are one of the most popular classes of classical error-correcting codes, both in theory and in practice. This popularity comes from the fact that there are many known constructions of classical LDPC codes that achieve linear rate and distance that can also be decoded in linear time [RU08].

6.2 Preliminaries and Overview

In this section we describe the results of [JMO+22], which was joint work with Fernando Granha Jeronimo, Tushant Mittal, Ryan O'Donnell and Madhur Tulsiani. In this paper we study a generalization of lifts based on groups and we describe explicit constructions of expanders obtained via abelian lifts. Expanding graphs obtained via abelian lifts, form a key ingredient in recent breakthrough constructions of quantum LDPC codes. However, these constructions are non-explicit. Our result obtains explicit quantum lifted product codes of almost linear distance (and also in a wide range of parameters) based on these non-explicit results.

Let's consider the graph lift operation. One way to generalize a graph lift is by restricting the types of matchings that are allowed to replace an edge. In general form, a group lifting operation takes a lift size parameter ℓ, a base graph G_0 on n vertices and a subgroup H of the symmetric group $\mathrm{Sym}(\ell)$ and constructs a new "lifted" graph G on $n\ell$ vertices where each vertex v of G_0 is replaced by ℓ-copies $(v,1), \ldots, (v,\ell)$ and for every edge $e = (u,v)$ of G_0 we associate an element of $h_e \in H$ and (u,i) is connected to $(v, h_e(i))$ for $i \in [\ell]$. Notice that an ordinary ℓ-lift is a lift based on the symmetric group, i.e. $H = \mathrm{Sym}(\ell)$.

An example of such group is the class of *shift lifts*, where we consider the cyclic group $\mathbb{Z}_\ell$. These were first studied by Agarwal et al. [ACKM19], who showed that an uniformly random shift k-lift of any n-vertex d-regular base graph G has the new eigenvalues bounded by $\lambda(G) + O(\sqrt{d})$ with probability $1 - k \cdot \exp(-\Omega(n/d^2))$. Later, Chandrasekaran and Velingker [CV17] showed that for bipartite graphs there is always a shift 3-lift and a 4-lift whose new eigenvalues are bounded by $2\sqrt{d-1}$, using techniques similar to those of [MSS15a]. They also conjectured that this is true for any shift k-lift, but Agarwal et al. [ACKM19] showed that for $k = 2^{\Omega(nd)}$ this is impossible (and the same applies to any lift based on an abelian group).

Calderbank-Shor-Steane (CSS) codes are a family of quantum error-correcting codes that was first described in [CS96]. A CSS code $\mathcal{Q}$ of dimension K is defined by a pair of classical linear codes $\mathcal{C}_Z$ and $\mathcal{C}_X$ such that $\mathcal{C}_X^\perp \subseteq \mathcal{C}_Z$ and $K = \dim \mathcal{C}_Z/\mathcal{C}_X^\perp$. The quantum analog of LDPC codes is thus defined as CSS codes where the parity check matrices of both $\mathcal{C}_X$ and $\mathcal{C}_Z$ have bounded row and column weights.

While we know many good constructions of classical LDPC codes, until recently we only knew how to construct a code with distance $\Theta(\sqrt{N}\text{polylog}(N))$ [DKP02, FML02, EKZ20]. The $\sqrt{N}$ barrier was finally broken by Hastings-Haah-O'Donnell, who introduced *fiber bundle codes*. These obtain dimension $\Theta(N^{3/5})$ and distance $\Omega(N^{3/5}\text{polylog}(N))$. Later, Pantaleev and Kalachev [PK20] introduced a similar construction they called *lifted products*, which obtains codes with dimension $\Theta(N^\alpha \log(N))$ and distance $\Omega(N^{1-\alpha/2}/log(N))$, for $0 \leqslant \alpha < 1$. Both constructions are only probabilistic and not explicit, meaning they cannot be generated in deterministic polynomial time.

6.3 Abelian Lifts

The action of a group H on a set of ℓ elements is defined by a map $\psi : H \to Sym(\ell)$ which satisfies $\psi(h_1h_2) = \psi(h_1)\psi(h_2)$. Since we only care about the action of the group, we will assume $\psi(H) \subseteq Sym(\ell)$ and the action is the natural one and we will use a slight abuse of notation and use H and $\psi(H)$ interchangeably.

