

# Explicit Abelian Lifts and Quantum LDPC Codes

Fernando Granha Jeronimo ✉🏠

Institute for Advanced Study, Princeton, NJ, USA

Tushant Mittal ✉🏠 

Department of Computer Science, University of Chicago, IL, USA

Ryan O’Donnell ✉🏠

Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA

Pedro Paredes ✉🏠

Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA

Madhur Tulsiani ✉🏠

Toyota Technological Institute at Chicago, IL, USA

---

## Abstract

For an abelian group  $H$  acting on the set  $[\ell]$ , an  $(H, \ell)$ -lift of a graph  $G_0$  is a graph obtained by replacing each vertex by  $\ell$  copies, and each edge by a matching corresponding to the action of an element of  $H$ .

Expanding graphs obtained via abelian lifts, form a key ingredient in the recent breakthrough constructions of quantum LDPC codes, (implicitly) in the fiber bundle codes by Hastings, Haah and O’Donnell [STOC 2021] achieving distance  $\tilde{\Omega}(N^{3/5})$ , and in those by Panteleev and Kalachev [IEEE Trans. Inf. Theory 2021] of distance  $\Omega(N/\log(N))$ . However, both these constructions are *non-explicit*. In particular, the latter relies on a randomized construction of expander graphs via abelian lifts by Agarwal et al. [SIAM J. Discrete Math 2019].

In this work, we show the following *explicit* constructions of expanders obtained via abelian lifts. For every (transitive) abelian group  $H \leq \text{Sym}(\ell)$ , constant degree  $d \geq 3$  and  $\epsilon > 0$ , we construct explicit  $d$ -regular expander graphs  $G$  obtained from an  $(H, \ell)$ -lift of a (suitable) base  $n$ -vertex expander  $G_0$  with the following parameters:

- (i)  $\lambda(G) \leq 2\sqrt{d-1} + \epsilon$ , for any lift size  $\ell \leq 2^{n^\delta}$  where  $\delta = \delta(d, \epsilon)$ ,
- (ii)  $\lambda(G) \leq \epsilon \cdot d$ , for any lift size  $\ell \leq 2^{n^{\delta_0}}$  for a fixed  $\delta_0 > 0$ , when  $d \geq d_0(\epsilon)$ , or
- (iii)  $\lambda(G) \leq \tilde{O}(\sqrt{d})$ , for lift size “exactly”  $\ell = 2^{\Theta(n)}$ .

As corollaries, we obtain *explicit* quantum lifted product codes of Panteleev and Kalachev of almost linear distance (and also in a wide range of parameters) and *explicit* classical quasi-cyclic LDPC codes with wide range of circulant sizes.

Items (i) and (ii) above are obtained by extending the techniques of Mohanty, O’Donnell and Paredes [STOC 2020] for 2-lifts to much larger abelian lift sizes (as a byproduct simplifying their construction). This is done by providing a new encoding of special walks arising in the trace power method, carefully “compressing” depth-first search traversals. Result (iii) is via a simpler proof of Agarwal et al. [SIAM J. Discrete Math 2019] at the expense of polylog factors in the expansion.

**2012 ACM Subject Classification** Theory of computation  $\rightarrow$  Pseudorandomness and derandomization; Theory of computation  $\rightarrow$  Expander graphs and randomness extractors

**Keywords and phrases** Graph lifts, expander graphs, quasi-cyclic LDPC codes, quantum LDPC codes

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2022.88

**Related Version** *Full Version:* <https://arxiv.org/abs/2112.01647>

**Funding** This material is based upon work supported by the National Science Foundation under grant numbers listed below. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation (NSF).

*Fernando Granha Jeronimo:* Supported by Grant No. CCF-1900460 and also supported in part by NSF grant CCF-1816372.



© Fernando Granha Jeronimo, Tushant Mittal, Ryan O’Donnell, Pedro Paredes, and Madhur Tulsiani; licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 88; pp. 88:1–88:21

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

*Tushant Mittal*: Supported in part by NSF grant CCF-1816372.

*Ryan O'Donnell*: Supported by NSF grant FET-1909310.

*Pedro Paredes*: Supported by NSF grant FET-1909310.

*Madhur Tulsiani*: Supported by NSF grant CCF-1816372.

**Acknowledgements** We would like to thank the anonymous reviewers for their comments and helpful feedback.

## 1 Introduction

Graphs are ubiquitous in theoretical computer science and the ability to explicitly construct graphs with special properties can be quite useful. Two such properties are expansion and symmetry. 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.) The theory of *explicit* constructions of expander graphs has seen a dramatic development over the past four decades<sup>1</sup> [22, 23, 25, 30, 9, 8, 13, 24, 27, 2]. We now have constructions via diverse methods achieving a wide range of expansion guarantees. These range from very explicit algebraic constructions of so-called Ramanujan graphs [22] to recursive combinatorial ones based on the Zig-Zag product [30]. These constructions have a plethora of applications specially to coding theory and pseudorandomness [33]. A highly sought goal is to make the expansion of a family of (bounded) degree  $d$  graphs as close to the Ramanujan bound as possible, i.e., having largest non-trivial eigenvalue at most  $2\sqrt{d-1}$ . The Alon-Boppana bound [26] states that the largest non-trivial eigenvalue is at least  $2\sqrt{d-1} - o(1)$ , so the Ramanujan bound is in a sense optimal. This goal of achieving strong spectral guarantees has been an important motivation.

Moving beyond spectral guarantees, we can ask for graphs that combine the important property of expansion with additional structure and the one we focus on is *symmetry*<sup>2</sup>. One of the problems that has been studied in graph theory is to construct graphs with a given automorphism group. Frucht proved in 1939 that for every finite group  $H$ , we have a graph  $G$  such that  $\text{Aut}(G) = H$ . Babai [6] later showed that there is such a graph on at most  $2|H|$  vertices<sup>3</sup>. Thus, we have a natural question

*Can we explicitly construct expanding graphs with given symmetries?*

While interesting in its own right, the ability to control symmetries also has concrete applications. For example, a very recent work [16] constructs many families of expanding asymmetric graphs, i.e., having no symmetries, and shows applications to property testing and other areas. We will focus on an important connection to both quantum and classical codes that was the motivation behind this work.

Low-density parity check (LDPC) codes were first introduced by Gallager [15] in the '60s and are one of the most popular classes of classical error-correcting codes, both in theory and in practice. LDPC codes are linear codes whose parity check matrices have row and column weights bounded by a constant (which means that each parity check depends only on a constant number of bits). The popularity of this family of codes 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 [31].

<sup>1</sup> See [18] for an excellent survey on expander graphs.

<sup>2</sup> Informally, we say that  $G$  has symmetries of  $H$  if  $H \subseteq \text{Aut}(G)$ , where  $\text{Aut}(G)$  denotes the group of all graph isomorphisms to itself.

<sup>3</sup> Except for  $\mathbb{Z}_3$ ,  $\mathbb{Z}_4$  and  $\mathbb{Z}_5$ .

A family of codes that has been extensively studied is cyclic codes, i.e., codes that are invariant under the action of  $\mathbb{Z}_N$  where  $N$  is the blocklength. This symmetry leads to efficient encoding and decoding algorithms and a major open problem is whether good cyclic codes exist. Babai, Shpilka and Stefankovich [5] showed that cyclic codes cannot be good LDPC codes and this negative result was extended by Kaufman and Wigderson [20] to LDPC codes with a *transitive* action by an arbitrary abelian group.

Quasi-cyclic codes are a generalization of cyclic codes in which symmetry is only under rotations of multiples of a parameter (called index)  $n$  where  $N = n\ell$ . This is equivalent to relaxing the transitivity condition to allow for  $n$  orbits. Unlike cyclic codes, good quasi-cyclic codes are known to exist as was shown by Chen, Peterson and Weldon [12]. More recently, Bazzi and Mitter [7] gave a randomized construction for any constant  $n > 2$  and showed that it attains Gilbert–Varshamov bound rate  $1/n$ . Quasi-cyclic codes have been extensively studied and are very useful in practice (e.g., their LDPC counterparts are part of the 5G standard of mobile communication [21]).

In the realm of quantum computing, the fragility of qubits makes quantum error correcting codes crucial for the realization of scalable quantum computation. *Calderbank-Shor-Steane* (CSS) codes are a family of quantum error-correcting codes that was first described in [11, 32]. A CSS code is defined by a pair of classical linear codes that satisfy an orthogonality condition. The quantum analog of LDPC codes is thus defined as CSS codes where the parity check matrices of both codes have bounded row and column weights.

Constructing quantum LDPC codes of large distance has been active area of research recently. After two decades, [14] broke the  $\sqrt{N}$  barrier and there was a flurry of activity with [17] extending it to  $N^{3/5}$  (up to poly log factors). Panteleev and Kalachev [28] came up with another breakthrough construction achieving almost linear distance. Both [17] and [28] are non-explicit constructions crucially relying on symmetries. The construction in [28] interestingly used quasi-cyclic LDPC codes which in turn was constructed using expander graphs with cyclic symmetry. Moreover, Breuckmann and Eberhardt [10] introduced a new approach for constructing quantum codes simultaneously generalizing [17] and [28] in order to obtain explicit codes out of a pair of graphs having the symmetries of any group. This provides a very concrete motive to study explicit construction of expander graphs symmetric under various families of groups.

## Current Techniques

Many of the current known constructions of expanders are Cayley graphs and therefore are highly symmetric but are somewhat rigid in the sense that one may not be able to finely control the symmetries of a given construction. One general approach is to construct an expanding Cayley graph for a given group but the Alon–Roichman theorem [4] only guarantees a logarithmic degree which is tight when the group is abelian (and this large degree is undesirable for some application in coding theory). The other technique used to build expanders is via an operation called *lifting*.

In general form, the *random* lifting operation takes a lift size parameter  $\ell$ , a base expander graph  $G_0$  on  $n$  vertices and a subgroup  $H$  of the symmetric group,  $\text{Sym}(\ell)$ , and constructs a new “lifted” graph  $G$  on  $n\ell$  vertices where each vertex  $v$  of  $G_0$  is replaced by  $\ell$ -copies  $(v, 1), \dots, (v, \ell)$  and for every edge  $e = (u, v)$  of  $G_0$  a uniformly random element of  $h_e \in H$  is sampled and  $(u, i)$  is connected to  $(v, h_e(i))$  for  $i \in [\ell]$ . We say that  $G$  obtained this way is a *random*  $(H, \ell)$ -lift of  $G_0$ . We call it an *unstructured*  $\ell$ -lift if there is no restriction on the group, i.e.,  $H = \text{Sym}(\ell)$ .

