

Explicit near-Ramanujan graphs of every degree

Sidhanth Mohanty*

Ryan O'Donnell[†]Pedro Paredes[†]

November 29, 2022

Abstract

For every constant $d \geq 3$ and $\epsilon > 0$, we give a deterministic $\text{poly}(n)$ -time algorithm that outputs a d -regular graph on $\Theta(n)$ vertices that is ϵ -near-Ramanujan; i.e., its eigenvalues are bounded in magnitude by $2\sqrt{d-1} + \epsilon$ (excluding the single trivial eigenvalue of d).

*EECS Department, University of California Berkeley. Supported by NSF grant CCF-1718695

[†]Computer Science Department, Carnegie Mellon University. Supported by NSF grant CCF-1717606. This material is based upon work supported by the National Science Foundation under grant numbers listed above. 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).

1 Introduction

In this work, we obtain explicit d -regular ϵ -near-Ramanujan graphs for every $d \geq 3$ and every $\epsilon > 0$. As an example, we give the first explicit family of 7-regular graphs with $\lambda_2(G), |\lambda_n(G)| \leq 2\sqrt{6} + \epsilon$. Our main result is the following:

Theorem 1.1. *For any $d \geq 3$ and any $\epsilon > 0$, there is an explicit (deterministic polynomial-time computable) infinite family of d -regular graphs G with $\max\{\lambda_2(G), |\lambda_n(G)|\} \leq 2\sqrt{d-1} + \epsilon$.*

The key technical result that we prove in service of this is the following:

Theorem 1.2. *Let G be an arbitrary d -regular n -vertex graph. Assume that the r -neighborhood of every vertex contains at most one cycle, where $r \gg (\log \log n)^2$. Then a random edge-signing of G has all its eigenvalues bounded in magnitude by $2\sqrt{d-1} + o_n(1)$, with high probability.*

See [Section 1.4](#) for a comparison of [Theorem 1.2](#) with a similar theorem of Bilu and Linial [\[BL06\]](#), which has an alternate hypothesis and a weaker conclusion.

1.1 On near-Ramanujan graphs

Let us put our results into context. Loosely speaking, *expander graphs* are sparse graphs in which every small set of vertices has many edges on its boundary. For an early paper working out relationships between various possible definitions, see Alon [\[Alo86\]](#). For a thorough reference describing expanders' myriad applications and connections to various parts of computer science and mathematics, see the survey of Hoory, Linial, and Wigderson [\[HLW06\]](#).

A good way to quantify the definition of expansion is through the eigenvalues of the graph.

Definition 1.3 (Graph eigenvalues). Let G be an n -vertex d -regular multigraph. We write $\lambda_i = \lambda_i(G)$ for the *eigenvalues* of its adjacency matrix A , and we always assume they are ordered with $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. A basic fact is that $\lambda_1 = d$ always; this is called the *trivial* eigenvalue. We also write $\lambda = \lambda(G) = \max\{\lambda_2, |\lambda_n|\}$.

The extent to which a d -regular graph G is “expanding” is governed by the magnitude of its nontrivial eigenvalues; in particular, by λ_2 and (to a lesser extent) $|\lambda_n|$. Together these are captured by the parameter $\lambda(G)$. The smaller $\lambda(G)/d$ is, the better G 's expansion; typically, a graph is called expanding when this ratio is bounded away from 1.

Definition 1.4 (Spectral expanders). An infinite sequence of d -regular (multi)graphs (G_n) is said to be a *family of expanders* if there is a constant $\delta > 0$ such that $\lambda(G_n) \leq (1 - \delta)d$ for all n .