Definition 6.1 ((H,ℓ)-lifts)**.** Fix a *base* graph $\underline{G} = (\underline{V}, \underline{E})$ on $\underline{n}$ vertices. Let H be a group such that $H \subseteq \text{Sym}(\ell)$. Then a *$(H,\ell)$-lift of $\underline{G}$* is the graph G defined by a collection of elements of the group $g_{uv} \in H$, one for each edge $(u,v) \in \vec{\underline{E}}$, under the constraint that $g_{uv} = g_{vu}^{-1}$. The vertex set of G is $\underline{V} \times [\ell]$, and the edges of G are given by all pairs $(u,i),(v,j)$ satisfying $(u,v) \in \underline{E}$ and $g_{uv}(i) = j$. When the group elements g_{uv} are independent and uniformly random, we call the associated graph $\boldsymbol{G}$ a *(uniformly) random (H,ℓ)-lift of $\underline{G}$*.

We will restrict to analyzing abelian H and the most important case to consider is when $H = \mathbb{Z}/\ell\mathbb{Z} = \mathbb{Z}_\ell$, the cyclic group of order ℓ (also defined as $\{\mu : \mu^\ell = 1\}$), and we refer to such lifts as shift ℓ-lifts. A necessary condition for the lift to be expanding is for it to be connected. A subgroup H is *transitive* if for every $i,j \in [\ell]$, there exists $h \in H$ such that $h \cdot i = j$. Lifts of non-transitive subgroups are disconnected because if the pair $\{i,j\}$ violate the condition then any pair (u,i) and (v,j) are disconnected. From here on we assume that H is a transitive abelian group.

Definition 6.2. A *generalized (H,ℓ)-signing* of a graph $G = (V,E)$ is a function $s : E(G) \to H$ such that $s(u,v) = s(v,u)^{-1}$. A generalized signing s uniquely defines a (H,ℓ)-lift of a graph in the natural way.

To analyze the spectral properties of (H,ℓ)-lifts of graphs it is useful to look at the representation theory of the underlying group. For a (H,ℓ)-lift of a graph $\underline{G} = (V,E)$ with adjacency matrix A given by a generalized signing $(s(u,v) = g_{uv})_{(u,v)\in E(\underline{G})}$, we define the family of matrices $A_s(\omega)$, parameterized by ω where ω is a ℓth root of unity such that when $(u,v) \in E(\underline{G})$ then $[A_s(\omega)]_{uv} = \omega^{g_{uv}}$, otherwise $[A_s(\omega)]_{uv} = 0$. Now we have the following lemma regarding the eigenvalues of abelian lifts.

Lemma 6.3. *Let $\underline{G} = (V,E)$ be a d-regular n-vertex graph and H a abelian group. Let G be the (H,ℓ)-lift of $\underline{G}$ given by the generalized signing $(s(u,v) = g_{uv})_{(u,v)\in E(\underline{G})}$. Then there exists a set $\{\omega_1,\ldots,\omega_\ell\}$ of ℓth roots of unity such that:*

$$\mathrm{Spec}(A_G) = \bigcup_i \mathrm{Spec}(A_s(\omega_i)).$$

The set $\{\omega_1, \ldots, \omega_\ell\}$ of roots of unity is given by the characters of the representations of H, which are always ℓth roots of unity if H is abelian. Additionally, if H is a transitive group, then at least one of the characters is the trivial character, meaning there is at least one i such that $\omega_i = 1$.

We can now state our main technical lemma.