Lifting has three very useful properties. One, it preserves the degree of the base graph. Secondly, random lifts preserve expansion<sup>4</sup> with high probability. Finally, (and importantly for us), if  $H$  is abelian, then the lifted graph inherits symmetries of  $H$ . The first two properties are clearly useful in constructing larger expanders from a small one, and for this reason, there has been extensive work on lift based constructions.

Bilu and Linial [9] introduced *2-lifts* in an explicit construction of graphs with expansion  $O(\sqrt{d} \log^{1.5}(d))$  for every degree. More recently, Mohanty, O’Donnell and Paredes [24] gave the first explicit construction of near-Ramanujan, i.e., largest non-trivial eigenvalue bounded by  $2\sqrt{d-1} + \epsilon$ , graphs of every degree. The key technique in their work was a finer derandomization of 2-lifts. Subsequently, Alon [2] gave explicit constructions of near-Ramanujan expanders of every degree and every number of vertices. The work in [24] was also generalized to achieve finer spectral guarantees together with local properties via *unstructured*  $\ell$ -lifts in O’Donnell and Wu [27].

When one restricts  $H$  to be abelian, Agarwal et al. [1] showed that *random*  $(\mathbb{Z}_\ell, \ell)$ -lifts (also known as *shift lifts*) are expanding. Motivated by the applications of these lifts to codes, we obtain explicit constructions of expanding abelian lifts, for a wide range of lift sizes.

## 1.1 Our Results and Techniques

Our construction of the lifts (and the expansion thereof) vary based on the parameter  $\ell$  and we make the following classification for ease in presenting the results. Let  $n, d, \epsilon$  be given.

- *Sub-Exponential* - This is the regime where  $\ell \leq \exp(n^{\delta(d,\epsilon)})$ . The exponent  $\delta(d,\epsilon)$  goes to zero as the degree ( $d$ ) increases or  $\epsilon$  vanishes.
- *Moderately-Exponential* - This is when  $\ell \leq \exp(n^{\delta_0})$ . The exponent is some fixed universal constant  $\delta_0 \in (0, 1)$ .
- *Exactly-Exponential* - This is the regime where  $\ell = \exp(\Theta_d(n))$ .

Our first main result shows explicit constructions in the sub-exponential and moderately exponential regimes.

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

- $G$  is  $(H, \ell)$ -lift of a graph  $G_0$  on  $\Theta(n)$  vertices.
- (*Sub-Exponential*) If  $\ell \leq \exp(n^{\delta(d,\epsilon)})$ , then  $\lambda(G) \leq 2\sqrt{d-1} + \epsilon$ .
- (*Moderately-Exponential*) If  $\ell \leq \exp(n^\delta)$  and also  $d \geq d_0(\epsilon)$ , then  $\lambda(G) \leq \epsilon \cdot d$ .

The bulk of the technical work is in the proof of Theorem 1. For this, we build on the techniques of [24] for derandomizing 2-lifts via the trace power method. When analyzing larger lift sizes (required in our derandomization of quantum and classical codes), we are led to consider much larger walk lengths in the trace power method. A central technical component in their work is the counting of some special walks which ultimately governs the final spectral bound of the construction. For lift sizes larger than  $2^{2^{\Theta(\sqrt{\log n})}}$ , their counting trivializes no longer implying expansion of the construction. Our main technical contribution consists in providing alternative ways of counting such special walks by carefully compressing the traversal of the depth-first search (DFS) algorithm.

---

<sup>4</sup> This holds for any lift size in the case of “unstructured”  $\ell$ -lifts, but only holds for  $\ell \leq 2^{O_d(n)}$  when  $H$  is abelian (and transitive).

We are able to extend the near-Ramanujan guarantee for 2-lifts from [24] to the entire sub-exponential regime of lift sizes  $\ell$ . In the moderately exponential regime, the walks are too long and we resort to another counting that can only guarantee an expansion of  $\varepsilon \cdot d$ . Theorem 1 can be seen (slight) simplification of the construction in [24] since we can now do a single large lift instead of performing a sequence of 2-lifts as in their work<sup>5</sup>.

Let us now formally state the results of Agarwal et al. in Theorem 2 showing *randomized* constructions of abelian lifts.

► **Theorem 2** (Agarwal et al. [1], Theorem 1.2). *Let  $G_0$  be a  $d$ -regular  $n$ -vertex graph, where  $2 \leq d \leq \sqrt{n/(3 \ln n)}$ . Let  $G$  be a random  $(\mathbb{Z}_\ell, \ell)$ -lift of  $G_0$ . Then*

$$\lambda(G) = O(\lambda(G_0)),$$

*with probability  $1 - \ell \cdot e^{-\Omega(n/d^2)}$ . Moreover, if  $\ell \geq \exp(O_\varepsilon(nd))$ , then no abelian  $(H, \ell)$  lift has  $\lambda(G) \leq \varepsilon \cdot d$ .*

This result is based on discrepancy methods building on the work of Bilu and Linial [9] and gives lower and upper bounds that are tight up to a factor of  $d^3$  in the exponent.

Theorem 1 can be seen as a (derandomization of the parameters) in Theorem 2 for every constant degree and lift size from 2 all the way to  $\exp(n^{\Theta_d(1)})$ . In the sub-exponential regime, our result improves their spectral guarantee from  $O(\sqrt{d})$  to  $2\sqrt{d-1} + \varepsilon$ .

Our second main result shows explicit constructions in the exponential regime. While it is not hard to observe that one can derandomize the exponential lift by using off-the-shelf tools, we give a short proof via a key lemma of Bilu and Linial [9] that is a converse of the expander mixing lemma. Although it gives a spectral guarantee that is weaker by a log factor, it yields an accessible proof and moreover, interpolates the exponent from  $\exp(O(n/d^2))$  all the way to the barrier of  $\exp(O(nd))$  thereby bridging the  $d^3$ -gap.

► **Theorem 3** (Exactly Exponential Lifts). *For any positive integers  $n, \ell$  and every constant degree  $d \geq 3$ , given  $\ell$ , the generating elements of a transitive abelian group  $H \leq \text{Sym}(\ell)$ , there exists a deterministic  $\text{poly}(\exp(n), \ell)$  time algorithm that constructs a  $d$ -regular graph  $G$  on  $n\ell$  vertices such that*

- $G$  is  $(H, \ell)$ -lift of a graph  $G_0$  on  $n$  vertices, and
- If  $\ell \leq \exp\left(\Theta\left(n/\sqrt{d}\right)\right)$ , then  $\lambda(G) \leq O\left(\sqrt{d} \cdot \log d\right)$ .
- If  $\ell = \exp\left(\Theta\left(nd^\delta\right)\right)$  for  $\delta \in [-1/2, 1)$ , then  $\lambda(G) \leq O\left(d^{\frac{2+\delta}{3}} \cdot \log d\right)$ .

*In particular, we have explicit polynomial time construction of a lift when  $\ell = \exp(\Theta(n))$ .*

## 1.2 Derandomized Quantum and Classical Codes

We first state the code constructions in [28] and then show how large explicit abelian lifts derandomize their codes.

► **Theorem 4** ([28]). *Let  $G$  be a  $d$ -regular graph on  $n\ell$ -vertices such that  $G$  has a symmetry<sup>6</sup> of  $\mathbb{Z}_\ell$  and  $\lambda_2(G) \leq \varepsilon \cdot d$ . Then we can construct the following,*

- A good quasi-cyclic LDPC code of block length  $N = \Theta(n\ell)$  and index  $\Theta(n)$ .
- A quantum LDPC code which has distance  $\Theta_{\varepsilon,d}(\ell)$  and dimension  $\Theta(n)$ .

<sup>5</sup> Performing a single lift also has the advantage of having to meet a technical condition (bicycle-freeness) only once instead of at each lift operation.

<sup>6</sup> To be more precise,  $\mathbb{Z}_\ell$  acts freely on  $G$ .

Panteleev and Kalachev use the aforementioned *randomized* construction of abelian lifted expanders by Agarwal et al. [1], where each edge of the base graph is associated with an element in  $\mathbb{Z}_\ell$  sampled uniformly. When  $\ell$  is in the exponential regime they obtain quantum LDPC codes with almost linear distance, i.e.,  $\Omega(N/\log(N))$ .

Breckmann and Eberhardt [10] gave a derandomization of [28] in a more restricted parameter regime by observing that the Ramanujan graph construction by Lubotsky, Philips and Sarnak [22] of size  $n$  has a (free) action of  $\mathbb{Z}_{n^{1/3}}$ . By Theorem 4, we have an explicit quantum LDPC code of distance  $O(N^{1/3})$  under the notion of distance<sup>7</sup> in [28, 17].

As a direct corollary of Theorem 3, we have a complete derandomization of [28] yielding explicit quantum LDPC codes of almost linear distance. This greatly improves the distance of the existing explicit construction. We also get good quasi-cyclic LDPC codes of almost linear circulant size. Moreover, the ability to construct a wide range of lift sizes from Theorem 1 lets us control the circulant size which can be useful in practice. By controlling the lift size, we can also directly amplify the rate of their quantum LDPC codes (without resorting to the product of complexes). To summarize,

► **Corollary 5** ([28], Theorem 1, Theorem 3). *We have explicit polynomial time construction of each of the following,*

- *Good quasi-cyclic LDPC code of block length  $N$  and any circulant size up to  $N/\text{polylog}(N)$  or  $\Theta(N/\log(N))$ .*
- *Quantum LDPC code with distance  $\Omega(N/\log(N))$  and dimension  $\Omega(\log(N))$ .*
- *Quantum LDPC code with distance  $\Omega(N^{1-\alpha})$  and dimension  $\Theta(N^\alpha)$  for every constant  $\alpha > 0$ .*

## Further Directions

Our work also leads to several natural avenues for further exploration.