Pinsker [\[Pin73\]](#) introduced the English terminology and showed that random (bipartite) graphs have positive expansion properties with high probability (see also [\[BK67, Mar73a\]](#)). Indeed, it can be shown [\[Alo86\]](#) that a uniformly random d -regular graph has $\lambda_2(G) < (1 - \delta)d$ with high probability, for some universal $\delta > 0$ (see [Theorem 1.8](#) below for a much stronger result). However, for almost all of the numerous practical applications of expanders in theoretical computer science (error correcting codes, derandomization, complexity theory, cryptography, metric embeddings, etc.) it is important for the graphs to be *explicit* — i.e., constructible by a deterministic polynomial-time algorithm. Indeed, it is even better if they are *strongly explicit*, meaning that their adjacency list is computable in polylog n time.

1.2 Review of Ramanujan and near-Ramanujan families

Margulis [Mar73b] was the first to provide an explicit expander family; a slight variant of it, which is 8-regular, was shown [GG81] to have $\lambda \leq 5\sqrt{2} \approx 7.1$ (see [HLW06]). A natural question then is to provide explicit d -regular expanders, for various values of d , with λ as small as possible as a function of d . The well-known *Alon–Boppana bound* shows that $2\sqrt{d-1}$ is essentially a lower bound:

Theorem 1.5. ([Alo86, Nil91, Fri93].) *Let G be an n -vertex d -regular multigraph. Then $\lambda_2(G) \geq 2\sqrt{d-1} - O(1/\log^2 n)$.*

On the other hand, 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 $\lambda(G) \leq 2\sqrt{d-1}$ for some values of d . Lubotzky–Phillips–Sarnak [LPS88] dubbed such graphs *Ramanujan*.

Definition 1.6 (Ramanujan graphs). A d -regular (multi)graph G is called (*two-sided*) *Ramanujan* whenever $\lambda(G) \leq 2\sqrt{d-1}$. When we merely have $\lambda_2(G) \leq 2\sqrt{d-1}$, we call G *one-sided Ramanujan*; if G is bipartite this implies that $|\lambda_i| \leq 2\sqrt{d-1}$ for all $i \neq 1, n$, with $\lambda_n(G) = -d$ being inevitable.

We remark that some expander properties (e.g., edge-expansion for small sets) only need a one-sided eigenvalue bound, whereas others (e.g., the Expander Mixing Lemma) need a two-sided bound.

Regarding the explicit construction of d -regular Ramanujan graphs using number theory, 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 mentioned below 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].

Theorem 1.7. ([Mor94].) *For any $d \geq 3$ 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 (but see Theorem 1.12 below for the one-sided bipartite case). However, it is known that *near-Ramanujan* graph families exist for every d . Alon [Alo86] conjectured that a random n -vertex d -regular graph G has $\lambda(G) \leq 2\sqrt{d-1} + o_n(1)$ with high probability, and this was proven two decades later by Friedman [Fri08]. Bordenave [Bor19] has recently given a simpler proof, and our paper will involve modifying and derandomizing Bordenave’s work.

Theorem 1.8. ([Fri08].) *Fix any $d \geq 3$ and $\epsilon > 0$ and let G be a uniformly random d -regular graph. Then*

$$\Pr\left[\lambda(G) \leq 2\sqrt{d-1} + \epsilon\right] \geq 1 - o_n(1).$$

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

A natural question then is whether, for every d , one can achieve *explicit* graph families that are “ ϵ -near-Ramanujan” as above. 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 $\lambda(G) \leq O(d^{2/3})$. By extending their approach, Ben-Aroya and Ta-Shma reached $d^{1/2+o(1)}$:

Theorem 1.9. ([RVW02, BT11].) *There are strongly explicit families of d -regular multigraphs G satisfying the bound $\lambda(G) \leq \sqrt{d} \cdot 2^{O(\sqrt{\log d})}$.*

Bilu and Linial [BL06] got even closer to $O(\sqrt{d})$, using a new approach based on random lifts that will prove important in our paper. Their graph families are not strongly explicit, although Bilu–Linial point out they are at least “probabilistically strongly explicit” (q.v. Theorem 1.13).