Lemma 6.4. *Let $G = (V, E)$ be an arbitrary d-regular n-vertex graph and ω a ℓth root of unity. Choose any $k \in \mathbb{N}^+$ such that $k \gg \log n$. Assume that G is bicycle-free at radius $r \geqslant O(\log \ell)$. Then for a uniformly random generalized signing $\mathbf{s}$, except with probability at most $\exp(-c \cdot k)$, we have the following spectral radius bound*

$$\rho(B_s(\omega)) \leqslant \sqrt{d-1} \cdot (1 + O(c + \log(\ell)/r)),$$

and hence (by a version of Corollary 2.9)

$$\rho(A_s(\omega)) \leqslant 2\sqrt{d-1} \cdot \left(1 + O(c + \log(\ell)/r)^2\right).$$

Furthermore, suppose we merely assume that the random generalized signing is $(\delta, 2\ell)$-wise independent for $\delta \leqslant \exp(-((1+c)\ell + \ell \log d + \ell \log \kappa))$, for any $\kappa = \kappa(n)$ such that $\kappa \geqslant 1$. Then the above bounds continue to hold, with an additional additive $\sqrt{d}/\kappa$ in the $B_s(\omega)$ bound and $\sqrt{d}/\kappa^2$ in the $A_s(\omega)$ bound.

Using Lemma 6.3 and Lemma 6.4, we can union bound over all ℓ roots of unity to obtain our main result.

Theorem 6.5. *For large enough n and constant degree $d \geqslant 3$, given ℓ such that $\ell \leqslant \exp(n^{\Theta(1)})$, the generating elements of a transitive abelian group $H \leqslant \mathrm{Sym}(\ell)$, and any fixed constant $\varepsilon \in (0, 1)$, we can construct in deterministic polynomial time, a d-regular graph G on $\Theta(n\ell)$ vertices such that:*

- *G is (H, ℓ)-lift of a graph G_0 on $\Theta(n)$ vertices.*
- *$\lambda(G) \leqslant 2\sqrt{d-1} + \epsilon$, if $\ell \leqslant 2^{n^\delta}$ where $\delta = \delta(d, \epsilon)$,*
- *$\lambda(G) \leqslant \epsilon \cdot d$, if $\ell \leqslant 2^{n^{\delta_0}}$ for a fixed $\delta_0 > 0$, when $d \geqslant d_0(\epsilon)$.*

6.4 Explicit Quantum LDPC Codes

As stated before, our main application for our abelian lift expansion result is in the construction of explicit quantum LDPC codes with near linear distance.

We now briefly recall the construction of quantum LDPC codes as in [PK20] and show how our results derandomize it. The construction is as follows. Let G be a d-regular graph (on $n\ell$ vertices) such that G is a $(\mathbb{Z}_\ell, \ell)$-lift of a graph on n-vertices. Let $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$ be a binary linear code (of block length d). Let B denote the bipartite graph of the Tanner code $\mathcal{T}(G, \mathcal{C}_0)$ and let F denote the cycle graph on ℓ vertices. They define the lifted product $\mathrm{LP}(B, F)$ of B and F which is a variation of the usual tensor product. The main result of [PK20] is the following.

Theorem 6.6 ([PK20]). *Let G be $(\mathbb{Z}_\ell, \ell)$-lift of a d regular graph on n-vertices with $\lambda_2(G) \leqslant \varepsilon \cdot d$. Let $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$ and its dual attain the Gilbert–Varshamov bound. sufficiently large constant, then the quantum lifted product code $\mathrm{LP}(B, F)$ is LDPC and has distance $\Theta_{\epsilon,d}(\ell)$ and rate $\Theta(n)$.*

To achieve these, [PK20] picks a d-regular expander on n vertices and creates a random shift ℓ-lift. The final graph is expanding with high probability, which follows from a result of [ACKM19]. The distance achieves the almost-linear bound only when the lift is large and thus lifts of exponential size are preferred.

For this application, the constant degree regime is important for two reasons. The locality of the code is essentially d and thus it has to be constant for it to be LDPC. Moreover, the code $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$ can be easily constructed via brute-force search since d is constant.

The following theorem now follows from the result of the previous section.

Theorem 6.7. *We have explicit polynomial time constructions of each of the following,*

- *Quantum LDPC code with distance $\Omega(N/\mathrm{polylog}(N))$ and rate $\Omega(\mathrm{polylog}(N))$.*
- *Quantum LDPC code with distance $\Omega(N^{1-\alpha}/\mathrm{polylog}(N))$ and rate $\Theta(N^\alpha \mathrm{polylog}(N))$ for every constant $\alpha > 0$.*

6.5 Future Directions and Open Problems

There are many open problems and possible future directions related to this area, we summarize a few.