1. *More Symmetries* - While these lift-based constructions yield graphs with symmetries arising from abelian groups, it is interesting to understand whether one can construct sparse graphs with symmetries corresponding to other families of groups. Such constructions may require new ways of using the symmetry groups, in ways other than in lifts of a base graph. More generally, it may be useful to investigate other ways of exploiting graph symmetry, beyond their applications to codes.
2. *Better notions of explicitness* - It is a very interesting problem to find strongly explicit constructions of lifted abelian expander. Even making the running time closer to linear would be interesting. Also, since quasicyclic codes are widely used in practice, it may be helpful to find explicit constructions which are efficiently implementable.
3. *Complete Range* - Can we derandomize abelian lifts for  $\ell$  in between  $2^{n^{\Theta(1)}}$  and  $2^{O_d(n)}$ ? Can we extend the near-Ramanujan bound beyond the subexponential range?

## 2 Preliminaries

For an operator  $M$ , let its eigenvalues be ordered such that  $\{|\lambda_1(M)| \geq \dots \geq |\lambda_n(M)|\}$ . We define  $\rho_2(M) = |\lambda_2(M)|$ . For an  $n$ -vertex graph  $G = (V, E)$ , we denote by  $\lambda(G) = \rho_2(A)$ , where  $A$  is its adjacency operator.

We assume that we have an ordering on  $V$  and by convention,  $(u, v) \in E$  if  $u \leq v$ .

<sup>7</sup> [10] state their result for a slightly different notion of a quantum codes called subsystems codes for which the corresponding distance (also known as dressed distance) is larger.

A *character*<sup>8</sup> of a group is a map  $\chi : H \rightarrow \mathbb{C}^*$  that respects group multiplication, i.e.,  $\chi(h_1 h_2) = \chi(h_1)\chi(h_2)$ . For a finite group  $|\chi(h)| = 1$  for every  $h \in H$ . The *trivial character* is the one which has  $\chi(h) = 1$  for every  $h$ . The rest of the characters we call *non-trivial*.

The action of a group  $H$  on a set of  $\ell$  elements is defined by a map  $\psi : H \rightarrow \text{Sym}(\ell)$  which satisfies  $\psi(h_1 h_2) = \psi(h_1)\psi(h_2)$ . Since we only care about the action of the group, we will assume that our input is actually  $\psi(H) \subseteq \text{Sym}(\ell)$  and the action is the natural one.

► **Definition 6** ( $(H, \ell)$ -lift of a graph). An  $(H, \ell)$ -signing of an undirected graph  $G = (V, E)$  is a function  $s : E \rightarrow H \subseteq \text{Sym}(\ell)$ . The lifted graph  $G(s) = (V', E')$  is a graph on  $\ell$  copies of the vertices  $V' = V \times [\ell]$  where for every edge  $(u, v) \in E$  we have  $((u, i), (v, s(u, v) \cdot i)) \in E'$

We will restrict to analyzing abelian  $H$  and the most important case to consider is when  $H = \mathbb{Z}_\ell$ , i.e. the cyclic group. 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. Thus, we will assume henceforth that we work with transitive abelian subgroups.

Let  $E^d$  denote the set of directed edges i.e.  $E^d = \{(u, v), (v, u) \mid (u, v) \in E\}$ . We extend the signing to  $E^d$  such that for an edge  $(u, v) \in E$ ,  $s(v, u) := s(u, v)^{-1}$ .

► **Definition 7** (Non-backtracking walk operator). For an extended signing  $s : E^d \rightarrow H$  and a character  $\chi$  of  $H$ , the signed non-backtracking walk matrix  $B_s(\chi)$  is a non-symmetric matrix of size  $|E^d| \times |E^d|$  in which the entry corresponding to the pair of edges  $(u, v), (x, y)$  is  $\chi(s(x, y))$  if  $v = x$ ,  $u \neq y$ , and zero otherwise.

The unsigned variant is obtained by taking the trivial character in the definition above. Let the non-backtracking walk matrix of  $G$  be  $B$  and the lifted graph with respect to a signing  $s$  be  $B_{G(s)}$ . We use the following standard facts.

► **Fact 8.** Let  $B$  be the non-backtracking walk matrix of a  $d$ -regular graph  $G$ . Then,

$$\lambda(G) \leq 2 \cdot \max\{\sqrt{d-1}, \rho_2(B)\}.$$

► **Fact 9.** If  $H \subseteq \text{Sym}(\ell)$  is abelian, then there exist characters  $\{\chi_1, \dots, \chi_\ell\}$ <sup>9</sup> such that we have  $\text{Spec}(B_{G(s)}) = \bigcup_i \text{Spec}(B_s(\chi_i))$ . If  $H$  is transitive, then exactly one of the characters is trivial.

### 3 Proof Strategy

We give an overview of the proof of Theorem 1. As mentioned earlier, our results build on the work of Mohanty, O'Donnell and Paredes [24], so we briefly recall notions and ideas from their work that we will need. Let  $G_0$  be a base expander graph and  $s : E_0 \rightarrow \mathbb{Z}_2$  be a signing that defines a lift. It is convenient to first think that the signing is chosen uniformly at random and later see which properties were indeed used so that an appropriate derandomization tool may be used. Using well known facts (Fact 8 and Fact 9) they reduce the problem of analyzing the expansion of the lifted graph to that of bounding the spectral radius of the non-backtracking operator  $B_s$ .

<sup>8</sup> The definition we give is that of a *linear character*. We use the term character as we work only with abelian groups.

<sup>9</sup> These need not be distinct. For example if  $H$  is trivial, then all the  $\chi_i$  are trivial

**The MOP Argument**

A common technique to bound the spectral radius is the trace power method which in our case amounts to counting special non-backtracking walks. This is the motivation for using the non-backtracking operator  $B_s$  instead of the more common adjacency operator which require counting closed walks (which is potentially harder). Another standard fact<sup>10</sup> is that

$$\rho(B_s)^{2k} \leq \text{tr}((B_s^*)^k B_s^k) = \sum_{\substack{(e_1, \dots, e_{2k}) \\ \text{closed edge walk}}} \prod_{i=1}^{2k} \chi(s(e_i)).$$

The above expression greatly simplifies when we take the expectation over a uniformly random signing since only walks in which every edge occurs at least twice stand a chance of surviving the expectation. These walks are called singleton free in [24]. We have

$$\mathbb{E}_{s \in \mathbb{Z}_2^{E_0}} [\rho(B_s)^{2k}] \leq \sum_{\substack{(e_1, \dots, e_{2k}) \\ \text{closed edge walk}}} \mathbb{E}_{s \in \mathbb{Z}_2^{E_0}} \left[ \prod_{i=1}^{2k} \chi(s(e_i)) \right] \leq \left| \left\{ \begin{array}{c} 2k\text{-length singleton free} \\ \text{non-backtracking walks in } G_0 \end{array} \right\} \right|,$$

reducing the problem of bounding the spectral radius to a counting problem of these special walks. In the hypothetical (idealized) scenario of  $G_0$  being Ramanujan and the counting on the RHS above being  $(d - 1)^k$ , we would have a Ramanujan lift. The above expression also hints that  $\epsilon$ -bias distributions might be a useful derandomization tool here. This idealized scenario can be too optimistic and the count of  $(d - 1)^k$  has additional factors, but they remain small after taking a  $2k$ -th root (when  $k$  is neither too small or large).

One of the main technical contributions in [24] is the counting of  $2k$ -length singleton free non-backtracking walks in  $G_0$ , which they call hikes. For the sake of intuition, we will assume that  $G_0$  has girth  $g$ , but it is not hard to modify the argument when  $G_0$  has at most one cycle around any neighborhood of radius  $< g/2$  centered at vertex in  $G_0$  (the bicycle freeness property). They view the vertices and edges visited in a hike as forming a hike graph  $\mathcal{H}$ . Assuming that  $g = \Omega(\log_{d-1}(n))$ , if  $k$  is not too large, then  $\mathcal{H}$  looks like a tree possibly with a few additional edges forming cycles as established by Alon, Hoory and Linial in [3] (and generalized in [24] to bicycle-free radius from girth).

Assuming that the hike is singleton free, we can have at most  $k$  steps that visit an edge that was not previously visited. This implies that the hike graph  $\mathcal{H}$  has at most  $k$  edges and at most  $k + 1$  vertices (since it is connected). They count the number of these special walks by directly specifying an encoding for the hike. Up to negligible factors (after  $2k$ -th root for  $k$  not too small), they show that there are at most

$$n \cdot (d - 1)^k \cdot k^{O\left(\frac{\ln(k)}{g}\right)},$$

singleton free hikes of length  $2k$  (see [24, Theorem 3.9] for precise details). This bound trivializes, i.e., it becomes at least  $(d - 1)^{2k}$ , for  $\ln(k) \gg \sqrt{g} = \Theta(\sqrt{\log_{d-1}(n)})$ . This means that we cannot use their bound for very long walks and this in turn prevents us from getting lift sizes larger than  $2^{2^{\Theta(\sqrt{\log_{d-1}(n)})}}$  from their results.

---

<sup>10</sup>To avoid discussing some unimportant technicalities, we will make some simplifications in this high-level overview.



## Our Approach

Now, let's consider  $\mathbb{Z}_\ell$  lifts for large  $\ell$ . The spectral radius of each individual  $B_s(\chi)$  can be analyzed in a similar fashion as above via the trace power method. However, we need to bound all of them *simultaneously*. We know no better way than a simple union bound over the  $\ell - 1$  cases, but this will force us to obtain a much better concentration guarantee out of the trace power method which in turn entails having to consider much larger walk lengths.