Theorem 1.10. ([BL06].) *There are explicit families of d -regular multigraphs G satisfying the bound $\lambda(G) \leq \sqrt{d} \cdot O(\log^{1.5} d)$.*

Due to their asymptotic-in- d nature, neither of Theorems 1.9 and 1.10 gives much help for specific small values of d not covered by Morgenstern, such as $d = 7$. In such cases, one can use a simple idea due to Cioabă and Murty [CM08] (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 1.11. ([CM08].) *For any $d \geq 3$, there is a strongly explicit family of d -regular multigraphs with $\lambda(G) \leq 2\sqrt{d-1} + \text{gap}(d)$, where $\text{gap}(d)$ denotes the least value g such that $d - 1 - g$ is a prime (power). One can bound $\text{gap}(d)$ 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.*

For example, this gives strongly explicit 7-regular multigraphs with $\lambda(G) \leq 2\sqrt{5} + 1 < 5.5$. For comparison, the Ramanujan bound is $2\sqrt{6} < 4.9$.

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

Theorem 1.12. ([MSS15a, MSS15b, Coh16].) *For any $d \geq 3$, there is an explicit family of one-sided bipartite, d -regular, Ramanujan multigraphs.*

As mentioned, this theorem gives an n -vertex graph for every even n , which is slightly better than all other results mentioned in this section, which merely give graphs for a dense sequence of n ’s (typically, a sequence n_j with $n_{j+1} - n_j = o(n_j)$). Also, as pointed out to us by Nikhil Srivastava, pairing left and right vertices in the construction from Theorem 1.12 and merging them gives “twice-Ramanujan” graphs of every even degree; i.e., $2d$ -regular graphs for all $d \geq 3$ with $\lambda(G) \leq 4\sqrt{d-1}$.¹ One can then obtain $(2d + 1)$ -regular graphs with $\lambda(G) \leq 4\sqrt{d-1} + 1$ by adding an arbitrary perfect matching via the result of [CM08].

Our results. As mentioned, our Theorem 1.1 gives $\text{poly}(n)$ -time deterministically computable n -vertex d -regular graphs G with $\lambda(G) \leq 2\sqrt{d-1} + \epsilon$, for any $d \geq 3$ and $\epsilon > 0$. To be more precise, the running time of our algorithm is $n^{f(d, \epsilon)}$ where $f(d, \epsilon) = O(d^{1/4} \log(d) / \sqrt{\epsilon})$. Although

¹We include a short proof here: let $\tilde{A} = \begin{bmatrix} 0 & A \\ A^T & 0 \end{bmatrix}$ be the adjacency matrix of a d -regular bipartite Ramanujan graph.

Then $A + A^T$ is the adjacency matrix of the merged graph. For any x orthogonal to $\vec{1}$, $(A + A^T)x = \begin{bmatrix} \mathbb{1} & \mathbb{1} \end{bmatrix} \tilde{A} \begin{bmatrix} x \\ x \end{bmatrix}$. Thus $\|(A + A^T)x\| \leq \sqrt{2} \cdot \left\| \tilde{A} \begin{bmatrix} x \\ x \end{bmatrix} \right\|$. Since $\begin{bmatrix} x \\ x \end{bmatrix}$ is orthogonal to both $\begin{bmatrix} \vec{1} \\ \vec{1} \end{bmatrix}$ and $\begin{bmatrix} \vec{1} \\ -\vec{1} \end{bmatrix}$, we have $\left\| \tilde{A} \begin{bmatrix} x \\ x \end{bmatrix} \right\| \leq 2\sqrt{d-1}\sqrt{2}\|x\|$. One can then conclude that $\|(A + A^T)x\| \leq 4\sqrt{d-1}\|x\|$.

Table 1: Comparison of our **Theorem 1.1** with prior work.