Open Question 6.8. What can we say about the expansion of non-abelian lifts?

One of the reasons why shift lifts were studied in the context of expanders was as a potential way to build Ramanujan graphs of all degrees [CV15]. Suppose we could prove the following: There exists a shift k-lift that maintains the Ramanujan property of d-regular graphs on n vertices for all n. Then, we could start with a complete d-regular graph K_{d+1} and then there would be a shift k-lift for $k \sim n$ that lifts this starting graph to a Ramanujan graph with n vertices. Since there are at most k^{d^2} shift lifts, a simple brute force algorithm would work in polynomial time.

Unfortunately, [ACKM19] showed that this is impossible since for $k = 2^{\Omega(n_0 d)}$ (where n_0 is the number of vertices of the starting graph) there is no expanding shift lift. Even more, they show the same also applies for any abelian lift. This closes a lot of possibilities, however, we know that for general graph lifts, a generalization [HPS18] of [MSS15a] shows that there is always a one-sided Ramanujan k-lift of any graph. This result is only existential and it is hard to make explicit, but it suggests the question: what can we say about the expansion of other non-abelian group lifts? Can we find a good expanding non-abelian group that is easy to derandomize, just like shift lifts?

Open Question 6.9. Can we obtain strongly explicit constructions of expanding abelian lifts?

As we mentioned before, strong explicitness is required for many applications, especially in coding theory. Given the application of abelian lifts to quantum LDPC codes, it is natural to ask if we can find strongly explicit such constructions.

7 More Future Directions

The expansion of graphs has been heavily studied since its introduction in the '70s. Even though there are still many open problems directly related to expanders, recently there has been a lot of work towards studying higher dimensional versions of expander graphs. Graphs are great tools to model all kinds of information, but using higher dimensional objects like simplicial complexes or hypergraphs allows us to explore more structure and thus make a better model. This is one of the reasons why these objects are getting more attention recently from the computer science and mathematical communities. Not surprisingly, there are still many open problems in the area.

Open Question 7.1. Are there randomized models of higher dimensional objects (e.g. simplicial complexes) that are expanding?

Uniformly random d-regular graphs are near-Ramanujan with high probability, but it is much harder to describe a random model of a higher dimensional object that has a similar property.

Open Question 7.2. What combinatorial constructions of high dimensional expanders can we obtain?

We know of some constructions of high dimensional expanders (see, for instance, [KO18]), but what other constructions can we find? What about combinatorial constructions?

Given the multitude of applications of high dimensional expanders including to coding theory, complexity theory (for example, in probabilistically checkable proofs), bounding mixing times of Markov chains, counting and sampling of objects (like bases of matroids), there are many exciting future directions. Even though expander graphs are a (relatively) old concept their full potential is still yet to be discovered.

References

[AC88] N. Alon and F. R. K. Chung. Explicit construction of linear sized tolerant networks. In Proceedings of the First Japan Conference on Graph Theory and Applications (Hakone, 1986), volume 72, pages 15–19, 1988. 4

[ACKM19] Naman Agarwal, Karthekeyan Chandrasekaran, Alexandra Kolla, and Vivek Madan. On the expansion of group-based lifts. SIAM J. Discrete Math., 33(3):1338–1373, 2019. 22, 25

[AGS19] Noga Alon, Shirshendu Ganguly, and Nikhil Srivastava. High-girth near-ramanujan graphs with localized eigenvectors. arXiv preprint arXiv:1908.03694, 2019. 19

[Alo86] Noga Alon. Eigenvalues and expanders. Combinatorica, 6(2):83–96, 1986. 4, 6

[AM85] N. Alon and V. D. Milman. λ_1, isoperimetric inequalities for graphs, and superconcentrators. J. Combin. Theory Ser. B, 38(1):73–88, 1985. 4

[Bas92] Hyman Bass. The Ihara-Selberg zeta function of a tree lattice. Internat. J. Math., 3(6):717–797, 1992. 9