Instead of encoding a hike directly as in [24], we will first encode the subgraph of  $G_0$  traversed by the hike, which we call hike graph, and then encode the hike having the full hike graph at our disposal. We will give two different encodings for the hike graph. The first one is simpler and can encode an arbitrary graph. The second encoding uses the special structure of the hike graph, namely, having few vertices of degree greater than 2. Both encodings are based on the traversal history of the simple depth-first search (DFS) algorithm. Let  $\mathcal{H}$  be the hike graph on  $m \leq k$  edges and  $n' \leq k + 1$  vertices. As DFS traverses  $\mathcal{H}$ , each of its edges will be visited twice: first “forward” via a recursive call and later “backwards” via a backtracking operation. We view each step of the DFS traversal as being associated with an edge that is being currently traversed and the associated type of traversal: recursive (R) or backtracking (B). A key observation is that only for the recursive traversals we need to know the next neighbor out of  $d - 1$  possibilities (except for the first step). For the backtracking steps, we can rely on the current stack of DFS. Thus, if we are given a starting vertex from  $G_0$ , a binary string in  $\{R, B\}^{2m}$  and a next neighbor for each recursive step, we can reconstruct  $\mathcal{H}$ . Note that there are at most

$$n \cdot d \cdot (d - 1)^k \cdot 2^{2k},$$

such encodings. Having access to the hike graph and again assuming that the graph has girth  $g = \Omega(\log_{d-1}(n))$  (similarly, bicycle freeness is also enough). Using the locally tree-like structure, a  $2k$ -length hike can be specified by splitting it into segments of length  $< g/2$ , by specifying the starting vertex of the first segment and the ending vertex of each segment, we have enough information to recover the full hike. Note that there are at most

$$k^{O(k/g)},$$

ways of encoding a hike. Then, the number of  $2k$ -hikes in  $G_0$  is at most

$$n \cdot d \cdot (d - 1)^k \cdot 2^{2k} \cdot k^{O(k/g)}.$$

Now we can take  $k \approx n^\delta$  for a sufficiently small  $\delta = \delta(d) > 0$  and obtain, after taking the  $2k$ -th root of the above quantity,

$$\rho(B_s) \leq (1 + \epsilon) \cdot 2 \cdot \sqrt{(d - 1)},$$

when  $k = k(n, d, \epsilon)$  is sufficiently large and  $c = c(\epsilon)$  is sufficiently small. The extra factor 2 prevent us from obtaining near-Ramanujan bounds with this counting. Nonetheless, the simple counting already allows us to obtain expansion  $O(\sqrt{d})$  for lifts sizes as large as  $2^{n^{\delta(d)}}$ . Moreover, by weakening the expansion guarantee we can obtain lift sizes as large as  $2^{n^{\Theta(1)}}$  from this counting and obtain part of Theorem 1. If we insist on getting a near-Ramanujan bound, we need to compress the traversal history further since storing a string  $\{R, B\}^{2m}$  is too costly and leads to this factor of 2. Note that this string has an equal number of  $R$  and  $B$  symbols, so it cannot be naively compressed.

To obtain a near-Ramanujan graph, we will take advantage of the special structure of the hike graph (when the walk length is large but not too large) in which most of its vertices have degree exactly 2. These degree 2 vertices are particularly simple to handle in a DFS

traversal. For them, we only need to store the next neighbor out of  $d - 1$  possibilities in  $G_0$  (except possibly for the first step). In a sequence of backtrackings, if the top of the DFS stack is a degree 2 vertex we know that we are done processing it since no further recursive call will be initiated from it. Then, we simply pop it from the stack. It is for the “rare” at most  $\delta \cdot n'$  vertices  $v$  of degree  $\geq 3$  that we need to store how many extra recursive calls  $t_v$  we issue from  $v$  and a tuple of additional next neighbors  $(d_1, \dots, d_{t_v})$ . The total number of such encodings is at most

$$n \cdot d \cdot (d - 1)^k \cdot \binom{k + 1}{\delta(k + 1)} \cdot (d - 1)^{\delta(k+1)},$$

which combined with the same previous way of encoding a hike given its graph results in a total number of hike encodings of  $G_0$  of at most

$$n \cdot d \cdot (d - 1)^k \cdot \binom{k + 1}{\delta(k + 1)} \cdot (d - 1)^{\delta(k+1)} \cdot k^{O(k/g)},$$

By choosing  $\delta = \delta(d, \epsilon)$  sufficiently small and taking  $k = k(n, d, \epsilon) \leq 2^{\delta \cdot g} \approx n^{O_a(\delta)}$  sufficiently large, we obtain after taking the  $2k$ -th root

$$\rho(B_s) \leq \sqrt{(d - 1)} + \epsilon,$$

indeed leading to a near-Ramanujan bound for lifts as large as  $2^{n^\delta}$  in Theorem 1.

Now we briefly explain how to handle the union bound to ensure that  $\rho(B_s(\chi))$  is *simultaneously* small for all  $(\ell - 1)$  non-trivial characters (in the decomposition of Fact 9). This union bound is *standard* when using the trace power method, what is relevant is the trade-off between lift size and walk length. To obtain a high probability guarantee from a guarantee on expectation, it is standard to consider larger walk lengths from which concentration follows from a simple Markov inequality. More precisely, if for some function  $f$ ,  $\mathbb{E}\rho(B_s(\chi_j))^{2k} \leq f(n, d, g, k)$ , then by Markov’s inequality,

$$\Pr_{s \in \mathbb{Z}_\ell^{E_0}} \left[ \rho(B_s(\chi)) \geq 2^{\log_2(\ell)/(2k)} \cdot f(n, d, g, k)^{1/(2k)} \right] \leq \frac{1}{\ell}.$$

Therefore, for  $k \geq \log_2(\ell)$  sufficiently large, we can union bound over all characters  $\chi$  and obtain similar bounds as before. As alluded above, this lower bound on the length of the walk depending on the lift size is the reason why we are led to consider much longer walks. To conclude this proof sketch, we need to replace a random signing by a pseudorandom random one. As in [24], we use  $\epsilon$ -biased distributions but suitably generalized to abelian groups, e.g., the one<sup>11</sup> by Jalan and Moshkovitz in [19]. We may be taking very large walks on the base graph  $G_0$ , so the error of the generator needs to be smaller than  $n \cdot d^{2k}$ , where  $k$  can be as large as  $n^{\Theta(1)}$ . We note that as long as the degree  $d$  is a constant this quantity is at most a polynomial in the size of the *final* lifted graph  $G$  since walks of length  $O(\log(|V(G)|))$  suffice for any lift size up to full extent of  $2^{O(n)}$ , for which abelian lifts can be expanding.

The above argument covers Theorem 1, namely, the sub-exponential and moderately-exponential abelian lift sizes. The “exact” exponential regime of Theorem 3 relies on an elegant converse of the expander mixing lemma by Bilu and Linial [9]. Since this regime is simpler, we defer the details to Section 6, where it is formally presented.

<sup>11</sup> For our application, it suffices to have the support size of the  $\epsilon$ -biased distribution polynomial in  $1/\epsilon$ .

## 4 A New Encoding for Special Walks

In this section, we will count the total number of singleton-free hikes of a given length on a fixed graph,  $G$ . We split the count into two parts. First, we count the number of possible hike graphs and then, for a given hike graph  $\mathcal{H}$ , we count the number of hikes that can i.e., yield  $\mathcal{H}$  on traversal. Each of these counts is via an encoding argument and therefore we have two kinds of encoding. One for graphs and the other for hikes. In the first part of the section we give two ways of encoding graphs, and in the other half, we encode hikes. Since the first section is a general encoding for subgraphs, we relegate formal definitions related to hikes to a later section.

### 4.1 Graph Encoding

Let  $\mathcal{H}$  be a subgraph of a fixed  $d$ -regular graph  $G$ . We wish to encode  $\mathcal{H}$  in a succinct way such that given the encoding and  $G$ , we can recover  $\mathcal{H}$  uniquely. We will give two ways of encoding  $\mathcal{H}$ . The first one will be generic that works for any subgraph of a  $d$ -regular graph. The second encoding takes advantage of the special sparse structure (not too many vertices of degree greater than two). We assume that we have an order on the neighbors of every vertex, and thus, given  $(v, j)$ , we can access the  $j^{\text{th}}$  neighbor of  $v$  efficiently.

We will do this by encoding a DFS based-traversal of it from a given start vertex. Here, we really need our DFS traversal to be optimal in the sense that the number of times each edge is traversed is at most two and not any higher.

To reconstruct the graph, we reconstruct the traversal and so need access to two types of data before every step - (1) Is this step recursive or backtracking (2) If it is a recursive step, then which neighbour do we recurse to.

To determine the neighbor of the current vertex we need to move to in a recursive call we need to specify one out of  $d - 1$  possibilities (except in the first step which has  $d$  possibilities). This can be specified by a tuple  $(d_1, \dots, d_{|E(\mathcal{H})|}) \in [d] \times [d - 1]^{|E(\mathcal{H})|-1}$  indicating the neighbor. For a backtracking step, we just pop the stack and thus don't need any additional data.

We use two ways to figure out whether a step is recursive or backtracking. The direct way is to just record the sequence in a binary string of length  $2|E(\mathcal{H})|$ . A neighbour  $u$  of  $v$  is called *recursive* if the edge  $(v, u)$  is visited by a recursive call from  $v$ . A simple observation about backtracking sequences is that - It starts when we encounter a vertex that has already been visited or we reach a degree one vertex and ends when we see a visited vertex that has unvisited recursive neighbors. Therefore, we store a string  $\sigma \in [d] \times [d - 1]^{|V(\mathcal{H})|-1}$  in which  $\sigma_i$  denotes the number of recursive neighbors of the  $i^{\text{th}}$  visited vertex. To summarize, **GraphEnc**( $\mathcal{H}$ ):

- (a) Starting vertex  $v_1 \in V(G)$
- (b) A sequence of degrees  $(d_1, \dots, d_{|E(\mathcal{H})|}) \in [d] \times [d - 1]^{|E(\mathcal{H})|-1}$
- (c) Either  $\sigma \in \{R, B\}^{2|E(\mathcal{H})|}$  (**Encoding I**) or  $\sigma \in [d] \times [d - 1]^{|V(\mathcal{H})|-1}$  (**Encoding II**)

#### 4.1.1 Counting the encodings

For the first kind of encoding of type, we have  $2^{2k}$  strings of length  $2k$  over  $\{R, B\}$ . The second encoding might seem wasteful in general but it is much better when the graph has special structure that our hike graph will satisfy. We first note that for any vertex  $v$ , the number of recursive neighbours  $\sigma_v \leq \text{deg}_{\mathcal{H}}(v) - 1$  (or  $\leq \text{deg}_{\mathcal{H}}(v)$  if  $v = v_0$ ).