Who?	Which d ?	Eigenvalue bound	2-sided?	Strongly explicit?	Always simple?	# vertices given n
[Iha66, LPS88, Mar88, Chi92, Mor94]	prime power + 1	$2\sqrt{d-1}$	✓	✓	✓	$n(1+o(1))$
[Piz90, Cla06]	any d	$2^{\text{om}(d-1)}\sqrt{d-1}$ *	✓	✓	✗	$n(1+o(1))$
[RVW02, BT11]	any d	$\sqrt{d} \cdot 2^{O(\sqrt{\log d})}$	✓	✓	✗	$\Theta(n)$
[dlHM06, CM08]	any d	$\begin{cases} 2\sqrt{d-1} + O(\log^2 d) & ^{\dagger} \\ \sqrt{d} \cdot O(\log d) & ^{\ddagger} \\ O(d^{.525}) \end{cases}$	✓	✓	✓ [§]	$n(1+o(1))$
[BL06]	any d	$\sqrt{d} \cdot O(\log^{1.5} d)$	✓	✗ [¶]	✓	$n(1+o(1))$
[MSS15a, MSS15b, Coh16]	any d	$2\sqrt{d-1}$	✗	✗	✗	$2\lceil n/2 \rceil$
this paper	any d	$2\sqrt{d-1} + \epsilon$	✓	✗ [¶]	✓	$n(1+o(1))$

* In the this entry we have written $\text{om}(d-1)$ for the number of distinct prime divisors of $d-1$. Thus [Cla06] generalizes the preceding “prime power + 1” entry of [Mor94]. Also, $2^{\text{om}(d-1)}$ is at most $2^{O(\log d / \log \log d)} = d^{o(1)}$ for all d , and is $(2+o(1))^{\ln \ln d} = O(\log^{0.7} d)$ for “most” d .

[†] Assuming Cramér’s conjecture. [‡] Assuming the Riemann Hypothesis.

[§] The construction can be made simple at the expense of making it not strongly explicit.

[¶] The construction is “probabilistically strongly explicit”.

our graphs are not strongly explicit, they are “probabilistically poly log n -time computable”, a relaxation of a notion defined by [BL06]. Essentially, this means we show there *exist* near-Ramanujan graphs whose adjacency lists are computable in polylog n time, and furthermore there is a polylog(n)-time randomized algorithm for finding them with high probability. More precisely, the following statement holds:

Theorem 1.13. *There is a deterministic polynomial-time algorithm with the following properties:*

- It takes as input N , $d \geq 3$, and $\epsilon > 0$ written as binary strings.
- It also takes as input a “seed” $s \in \{0,1\}^{O(\log^2 N)}$ (the $O(\cdot)$ hides a factor of $O(d^{1/4} \log(d) / \sqrt{\epsilon})$).
- It outputs a Boolean circuit C that implements the “adjacency list” of a d -regular graph G on $N' \sim N$ vertices in 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 i th neighbor of u in G .)
- With high probability over the choice of seed s , the resulting graph G satisfies the bound $\lambda(G) \leq 2\sqrt{d-1} + \epsilon$.

The difference between our notion and that of [BL06] is that we use a seed of length- $O(\log^2 N)$, whereas the notion in [BL06] requires the seed length to be $O(\log N)$.

1.3 On Bordenave’s theorem with random edge-signs

Since our result may be viewed as a derandomization of the Friedman/Bordenave theorem (**Theorem 1.8**), let us take some time to describe this result. Friedman’s original proof is notably quite involved (100 pages). Bordenave’s proof is certainly simpler (more like 30 pages), although it is by no means easy. However, Bordenave’s proof can become still simpler if one is willing consider a variant: when G is not just a random d -regular graph, but rather a *randomly edge-signed* random d -regular graph.

Let us say a few words about why this makes things simpler. First, it turns out that in this case one need not worry about the “trivial eigenvalue” of d ; it no longer exists, and the statement to be proven is simply that $\rho(G) \leq 2\sqrt{d-1} + \epsilon$ with high probability, where $\rho(G)$ is the spectral radius

(largest eigenvalue-magnitude) of the (signed) adjacency matrix of G . Second, with random edge-signs, each entry of G 's adjacency matrix becomes a symmetric random variable, and it is always more pleasant in probability theory when one's random variables naturally have mean zero.