[BL06] Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap. Combinatorica, 26(5):495–519, 2006. 6, 8

[Bor19] Charles Bordenave. A new proof of Friedman's second eigenvalue theorem and its extension to random lifts. Technical Report 1502.04482v4, arXiv, 2019. To appear in Annales scientifiques de l'École normale supérieure. 6, 9

[BT11] 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. 6

[Chi92] Patrick Chiu. Cubic Ramanujan graphs. Combinatorica, 12(3):275–285, 1992. 5

[Cla06] Pete Clark. Ramanujan graphs and Shimura curves. Retrieved from http://alpha.math.uga.edu/~pete/ramanujanrevisited.pdf, 2006. 5

[CM08] Sebastian M. Cioabă and M. Ram Murty. Expander graphs and gaps between primes. Forum Mathematicum, 20(4):745–756, 2008. 6

[Coh16] Michael Cohen. Ramanujan graphs in polynomial time. In Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science, pages 276–281, 2016. 6

[CS96] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. Physical Review A, 54(2):1098, 1996. 23

[CV15] Karthekeyan Chandrasekaran and Ameya Velingker. Towards constructing ramanujan graphs using shift lifts. arXiv preprint arXiv:1502.07410, 2015. 25

[CV17] Karthekeyan Chandrasekaran and Ameya Velingker. Shift lifts preserving Ramanujan property. Linear Algebra Appl., 529:199–214, 2017. 22

[DKP02] Eric Dennis, Alexei Kitaev, and John Preskill. Topological quantum memory. volume 43, pages 4452–4505. 2002. Quantum information theory. 23

[dlHM06] Pierre de la Harpe and Antoine Musitelli. Expanding graphs, Ramanujan graphs, and 1-factor perturbations. Bulletin of the Belgian Mathematical Society — Simon Stevin, 13(4):673–680, 2006. 6

[Dod84] Jozef Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. Trans. Amer. Math. Soc., 284(2):787–794, 1984. 4

[EKZ20] Shai Evra, Tali Kaufman, and Gilles Zémor. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders. In 2020 IEEE 61st Annual Symposium on Foundations of Computer Science, pages 218–227. IEEE Computer Soc., Los Alamitos, CA, [2020] ©2020. 23

[FK81] Z. Füredi and J. Komlós. The eigenvalues of random symmetric matrices. Combinatorica, 1(3):233–241, 1981. 9

[FML02] Michael H. Freedman, David A. Meyer, and Feng Luo. Z_2-systolic freedom and quantum codes. In Mathematics of quantum computation, Comput. Math. Ser., pages 287–320. Chapman & Hall/CRC, Boca Raton, FL, 2002. 23

[Fri93] Joel Friedman. Some geometric aspects of graphs and their eigenfunctions. Duke Mathematical Journal, 69(3):487–525, 1993. 4

[Fri08] Joel Friedman. A proof of Alon's second eigenvalue conjecture and related problems. Memoirs of the American Mathematical Society, 195(910):viii+100, 2008. 6

[Gal62] R. G. Gallager. Low-density parity-check codes. IRE Trans., IT-8:21–28, 1962. 22

[GG81] Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. Journal of Computer and System Sciences, 22(3):407–420, 1981. Special issued dedicated to Michael Machtey. 5

[Gol00] Oded Goldreich. Candidate one-way functions based on expander graphs. Technical Report 90, Electronic Colloquium on Computational Complexity, 2000. 13

[Has89] Ki-ichiro Hashimoto. Zeta functions of finite graphs and representations of p-adic groups. In Automorphic forms and geometry of arithmetic varieties, volume 15 of Adv. Stud. Pure Math., pages 211–280. Academic Press, Boston, MA, 1989. 9

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. American Mathematical Society Bulletin, 43(4):439–561, 2006. 5, 7

[HPS18] Chris Hall, Doron Puder, and William F. Sawin. Ramanujan coverings of graphs. Adv. Math., 323:367–410, 2018. 25

[Iha66] Yasutaka Ihara. On discrete subgroups of the two by two projective linear group over p-adic fields. J. Math. Soc. Japan, 18:219–235, 1966. 5, 9