► **Definition 10** (Excess). *The excess of  $\mathcal{H}$  is defined as  $\text{exc}(\mathcal{H}) := |E(\mathcal{H})| - |V(\mathcal{H})|$ .*

► **Definition 11** (Excess Set). We define a vertex to be an excess vertex in  $\mathcal{H}$  if  $\deg_{\mathcal{H}}(v) > 2$  and we define the excess set to be the set consisting of such vertices i.e

$$\text{excSet}(\mathcal{H}) := |\{v \in V(\mathcal{H}) \mid \deg(v) > 2\}|.$$

► **Lemma 12.** Let  $G$  be a fixed  $d$ -regular graph on  $n$  vertices. The total number of connected subgraphs  $\mathcal{H}$  of  $G$  having at most  $\leq k$  edges is at most

$$2n \cdot d \cdot (d-1)^{k-1} \cdot 2^{2k}$$

Moreover, if  $\mathcal{H}$  is constrained to have at most two vertices of degree one<sup>12</sup> and  $\text{exc}(\mathcal{H}) \leq \delta k$ , the count is at most

$$2nk^3 \cdot d \cdot (d-1)^{k-1} \cdot 2^{H_2(\frac{\delta}{1-\delta})k} \cdot d^{\delta k}$$

**Proof.** We first fix the number of edges as  $m$  and we will then sum up the expression for  $m \leq k$ . It is not hard to see that we can unambiguously recover the graph<sup>13</sup> and therefore the number of possible graphs can be counted by counting the number of possible inputs. The number of degree sequences and start vertices are  $n \cdot d(d-1)^{m-1}$ . The number of  $\sigma$ -strings of encoding I are  $2^{2m}$ . Therefore for a given  $m$ , we have  $nd \cdot (d-1)^{m-1} \cdot 2^{2m}$  and summing this gives the first claim.

In the second case, the key idea is that for every vertex (except the start) of degree 2,  $\sigma_v$  must be 1. Since  $|\text{excSet}(\mathcal{H})| \leq \delta m$ , almost all of the string  $\sigma$  is filled by 1.

We first pick the number of vertices, say  $t$ . There are at most  $m$  choices for this. Then, we let the number of excess vertices be  $j$ . Summing over all possible  $j$ , the number of  $\sigma$ -strings of length  $t$  is  $\leq t^2 \sum_{j=0}^{\delta m} \binom{t}{j} d^j \leq t^2 d^{\delta m} \sum_{j=0}^{\delta m} \binom{t}{j} \leq t^2 d^{\delta m} 2^{H_2(\frac{\delta}{1-\delta})t}$ .

Here the first term counts the ways of having or up to two vertices of degree 1, the second counts the ways to choose the excess vertices and the third counts the number of their recursive neighbours. In the last inequality we used that  $t = m - \text{exc}(\mathcal{H}) \geq (1-\delta)m$ .

The complete expression for the number of graphs would then be

$$\sum_{m \leq k} \left( nd(d-1)^{m-1} \sum_{t=(1-\delta)m}^m t^2 d^{\delta m} 2^{H_2(\frac{\delta}{1-\delta})t} \right) \leq 2nk^3 \cdot d \cdot (d-1)^{k-1} \cdot 2^{H_2(\frac{\delta}{1-\delta})k} \cdot d^{\delta k}. \blacktriangleleft$$

## 4.2 Bounding Singleton Free Hikes

Following [24], we make the following useful definitions,

► **Definition 13** (Singleton-free hikes). A  $k$ -hike  $W$  is a closed walk of  $2k$ -steps<sup>14</sup> in  $G$  in which every step except possibly the  $(k+1)^{\text{st}}$  is non-backtracking. A hike is singleton-free if no edge is traversed exactly once.

► **Definition 14** (Bicycle free radius [24]). A graph  $G$  is said to have a bicycle-free radius at radius  $r$  if the subgraph  $\mathcal{H}$  of distance- $r$  neighborhood of every vertex has  $\text{exc}(\mathcal{H}) \leq 0$ .

We will work with singleton-free hikes in this section. A singleton-free  $k$ -hike on  $G$  defines a subgraph  $\mathcal{H}$  such that there at most two vertices of degree 1 (the start vertex and the middle vertex) and the number of edges is at most  $k$  as every edge is traversed at least twice. The goal now is to count the possible number of singleton-free  $k$ -hikes that yield a fixed subgraph  $\mathcal{H}$ . Having access to  $\mathcal{H}$ , we will need to encode the hike in a way similar to the encoding of stale stretches in [24].

<sup>12</sup>We will see later that hike graphs satisfy this strange property

<sup>13</sup>We include a detailed algorithm to do so in the full version.

<sup>14</sup>That is sequence of  $(v_0, \dots, v_{2k-1})$  such that  $(v_i, v_{i+1}) \in E(G)$  and  $v_0 = v_{2k-1}$

### HikeEnc

1.  $(v_1, \dots, v_s) \in V(\mathcal{H})^s$ , where  $s = \lceil 2k/r \rceil$  and  $r$  is the bicycle free radius of  $\mathcal{H}$
2.  $(c_1, \dots, c_s) \in \{0, \pm 1, \dots, \pm \lfloor r/2 \rfloor\}^s$ . Here,  $c_i$  denotes the number of times the unique cycle (in the neighborhood of  $v_i$ ) is to be traversed and the sign indicates the orientation. Since each stretch is of length  $r$  and each cycle of length at least 2 we can traverse a cycle at most  $\lfloor r/2 \rfloor$  times.

▷ **Claim 15.** For any graph  $\mathcal{H}$  that is bicycle free at radius  $r$ , the number of simple singleton-free  $k$ -hikes that have  $\mathcal{H}$  as their hike graph is at most  $(|rV(\mathcal{H})|)^{\lceil 2k/r \rceil}$ .

Proof. Follows from the possible values the encoding **HikeEnc** can take. ◀

We use a generalization of the bound of Alon et al. [3] on the excess number (originally involving the girth), extended to bicycle-free radius in [24].

► **Theorem 16** ([24, Theorem 2.13]). *Let  $\mathcal{H}$  be a bicycle free graph of radius  $r \geq 10 \ln(|V(\mathcal{H})|)$ . Then*

$$\text{exc}(\mathcal{H}) \leq \frac{\ln(e|V(\mathcal{H})|)}{r} \cdot |V(\mathcal{H})|.$$

► **Corollary 17.** *Let  $G$  be a  $d$  regular graph on  $n$  vertices bicycle free at radius  $r$ . Let  $\mathcal{H}$  be a subgraph with at most two vertices of degree one on  $n_0$  vertices where  $n_0 = e^{\delta r - 1}$  for some  $\delta \leq 1/10$ . Then,*

$$\text{excSet}(\mathcal{H}) \leq 2\delta n_0 + 2.$$

► **Lemma 18.** *Let  $G$  be a  $d$  regular graph, with  $d \geq 3$ , on  $n$  vertices bicycle free at radius  $r$ . Then, the total number of singleton free  $(k-1)$ -hikes on  $G$  is at most*

$$\left(2^{\gamma_1} \sqrt{d-1}\right)^{2k} \text{ where } \gamma_1 = 1 + \frac{\log(nrk)}{2k} + \frac{\log(rk)}{r}.$$

*If we assume that  $3 \leq k \leq e^{\delta r}$ , then it is at most*

$$\left(2^{\gamma_2} \sqrt{d-1}\right)^{2k} \text{ where } \gamma_2 = \frac{\log(16nk^3rd)}{2k} + \frac{\log(rk)}{r} + H_2(5\delta)/2 + \delta \log d.$$

**Proof.** Follows mainly from Lemma 12 and Claim 15. Complete proof can be found in the full version. ◀

## 5 Instantiation of The First Two Main Results

In this section, we will use the bound on singleton-free hikes obtained in the last section to bound the eigenvalue of the lifted graph. We first handle non-singleton free hikes and show that they can be easily bounded by the  $\varepsilon$ -biased property of the distribution of the signings. We then formalize the construction by instantiating it using an expander from MOP having large bicycle-free radius and then bring the bounds together.

### 5.1 A Simple Generalization of The Trace Power Method in MOP

We now show that the problem of bounding the spectral radius of the signed non-backtracking operator reduces to counting singleton-free hikes. This reduction is a straightforward generalization of the argument [24, Prop. 3.3] for  $\mathbb{Z}_2$  to any abelian group.

## 88:14 Explicit Abelian Lifts and Quantum LDPC Codes

Let  $B_s(\chi)$  (as defined in Definition 7) be the signed non-backtracking operator with respect to a signing and a non-trivial character  $\chi$  and  $\rho(B_s)$  denote its spectral radius. The goal is to bound the largest eigenvalue of  $B_s(\chi)$ . The trace method is the name for utilizing the following inequality,

$$\text{tr}((B^*)^k B^k) = \|B^k\|_F^2 = \sum_i |\lambda_i^k|^2 \geq \rho(B)^{2k}.$$

The signing  $s$  is drawn from some distribution  $\mathcal{D}$  and we wish to show via the probabilistic method that there exists a signing in  $\mathcal{D}$  for which  $\rho(B_s(\chi))$  is small for any set of  $(l-1)$  non-trivial characters  $\chi$ . We will use a first-order Markov argument and therefore wish to bound  $\mathbb{E}_{s \sim \mathcal{D}} \text{tr}(B_s^k (B_s^*)^k)$ . Writing it out we get,

$$\begin{aligned} T_\chi(s) &= \text{tr}((B_s^*)^k B_s^k) = \sum_{e \in E^d} ((B_s^*)^k B_s^k e)_e \\ &= \sum_{(e_0, \dots, e_{2k})} B(e_0, e_1) \cdots B(e_{k-1}, e_k) B^*(e_k, e_{k+1}) \cdots B^*(e_{2k-1}, e_{2k}) \\ &= \sum_{(e_0, \dots, e_{2k})} \chi(s(e_1)) \cdots \chi(s(e_k)) \chi^*(s(e_{k+1})) \cdots \chi^*(s(e_{2k})) \\ &= \sum_{(e_0, \dots, e_{2k})} \chi(s(e_1)) \cdots \chi(s(e_{k-1})) \chi^*(s(e_{k+1})) \cdots \chi^*(s(e_{2k})). \end{aligned}$$

Notice that  $e_0, e_k$  don't appear in the term and so we define  $\mathcal{H}_{k-1}$  as the multiset of all tuples  $(e_1, \dots, e_{k-1}, e_{k+1}, \dots, e_{2k-1})$  appearing in the support of this summation. We denote each term in the summation above by  $\chi_w(s)$  where  $w \in \mathcal{H}_{k-1}$ . It follows directly from the definition that each  $w \in \mathcal{H}_{k-1}$  defines a  $(k-1)$ -hike. Also observe that, any tuple appears at most  $(d-1)^2$  times as given a tuple  $w$ , we have at most  $(d-1)$  choices for each  $e_0, e_k$ . Let  $\mathcal{H}_{k-1}^s$  denote the singleton-free hikes in  $\mathcal{H}_{k-1}$ . We can split  $T_\chi(s) = T_1(s) + T_2(s)$  where

$$T_1(s) = \sum_{w \in \mathcal{H}_{k-1}^s} \chi_w(s), \quad T_2(s) = \sum_{w \notin \mathcal{H}_{k-1}^s} \chi_w(s).$$

We now define  $\varepsilon$ -biased distributions that will be the key pseudorandomness tool.