In fact, there are scenarios in which one might actually *want* to consider random edge-signed d -regular graphs. For example when studying the Max-Cut problem, the setting of sparse random graphs is a very natural and challenging one, and many algorithms/complexity results depend on eigenvalue bounds for such graphs. Having random edge-signs simply means studying the equally natural 2XOR (aka 2Lin) problem, one that has a long history in theoretical computer science as well [Hås84].

Undoubtedly experts would know that including random edge-signs should make Bordenave's proof simpler, but it doesn't appear to have been directly explored until the recent work of Deshpande et al. [DMO⁺19]. That paper proved the analogue of Friedman/Bordenave for random edge-signings of random (c, d) -biregular graphs. The case when $c = d$ is essentially the same as the d -regular random graph case, but the nature of the proof simplification is perhaps obscured, particularly because [DMO⁺19] directly cited several lemmas from Bordenave [Bor19]. A similar situation occurred in a subsequent work [MOP19], which has random edge-signs within an even more complicated random graph model.

In fact, a side motivation we had for this paper was to carefully set out a self-contained proof — as simple as possible — of “Alon's Conjecture” for randomly edge-signed graphs. A reader not interested in derandomization may nevertheless find our proof of the below theorem of interest, particularly since it contains a substantial portion of Bordenave's proof of Friedman's theorem.

Theorem 1.14. *Let $d \geq 3$ and $\epsilon > 0$. If G is a random edge-signed d -regular n -vertex graph, then*

$$\Pr\left[\rho(G) \leq 2\sqrt{d-1} + \epsilon\right] \geq 1 - o_n(1).$$

In the course of proving this theorem, we are able to observe that in fact [Theorem 1.2](#) holds. That is, [Theorem 1.14](#) does not thoroughly rely on having a random edge-signing of a *random* d -regular graph. Instead, it works for a random edge-signing of *any* d -regular graph that has one particular property: namely, every vertex-neighborhood of radius $O((\log \log n)^2)$ should have at most one cycle. This property — called tangle-freeness by Bordenave (simplifying Friedman's notion of “tangles”) — is a property that random d -regular graphs have with high probability, even for neighborhoods of the much larger radius $\Theta(\log_{d-1} n)$.

With [Theorem 1.2](#) in hand, we are in a position rather like that of Bilu–Linial, who similarly showed [BL06, Cor. 3.1] that a random edge-signing of any sufficiently good small-set expander has spectral radius at most $\sqrt{d} \cdot O(\log^{1.5} d)$ (with high probability). As in Bilu–Linial, it is also fairly straightforward to see that [Theorem 1.2](#) can be derandomized effectively using almost- k -wise independent binary random variables.

We next describe how this derandomized result on edge-signings leads to our main [Theorem 1.1](#).

1.4 Explicit near-Ramanujan graphs via repeated 2-lifts

Let $G = (V, E)$ be an n -vertex d -regular graph, and let \tilde{G} be the edge-signed version of it associated to edge-signing $w : E \rightarrow \{\pm 1\}$. As observed by Bilu and Linial [BL06], this edge-signing is in a sense equivalent to the “2-lift” $G_2 = (V_2, E_2)$ of G defined by

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

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 \tilde{G} 's eigenvalues. (The latter refers to the eigenvalues of \tilde{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 \tilde{G} have magnitude at most $2\sqrt{d-1} + \epsilon$ (excluding G 's trivial eigenvalue of d), then the same is true of G_2 (excluding *its* trivial eigenvalue). Thus [Theorem 1.2](#) 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 ([Proposition 2.12](#)) that if G is “ r -bicycle-free” — meaning that every radius- r vertex neighborhood in G has at most one cycle — then G_2 will also be r -bicycle-free. Thus we may repeatedly double the number of vertices in an ϵ -near-Ramanujan graph, so long as the parameter r remains $\omega((\log \log |V|)^2)$, where $|V|$ is the “current” number of vertices. (Unfortunately, we do not see an obvious way to get the parameter r to increase as we perform 2-lifts.) This is roughly the same strategy employed in [\[BL06\]](#).