[JMO+22] Fernando Granha Jeronimo, Tushant Mittal, Ryan O'Donnell, Pedro Paredes, and Madhur Tulsiani. Explicit abelian lifts and quantum ldpc codes. 2022. 7, 22

[JP00] Ari Juels and Marcus Peinado. Hiding cliques for cryptographic security. Designs, Codes and Cryptography, 20(3):269–280, 2000. 13

[Kah95] Nabil Kahale. Eigenvalues and expansion of regular graphs. Journal of the ACM (JACM), 42(5):1091–1106, 1995. 20

[KO18] Tali Kaufman and Izhar Oppenheim. Construction of new local spectral high dimensional expanders. In STOC'18—Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, pages 773–786. ACM, New York, 2018. 26

[Kow19] Emmanuel Kowalski. An introduction to expander graphs. Société mathématique de France, 2019. 7

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. Combinatorica, 8(3):261–277, 1988. 5

[LR00] John Lafferty and Dan Rockmore. Codes and iterative decoding on algebraic expander graphs. In the Proceedings of ISITA. Citeseer, 2000. 19

[LS19] Nati Linial and Michael Simkin. A randomized construction of high girth regular graphs. arXiv preprint arXiv:1911.09640, 2019. 21

[Mar73] Grigory Margulis. Explicit construction of concentrators. Problemy Peredachi Informatsii, 94(4):71–80, 1973. 5

[Mar82] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes. Combinatorica, 2(1):71–78, 1982. 19

[Mar88] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. Problemy Peredachi Informatsii, 24(1):51–60, 1988. 5

[MOP20a] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-ramanujan graphs of every degree. In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, pages 510–523, 2020. 7, 10, 21

[MOP20b] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. The sdp value for random two-eigenvalue csps. In 37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020). Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020. 7, 13

[Mor94] Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. J. Combin. Theory Ser. B, 62(1):44–62, 1994. 5

[MS02] Mohammad M Mansour and Naresh R Shanbhag. Construction of ldpc codes from ramanujan graphs. In 36th Annu. Conf. on Information Sciences and Systems, 2002. 19

[MSS15a] Adam Marcus, Daniel Spielman, and Nikhil Srivastava. Interlacing families I: Bipartite Ramanujan graphs of all degrees. Annals of Mathematics. Second Series, 182(1):307–325, 2015. 6, 22, 25

[MSS15b] Adam Marcus, Daniel Spielman, and Nikhil Srivastava. Interlacing families IV: Bipartite Ramanujan graphs of all sizes. In Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science, pages 1358–1377, 2015. 6

[Nil91] A. Nilli. On the second eigenvalue of a graph. Discrete Mathematics, 91(2):207–210, 1991. 4

[Par21] Pedro Paredes. Spectrum preserving short cycle removal on regular graphs. In 38th International Symposium on Theoretical Aspects of Computer Science, 2021. 7, 19

[Piz90] Arnold Pizer. Ramanujan graphs and Hecke operators. American Mathematical Society. Bulletin. New Series, 23(1):127–137, 1990. 5

[PK20] Pavel Panteleev and Gleb Kalachev. Quantum ldpc codes with almost linear minimum distance. arXiv preprint arXiv:2012.04068, 2020. 23, 24, 25

[RU08] Tom Richardson and Ruediger Urbanke. Modern coding theory. Cambridge university press, 2008. 22

[RV00] Joachim Rosenthal and Pascal O Vontobel. Constructions of ldpc codes using ramanujan graphs and ideas from margulis. In in Proc. of the 38-th Allerton Conference on Communication, Control, and Computing. Citeseer, 2000. 19

[RVW02] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. Annals of Mathematics, 155(1):157–187, 2002. 6, 13

[Ser77] Jean-Pierre Serre. Arbres, amalgames, SL_2. Astérisque, No. 46. Société Mathématique de France, Paris, 1977. Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass. 9

[Wor99] Nicholas C Wormald. Models of random regular graphs. London Mathematical Society Lecture Note Series, pages 239–298, 1999. 8