► **Definition 19 (Bias).** *Given a distribution  $\mathcal{D}$  on a group  $H$  and a character  $\chi$ , we can define the bias of  $\mathcal{D}$  with respect to  $\chi$  as  $\text{bias}_\chi(\mathcal{D}) := |\mathbb{E}_{h \sim \mathcal{D}} \chi(h)|$  and the bias of  $\mathcal{D}$  as  $\text{bias}(\mathcal{D}) = \max_\chi \text{bias}_\chi(\mathcal{D})$ , where the maximization is over non-trivial characters.*

► **Lemma 20.** *Let  $\mathcal{D} \subseteq H^{E(G)}$  be an  $\nu$ -biased distribution and let  $w \notin \mathcal{H}_{k-1}^s$  be a singleton-hike i.e. there is an edge that is travelled exactly once. Then,  $|\mathbb{E}_{s \sim \mathcal{D}} \chi_w(s)| \leq \nu$ .*

**Proof.** Let the set of distinct edges in  $w$  be  $\{e_1, \dots, e_r\}$  and let edge  $e_i$  be travelled  $t_i$  times where  $t_i$  takes the sign into account.<sup>15</sup> Let  $e_j$  be the edge traversed exactly once. Then,  $t_j = \pm 1$ . Now, we can rewrite  $\chi_w(s) = \prod_{i=1}^r \chi(s(e_i))^{t_i}$  and it can be extended to a character on  $H^{E(G)}$ . Since  $t_j = \pm 1$ , this character is non-trivial and the claim follows from the  $\nu$ -biased property. ◀

<sup>15</sup> Let  $e_i$  appear  $f_1$  times in the first  $k-1$  steps and  $b_1$  times in the next  $(k-1)$  steps. Similarly let  $e_i^T$  which is the reverse direction of  $e$  appear  $f_2$  times in the first  $k-1$  steps and  $b_2$  times in the next  $(k-1)$  steps. Then,  $t_i = f_1 + b_2 - f_2 - b_1$ .

► **Lemma 21** (Analog of Corr. 3.11 in [24]). *Let  $G$  be a  $d$ -regular graph on  $n$ -vertices,  $\varepsilon < 1$  be a fixed constant,  $\ell$  be a parameter,  $H \subseteq \text{Sym}(\ell)$  be an abelian group and  $\mathcal{D} \subseteq H^m$  be an  $\nu$ -biased distribution such that  $\nu \leq (n\ell d^2)^{-1} \cdot \left(\frac{\varepsilon}{d}\right)^{2k}$ .*

*Assume that the number of singleton-free  $(k-1)$ -hikes is bounded by  $(2^\gamma \sqrt{d-1})^{2k}$ . Then for any non-trivial character  $\chi$  of  $H^m$ , we have that except with probability at most  $1/\ell$  over  $\mathcal{D}$ ,  $\rho(B(\chi)) \leq 2^{\gamma'} \sqrt{d-1} + \varepsilon$  where  $\gamma' = \gamma + \frac{\log(\ell d^2)}{2k}$ .*

**Proof.** By the decomposition above, we have  $T(s) = T_1(s) + T_2(s)$ . As each term in the expression is of the form  $\chi(h)$  and as remarked earlier, all the characters are roots of unity so  $|\chi(s(e))| = 1$ . Thus,  $|T_1(s)| \leq |\pi^{-1}(\mathcal{H}_{k-1}^*)| \leq (d-1)^2 |\mathcal{H}_{k-1}^*|$

$$\begin{aligned} \mu &:= |\mathbb{E}_{s \sim \mathcal{D}} T| = |\mathbb{E} T_1 + \mathbb{E} T_2| \\ &\leq |\mathbb{E} T_1| + |\mathbb{E} T_2| \\ &\leq |\mathcal{H}_{k-1}^s| + \sum_{w \notin \mathcal{H}_{k-1}^s} |\mathbb{E}_{s \sim \mathcal{D}} \chi_w(s)| \\ &\leq d^2 (2^\gamma \sqrt{d-1})^{2k} + \nu |\mathcal{H}_{k-1}| \\ &\leq d^2 (2^\gamma \sqrt{d-1})^{2k} + \nu n d^{2k+2}. \end{aligned}$$

Here we have used the observation that  $|\mathcal{H}_{k-1}^s| \leq (d-1)^2 \{|\text{Singleton-free } (k-1)\text{-hikes}|\}$  and Lemma 20. The bound on  $|\mathcal{H}_{k-1}|$  is trivial as we have  $nd$  choices for the starting edge and a walk of length of  $2k+1$ . Since  $T$  is a non-negative random variable, we apply Markov to conclude that  $T \leq \mu \ell$  with probability at most  $1/\ell$ .

$$\begin{aligned} \rho(B_s(\chi)) &\leq T^{1/2k} < (\mu \ell)^{1/2k} \leq \left( d^2 \ell \left( 2^\gamma \sqrt{d-1} \right)^{2k} + \nu \ell n d^{2k+2} \right)^{1/2k} \\ &\leq (d^2 \ell)^{1/2k} 2^\gamma \sqrt{d-1} + (\nu \ell n d^{2k+2})^{1/2k} \\ &\leq 2^{\gamma'} \sqrt{d-1} + (\nu \ell n d^2)^{1/2k} d \\ &\leq 2^{\gamma'} \sqrt{d-1} + \frac{\varepsilon}{d} d \\ &\leq 2^{\gamma'} \sqrt{d-1} + \varepsilon. \end{aligned} \quad \blacktriangleleft$$

## 5.2 The Instantiation

Before we instantiate the explicit construction of abelian lifted expanders leading to Theorem 1, we will need two tools. The first one is an explicit construction of expander graphs to be used as base graphs in the lifting operation. Since we need this technical condition of bicycle-freeness, we use the construction in [24].

► **Theorem 22.** [24, Theorem 1.1] *For any given constants  $d \geq 3, \varepsilon > 0$ , one can construct in deterministic polynomial time, an infinite family of graphs  $\{G_n\}$  with  $\lambda(G_n) \leq 2\sqrt{d-1} + \varepsilon$  and  $G_n$  is*

- $n \leq |V(G_n)| \leq 2n$
- $G_n$  is bicycle-free at radius  $c \log_{d-1}(|V(G_n)|)$ .
- $\lambda_2(B_G) \leq \sqrt{d-1} + \varepsilon$ .

The second tool is a  $\nu$ -biased distribution for abelian groups (having a sample space depending polynomial on  $1/\nu$ ). In particular, we use a recent construction by Jalan and Moshkovitz.

► **Theorem 23.** [19] Given the generating elements of a finite abelian group  $H$  and an integer  $m \geq 1$  and  $\nu > 0$ , there is a deterministic polynomial time algorithm that constructs subset  $S \subseteq H^m$  with size  $O\left(\frac{m \log(H)^{O(1)}}{\nu^{2+o(1)}}\right)$  such that the uniform distribution over  $S$  is  $\nu$ -biased.

We now state our first main result whose proof we defer to the full version.

► **Theorem 1.** For large enough  $n$  and constant degree  $d \geq 3$ , given  $\ell$  such that  $\ell \leq \exp(n^{\Theta(1)})$ , the generating elements of a transitive abelian group  $H \leq \text{Sym}(\ell)$ , 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  $(H, \ell)$ -lift of a graph  $G_0$  on  $\Theta(n)$  vertices.
- (Sub-Exponential) If  $\ell \leq \exp(n^{\delta(d, \varepsilon)})$ , then  $\lambda(G) \leq 2\sqrt{d-1} + \varepsilon$ .
- (Moderately-Exponential) If  $\ell \leq \exp(n^\delta)$  and also  $d \geq d_0(\varepsilon)$ , then  $\lambda(G) \leq \varepsilon \cdot d$ .

**Proof.** The proof can be found in the full version. ◀

## 6 Derandomizing Exponential Lifts

We will now construct explicit expanding graphs where the lift size is exponential. In this regime, known tools like expander Chernoff suffice and in fact one can verify that the results of [1] can be directly derandomized by an application of these. However, we give a simplified (mostly) self-contained proof relying on a key lemma of Bilu and Linial [9] which could be of independent interest and derandomize it.

### 6.1 The Setup and Construction

In this subsection, we will describe how the signings for the lift are generated via walks on an expander and utilize an expander Hoeffding bound which will be used to bound the spectrum. We will assume from now that the group is  $\mathbb{Z}_\ell$ <sup>16</sup> We use the construction from [2],

► **Theorem 24.** [2, Thm. 1.3] For every degree  $d \geq 3$ , every  $\varepsilon > 0$  and all sufficiently large  $m \geq n_0(d, \varepsilon)$  where  $md$  is even, there is an explicit construction of an  $(m, d, \lambda)$ -graph with  $\lambda \leq 2\sqrt{d-1} + \varepsilon$ .

We can fix the degree to be an even constant, say  $d'$ , and have  $\varepsilon = \sqrt{d'-1}$ . Then, for every large enough  $m$ , we have an expander on  $m$  vertices. We use this to get an explicit expander,  $L$ , on  $\ell$  vertices. To obtain a sequence of lifts i.e. elements of  $\mathbb{Z}_\ell$ , we first pick a random vertex,  $v_1$ , of  $L$  which uses  $\log \ell$  bits of randomness. Then, we do a random walk for  $dn - 1$  steps producing a sequence  $(v_1, \dots, v_{dn-1})$  of vertices of  $L$  which we interpret as elements of  $\mathbb{Z}_\ell$ . Each step of the random walk requires  $O(\log d')$  bits of randomness as the graph is  $d'$ -regular. Therefore, the total amount of randomness is  $O(\log \ell + (dn - 1) \log d')$ <sup>17</sup> The main observation is that an expander random walk suffices to guarantee that the lifted graph will be an expander. To formalize this, we first state a Hoeffding type concentration result for our random variables generated via the Markov chain on an expander.