As a consequence, to obtain a final d -regular ϵ -near-Ramanujan graph with $\Theta(N)$ vertices, all we need to get started is 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, 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 $n = \text{quasipoly}(\log \log N)$.

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 $\text{poly}(N)$ 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. And as we will see in [Section 4](#), it is possible to derandomize Bordenave's proof in deterministic $n^{O(\log n)}$ time using $O(\log n)$ -wise uniform permutations. The proof of this is not completely straightforward because Bordenave's proof uses a twist on the Trace Method (since the plain Trace Method provably fails).

2 Preliminaries

2.1 Standard derandomization tools

Throughout we use **boldface** to denote random variables.

Definition 2.1 ((δ, k) -wise uniform bits). Let $\delta \in [0, 1]$ and $k \in \mathbb{N}^+$. A sequence of Boolean random variables $\mathbf{y} = (y_1, \dots, y_n) \in \{\pm 1\}^n$ is said to be (δ, k) -wise uniform² if, for every $S \subseteq [n]$ with $0 < |S| \leq k$, it holds that $|\mathbf{E}[\prod_{i \in S} y_i]| \leq \delta$. 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.

A classic result of Naor and Naor [\[NN93\]](#) shows that (δ, k) -wise uniform bits can be constructed efficiently and deterministically from a truly random seed of length $O(\log k + \log \log n + \log(1/\delta))$. Indeed, these bits can be generated “strongly explicitly” (using [\[Sho90\]](#); cf. [\[AGHP92\]](#)):

Theorem 2.2. ([\[NN93\]](#).) *There is a deterministic algorithm that, given δ, k , and N , runs in time $\text{poly}(N/\delta)$ and outputs a multiset $Y \subseteq \{\pm 1\}^N$ of cardinality $S = \text{poly}(k \log(N)/\delta)$ (a power of 2) such that, for $\mathbf{y} \sim Y$ chosen uniformly at random, the sequence \mathbf{y} is (δ, k) -wise uniform. Indeed, if the algorithm is additionally given $1 \leq s \leq S$ and $1 \leq i \leq N$ (written in binary), it can output the i th bit of the s th string in Y in deterministic time $\text{polylog}(N/\delta)$.*

²Frequently called (δ, k) -wise independent in the literature.

We will make use of the fact that the parameters in this theorem have excellent dependence on N and k . We now discuss the analogous concept for random permutations, where it is not known if the parameter dependence can be as strong.

Definition 2.3 ((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 $\pi \in S_n$ is said to be (δ, k) -wise uniform if, for every sequence $(i_1, \dots, i_k) \in [n]_k$, the distribution of $(\pi(i_1), \dots, \pi(i_k))$ 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.

Kassabov [Kas07] and Kaplan–Naor–Reingold [KNR09] independently obtained a deterministic construction of (δ, k) -wise uniform permutations with seed length $O(k \log n + \log(1/\delta))$. Again, the construction is even “strongly explicit”:

Theorem 2.4. ([KNR09, Kas07].) *There is a deterministic algorithm that, given δ, k , and n , runs in time $\text{poly}(n^k/\delta)$ and outputs a multiset $\Pi \subseteq S_n$ (closed under inverses) of cardinality $S = \text{poly}(n^k/\delta)$ (a power of 2) such that, for $\pi \sim \Pi$ chosen uniformly at random, π is a (δ, k) -wise uniform permutation. Indeed, if the algorithm is additionally given $1 \leq s \leq S$ and $1 \leq i \leq n$ (written in binary), it can output $\pi_s(i)$ and $\pi_s^{-1}(i)$ (where π_s is the s th permutation in Π) in deterministic time $\text{poly}(k \log(n/\delta))$.*

We will also use a convenient theorem of Alon and Lovett [AL13]:

Theorem 2.5. ([AL13].) *Let $\pi \in S_n$ be a (δ, k) -wise uniform permutation. Then one can define a (truly) k -wise uniform permutation $\pi' \in S_n$ such that the total variation distance between π and π' is $O(\delta n^{4k})$.*