<sup>16</sup>This can be extended in a straightforward manner to any abelian subgroup  $H \leq \text{Sym}(\ell)$  by just taking the expander graph on  $|H|$  vertices. Since, we only work with abelian groups having a transitive action,  $|H| = \ell$ .

<sup>17</sup>Another way to say this is that the number of walks of length on  $dn$  on  $L$  is  $|H| \cdot d'^{dn}$ .



► **Theorem 25.** [29, Thm. 1.1] Let  $\{Y_i\}_{i=1}^\infty$  be a stationary Markov chain with state space  $[N]$ , transition matrix  $A$ , stationary probability measure  $\pi$ , and averaging operator  $E_\pi$ , so that  $Y_1$  is distributed according to  $\pi$ . Let  $\lambda = \|A - E_\pi\|_{L_2(\pi) \rightarrow L_2(\pi)}$  and let  $f_1, \dots, f_t : [N] \rightarrow \mathbb{R}$  so that  $\mathbb{E}[f_i(Y_i)] = 0$  for all  $i$  and  $|f_i(v)| \leq a_i$  for all  $v \in [N]$  and all  $i$ . Then for  $u \geq 0$ ,

$$\Pr \left[ \left| \sum_{i=1}^t f_i(Y_i) \right| \geq u \left( \sum_{i=1}^t a_i^2 \right)^{1/2} \right] \leq 2 \exp \left( \frac{-u^2(1-\lambda)}{64e} \right)$$

► **Corollary 26.** Let  $U$  be any subset of edges in the base graph  $G$ . Then,

$$\Pr \left[ \left| \sum_{e \in U} \operatorname{Re}(\chi(s(e))) \right| \geq t \right] \leq 2 \exp \left( \frac{-t^2}{128e|U|} \right)$$

$$\Pr \left[ \left| \sum_{e \in U} \operatorname{Im}(\chi(s(e))) \right| \geq t \right] \leq 2 \exp \left( \frac{-t^2}{128e|U|} \right).$$

**Proof.** Let  $Y_e = s(e)$  be the random variables associated to each edge  $e$ . From the construction described earlier,  $\{Y_{u,v}\}$  is a Markov chain with the transition matrix being the weighted adjacency matrix of the expander  $L$  with second (normalized) eigenvalue bounded by  $3\sqrt{d'-1}/d'$ . Thus,  $1 - \lambda \geq 1 - \frac{3}{\sqrt{d'}} \geq 1/2$  for  $d' \geq 36$ . The stationary measure  $\pi$  is the uniform measure on vertices of  $L$  and it is stationary as the all-ones vector is an eigenvector of the weighted adjacency matrix with eigenvalue 1. Recall that we picked the first vertex ( $Y_1$ ) uniformly i.e. from  $\pi$ . Let  $f_e = \operatorname{Re}(\chi(s(e)))$  if  $e \in U$  and 0 otherwise. Analogously  $g_e = \operatorname{Im}(\chi(s(e)))$  when the edge is in  $U$  and 0 otherwise.

$\mathbb{E}[f_e] = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \operatorname{Re}(\omega^i)$  because the characters are roots of unity and the expectation is over  $\pi$  which is uniform. Since the sum of roots of unity are zero, so is its real and imaginary part. This holds thus for  $g_e$  too. Moreover,  $a_e = 1$  if  $e \in U$  and is 0 otherwise. Applying 25 with  $u := t/\sqrt{|U|}$  gives the result. ◀

## 6.2 A Simpler Lifting Proof

In this section, we give a simpler proof of a weaker result similar to one in [1] which says that if the lifts were picked independently and uniformly at random, then the lifted graph is also expanding. In place of the random signings, we will use the signings generated from random walks as described in the earlier section. The proof can be seen as building up from the tools of [9] by simplifying their derandomization of the 2-lift and extending it to  $\ell$ -lifts.

Let  $G$  be a graph,  $H$  be an abelian group and  $s$  be a signing  $s : E \rightarrow H$  that gives a  $(H, \ell)$ -lift. Let  $A$  be its adjacency matrix. We will use the earlier notation and denote by  $A(\chi)$ , the matrix where for every edge  $e$ , we replace 1 by  $\chi(s(e))$ . Let  $A(\chi) = C + iD$  where  $C, D$  are real symmetric matrices. We want to bound the spectral radius of  $A(\chi)$ . It is not very hard to see that  $\|A\| \leq 2 \max\{\|C\|, \|D\|\}$ . This can be observed by letting  $v = v_1 + iv_2$  be an eigenvector and  $\alpha = \max\{\|C\|, \|D\|\}$ . Then,

$$\begin{aligned} v^* A v &= \operatorname{Re}(v^* A v) = (v_1^T C v_1 + v_2^T C v_2 - v_1^T D v_2 + v_2^T D v_1) \\ &\leq \|C\| \|v_1\|^2 + 2 \|D\| \|v_1\| \|v_2\| \\ &\leq \alpha (\|v_1\| + \|v_2\|)^2 \\ &\leq 2\alpha (\|v_1\|^2 + \|v_2\|^2) \\ &= 2\alpha \|v\|^2 \end{aligned}$$

## 88:18 Explicit Abelian Lifts and Quantum LDPC Codes

Therefore we reduce the problem to bounding spectral radius for the constituent real matrices. We now state a very useful lemma by Bilu and Linial which is a discretization result and can be seen as a converse to the expander mixing lemma. It says that bounding the Rayleigh coefficient on Boolean vectors suffices to bound the real spectrum up to logarithmic factors.

► **Theorem 27** ([9, Lemma 3.3]). *Let  $A$  be an  $n \times n$  real symmetric matrix such that the  $\ell_1$  norm of each row in  $A$  is at most  $d$ , and all diagonal entries of  $A$  are, in absolute value,  $O(\alpha(\log(d/\alpha) + 1))$ . If for any two vectors,  $u, v \in \{0, 1\}^n$ , with  $\text{Supp}(u) \cap \text{Supp}(v) = \emptyset$ :*

$$\frac{|u^t A v|}{\|u\| \|v\|} \leq \alpha,$$

then, the spectral radius of  $A$  is  $O(\alpha(\log(d/\alpha) + 1))$ .

Since the graph is  $d$ -regular,  $A(\chi)$  is  $d$ -sparse and so is  $C$  and  $D$ . The  $\ell_1$ -norm of any row of  $C, D \leq d$  as we have a sum of  $d$  entries of the form  $\text{Re}(\omega^j), \text{Im}(\omega^j)$  for some  $j$  and the absolute value of each of these is upper bounded by 1. Moreover, the diagonal entries are all zero. Therefore, these satisfy the norm criteria of the theorem. Now, we need to bound the (generalized) Rayleigh coefficient.

Let  $S, T$  be subsets of the vertices of a  $d$ -regular graph. Define  $E(S, T) = \{(x, y) \in E \mid x \in S, y \in T\}$  and let  $e(S, T) := |E(S, T)|$ . Let  $u, v \in \{0, 1\}^n$  and let  $S := \text{Supp}(u), T := \text{Supp}(v)$ . Then,

$$|u^T C v| \leq \sum_{e \in E(S, T)} |\text{Re}(\chi(s(e)))| \leq e(S, T) \quad (1)$$

$$|u^T D v| \leq \sum_{e \in E(S, T)} |\text{Im}(\chi(s(e)))| \leq e(S, T) \quad (2)$$

Let us now state the expander mixing lemma,

$$\left| e(S, T) - \frac{d|S||T|}{n} \right| \leq \lambda(G) \sqrt{|S||T|}. \quad (3)$$

Now we assume that the signing  $s$  was generated from the random walk as described earlier. This lets us use Corollary 26 to prove the following lemma.

► **Lemma 28.** *Let  $M$  be either  $C$  or  $D$  where these are the matrices defined above. Pick  $\gamma$  such that  $\gamma^3 \geq \frac{256e\sqrt{d}}{n} \ln(3\ell)$ . Then for every pair of vectors  $u, v \in \{0, 1\}^n$ ,  $|u^T M v| \leq \alpha \|u\| \|v\|$  where  $\alpha = (\gamma + 1)\lambda$  except with probability  $\frac{2}{3\ell}$  over choice of  $s$ .*

**Proof.** The proof is included in the full version. ◀

► **Theorem 29** (Exactly Exponential Lifts). *For any positive integers  $n, \ell$  and every constant degree  $d$ , there exists a deterministic  $\text{poly}(\exp(n), \ell)$  time algorithm that constructs a  $d$ -regular graph  $G$  on  $n\ell$  vertices such that*

- $G$  is quasi-cyclic with lift size  $\ell$ , and
- If  $\ell \leq \exp(cnd^{-1/2})$ , then  $\lambda(G) \leq O(\sqrt{d} \log d)$
- If  $\ell = \exp(cnd^\delta)$  for  $\delta \in [-1/2, 1)$ , then  $\lambda(G) \leq O\left(d^{\frac{2+\delta}{3}} \log d\right)$

In particular, this yields an explicit polynomial time construction of a lift in the regime when  $\ell = \exp(O(n))$ .

**Proof.** We construct a  $d$ -regular graph  $G_0$  using [2] on  $n$  vertices such that  $\lambda_2(G) \leq 2\sqrt{d}$ . We generate a set of signings as described above using a  $d'$ -regular expander on  $\ell$  vertices. This takes time  $\ell \exp(nd \ln(d'))$  and we can fix  $d' = 36$ . For each signing we compute the eigenvalue of the adjacency matrix of the lifted graph and pick the one with the smallest  $\lambda_2$ . The existence of a good signing is guaranteed as follows.

Lemma 28 gives a bound of  $\alpha = (\gamma + 1)\lambda$  on the Rayleigh quotient of  $C, D$  holds except with probability  $\frac{2}{3\ell}$  over the signings. Theorem 27 then implies that

$$\lambda_{\max} A(\chi) \leq 2 \max\{\|C\|, \|D\|\} \leq 2\alpha \log(d/\alpha) \leq O(\alpha \log d)$$

Here,  $\gamma^3 = O(\frac{\ln \ell \sqrt{d}}{n}) = O(d^{1/2+\delta})$ . Note that if  $\delta < -1/2$ , then  $O((\gamma + 1)\lambda) = O(\lambda)$ . Thus,  $\alpha = O(\sqrt{d}d^{1/6+\delta/3} + \lambda) = O\left(\max\left\{d^{\frac{2+\delta}{3}}, \sqrt{d}\right\}\right)$ .

To finish the proof we need to take a union bound over each of the  $\ell - 1$  non-trivial characters and bound the spectrum of  $A(\chi)$  as above. Thus, we have that the probability that there exists a good signing is at least  $1 - \ell \left(\frac{2}{3\ell}\right) > 0$ . ◀

## 7 Explicit Quantum and Classical Codes

We now briefly recall the construction of quantum LDPC codes as in [28] 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  $T(G, \mathcal{C}_0)$  and let  $F$  denote the cycle graph on  $\ell$  vertices. They define the lifted product  $LP(B, F)$  of  $B$  and  $F$  which is a variation of the usual tensor product and is also equivalent to the twisted product in [17]. The main result of [28] is the following.

► **Theorem 30** ([28]). *Let  $G$  be  $(\mathbb{Z}_\ell, \ell)$ -lift of a  $d$  regular graph on  $n$ -vertices with  $\lambda_2(G) \leq \varepsilon \cdot d$ . Let  $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$  and its dual attain the Gilbert–Varshamov bound. If  $\varepsilon > 0$  is sufficiently small and  $d$  is a sufficiently large constant, then*

- $T(G, \mathcal{C}_0)$  is a good quasi-cyclic LDPC code of blocklength  $\Theta(n\ell)$  and circulant size  $\Theta(\ell)$ .
- The quantum lifted product code  $LP(B, F)$  is LDPC and has distance  $\Theta_{\varepsilon, d}(\ell)$  and dimension  $\Theta(n)$ .

To achieve these, [28] picks a  $d$ -regular expander on  $n$  vertices and creates a random  $\ell$ -lift i.e. where each signing is chosen uniformly at random from  $\mathbb{Z}_\ell$ . The final graph is expanding with high probability from the results of [1] (Theorem 2). The distance achieves the almost-linear bound only when the lift is large and thus lifts of exponential size are preferred. By the upper bound in Theorem 2, better than exponential size lifts break expansion for abelian groups.

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.

While the corollary follows in a straightforward manner from our main results, we show the computations for completeness.

► **Corollary 31** ([28], Theorem 1, Theorem 3). *We have explicit polynomial time construction of each of the following,*

1. Good quasi-cyclic LDPC code of block length  $N$  and any circulant size up to  $N/\text{polylog}(N)$  or  $\Theta(N/\log(N))$ .

2. Quantum LDPC code with distance  $\Omega(N/\log(N))$  and dimension  $\Omega(\log(N))$ .
3. Quantum LDPC code with distance  $\Omega(N^{1-\alpha})$  and dimension  $\Theta(N^\alpha)$  for every constant  $\alpha > 0$ .

**Proof.** We always work in the constant degree regime so  $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$  can be found by brute-force. When  $\ell = \exp(\Theta(n))$ , we use Theorem 3 to construct  $G$  explicitly. Thus,  $N = n\ell$  and thus the circulant size and distance are both  $\Theta(\ell) = \Theta(N/\log N)$ .

For  $\ell \leq 2^{n^{\delta_0}}$  with some fixed  $\delta_0 \in (0, 1)$ , we can explicitly construct  $G$  which is a  $(\mathbb{Z}_\ell, \ell)$ -lift by Theorem 1 and by [28],  $T(G, \mathcal{C}_0)$  has circulant size  $\Theta(\ell)$  and  $\log(N) \leq \log n + n^{\delta_0} \leq 2n^{\delta_0}$  (for  $n$  sufficiently large) and thus,  $\ell = O(N/(\log N)^{1/\delta_0})$ . Therefore, the construction works for any size less than  $N/(\log N)^{1/\delta_0}$ . This calculation also shows that we get quantum LDPC codes for any distance less than  $N/(\log N)^{1/\delta_0}$ . So for a given  $\alpha$ , we take a base graph on  $n = N^\alpha$  vertices and construct a  $\ell = N^{1-\alpha} = n^{1/\alpha-1}$  lift. For any  $\alpha$ , this is a polynomial sized-lift and can be done via Theorem 1. ◀

---

## References

- 1 Naman Agarwal, Karthekeyan Chandrasekaran, Alexandra Kolla, and Vivek Madan. On the Expansion of Group-Based Lifts. *SIAM J. Discret. Math.*, 33(3):1338–1373, 2019. doi:10.1137/17M1141047.
- 2 Noga Alon. Explicit expanders of every degree and size. *Combinatorica*, February 2021. doi:10.1007/s00493-020-4429-x.
- 3 Noga Alon, Shlomo Hoory, and Nathan Linial. The Moore bound for irregular graphs. *Graphs and Combinatorics*, 18:53–57, 2002. doi:10.1007/s003730200002.
- 4 Noga Alon and Yuval Roichman. Random cayley graphs and expanders. *Random Struct. Algorithms*, 5(2):271–285, 1994. doi:10.1002/rsa.3240050203.
- 5 László Babai, Amir Shpilka, and Daniel Stefankovic. Locally testable cyclic codes. *IEEE Trans. Inf. Theory*, 51(8):2849–2858, 2005. doi:10.1109/TIT.2005.851735.
- 6 László Babai. On the minimum order of graphs with given group. *Canadian Mathematical Bulletin*, 17(4):467–470, 1974. doi:10.4153/CMB-1974-082-9.
- 7 L.M.J. Bazzi and S.K. Mitter. Some randomized code constructions from group actions. *IEEE Transactions on Information Theory*, 52(7):3210–3219, 2006. doi:10.1109/TIT.2006.876244.
- 8 Avraham Ben-Aroya and Amnon Ta-Shma. A combinatorial construction of almost-ramanujan graphs using the zig-zag product. In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 325–334, 2008. doi:10.1145/1374376.1374424.
- 9 Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap. *Combinatorica*, 26(5):495–519, October 2006. doi:10.1007/s00493-006-0029-7.
- 10 Nikolas P. Breuckmann and Jens N. Eberhardt. Balanced Product Quantum Codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, 2021. doi:10.1109/TIT.2021.3097347.
- 11 A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, August 1996. doi:10.1103/PhysRevA.54.1098.
- 12 C.L. Chen, W.W. Peterson, and E.J. Weldon. Some results on quasi-cyclic codes. *Information and Control*, 15(5):407–423, November 1969. doi:10.1016/s0019-9958(69)90497-5.
- 13 Michael B. Cohen. Ramanujan graphs in polynomial time. In *Proceedings of the 57th IEEE Symposium on Foundations of Computer Science*, 2016. doi:10.1109/FOCS.2016.37.
- 14 Shai Evra, Tali Kaufman, and Gilles Zémor. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, pages 218–227. IEEE, 2020. arXiv:2004.07935, doi:10.1109/FOCS46700.2020.00029.
- 15 R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962. doi:10.1109/TIT.1962.1057683.

- 16 Oded Goldreich and Avi Wigderson. Robustly self-ordered graphs: Constructions and applications to property testing. In Valentine Kabanets, editor, *Proceedings of the 36th IEEE Conference on Computational Complexity*, volume 200 of *LIPIcs*, pages 12:1–12:74. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.12.
- 17 Matthew B. Hastings, Jeongwan Haah, and Ryan O'Donnell. Fiber bundle codes: breaking the  $n^{1/2}$ polylog( $n$ ) barrier for quantum LDPC codes. In *Proceedings of the 53rd ACM Symposium on Theory of Computing*, pages 1276–1288. ACM, 2021. doi:10.1145/3406325.3451005.
- 18 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43(04):439–562, August 2006. doi:10.1090/S0273-0979-06-01126-8.
- 19 Akhil Jalan and Dana Moshkovitz. Near-optimal cayley expanders for abelian groups. *CoRR*, abs/2105.01149, 2021. arXiv:2105.01149.
- 20 Tali Kaufman and Avi Wigderson. Symmetric LDPC codes and local testing. In Andrew Chi-Chih Yao, editor, *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 406–421. Tsinghua University Press, 2010. URL: <http://conference.iis.tsinghua.edu.cn/ICS2010/content/papers/32.html>.
- 21 Huaan Li, Baoming Bai, Xijin Mu, Ji Zhang, and Hengzhou Xu. Algebra-assisted construction of quasi-cyclic LDPC codes for 5G new radio. *IEEE Access*, 6:50229–50244, 2018. doi:10.1109/ACCESS.2018.2868963.
- 22 Alexander Lubotzky, R. Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988. doi:10.1007/BF02126799.
- 23 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. URL: <http://mi.mathnet.ru/eng/ppi686>.
- 24 Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-ramanujan graphs of every degree. In *Proceedings of the 52nd ACM Symposium on Theory of Computing*, pages 510–523. ACM, 2020. doi:10.1145/3357713.3384231.
- 25 M. Morgenstern. Existence and explicit constructions of  $q + 1$  regular Ramanujan graphs for every prime power  $q$ . *J. Comb. Theory Ser. B*, pages 44–62, September 1994. doi:10.1006/jctb.1994.1054.
- 26 Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991. doi:10.1016/0012-365X(91)90112-F.
- 27 R. O'Donnell and X. Wu. Explicit near-fully X-Ramanujan graphs. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, pages 1045–1056, 2020. doi:10.1109/FOCS46700.2020.00101.
- 28 Pavel Panteleev and Gleb Kalachev. Quantum LDPC Codes with Almost Linear Minimum Distance. *IEEE Transactions on Information Theory*, December 2021. arXiv:2012.04068, doi:10.1109/TIT.2021.3119384.
- 29 Shravas Rao. A Hoeffding inequality for Markov chains. *Electronic Communications in Probability*, 24:1–11, 2019. doi:10.1214/19-ECP219.
- 30 O. Reingold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, 2000. doi:10.1109/SFCS.2000.892006.
- 31 Tom Richardson and Ruediger Urbanke. *Modern coding theory*. Cambridge university press, 2008. doi:10.1017/CB09780511791338.
- 32 Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, November 1996. doi:10.1098/rspa.1996.0136.
- 33 Salil P. Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012. doi:10.1561/04000000010.