Combining the previous two results yields the following:

Corollary 2.6. ([KNR09, Kas07, AL13]) *There is a deterministic algorithm that, given k and n , runs in time $\text{poly}(n^k)$ and outputs a multiset $\Pi \subseteq S_n$ (closed under inverses) such that, when $\pi \sim \Pi$ is chosen uniformly at random, π is n^{-100k} -close in total variation distance to a (truly) k -wise uniform permutation. (And the final “indeed” statement from Theorem 2.4 also holds.)*

2.2 Elementary graph theory

2.2.1 Random d -regular graphs

We will be concerned with d -regular (multi)graphs. We start by describing the standard way to generate random d -regular graphs: the *configuration model*, see [BC78, Bol80, Bol01].

Definition 2.7 (Configuration model). Given integers $n > d > 0$ with nd even, the *configuration model* produces a random n -vertex, d -regular undirected multigraph (with loops) G . This multigraph is induced by a uniformly random matching 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 i th edge emanating from vertex v). We identify 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 M being generated as follows: First a uniformly random permutation $\pi \in S_{nd}$ is chosen; then we set $M_{\pi(j), \pi(j+1)} = M_{\pi(j+1), \pi(j)} = 1$ for each odd $j \in [nd]$.

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

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

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

It is well known that a graph G drawn from the configuration model is simple — i.e., has no cycles of length 1 or 2 — with probability $\Omega_d(1)$. As it is pleasant to work with simple graphs, we will show in [Appendix A](#) that this continues to hold for *pseudorandom* d -regular graphs, when an $O(d^2)$ -wise uniform permutation is used in the configuration model. We also record the well known fact that for G drawn from the configuration model, when G is conditioned on being simple, its conditional distribution is uniformly random among all d -regular graphs.

Although the configuration model is the most natural way to generate large random d -regular graphs, the fact that it does not produce simple graphs with high probability is mildly annoying. (In particular, this causes a slight technical hitch for establishing our “probabilistically strongly explicit” construction.) To sidestep this, we will also consider the *random lift* model for producing random d -regular graphs.

Definition 2.8 (Lift model). Fix a (simple) *base* graph $\underline{G} = (\underline{V}, \underline{E})$ on \underline{n} vertices. Then for $n \in \mathbb{N}^+$, an n -lift of \underline{G} is graph G defined by a collection of permutations $\pi_{uv} \in S_n$, one for each edge $(u, v) \in \underline{E}$, 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 G a (uniformly) random n -lift of \underline{G} . Observe that if \underline{G} is a d -regular graph, then G is always a d -regular (simple) graph on $\underline{n}n$ vertices.

Bordenave [\[Bor19\]](#) also confirmed [Theorem 1.8](#) (the Alon Conjecture) in the case that G is a random n -lift of any fixed d -regular Ramanujan base graph \underline{G} . The simplest case is $\underline{G} = K_{d+1}$, the complete graph on $d + 1$ vertices. This gives a way to randomly construct arbitrarily large d -regular near-Ramanujan graphs that are always simple. We will also derandomize this result, as it will be convenient for our “probabilistically strongly explicit” construction to have guaranteed simplicity.

2.2.2 Bicycle-freeness

It is well known that a d -regular random graph is likely to have at most one cycle in any neighborhood of radius $c \log_{d-1} n$, for a certain universal $c > 0$. (This holds in either the configuration or the random lift model.) Let us make some definitions to codify this.

Definition 2.9 (Excess). Given a multigraph $H = (V, E)$, its *excess* is $\text{exc}(H) = |E| - |V|$.

Definition 2.10 (A/uni/bi-cyclic). A connected multigraph H with $\text{exc}(H) = -1, 0, 1$ (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 2.11 (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”. We remark that this notion was termed *r-tangle-free* by Bordenave [\[Bor19\]](#).

Proposition 2.12. *If G is bicycle-free at radius r , and G_2 is a 2-lift of G , then G_2 is bicycle-free at radius r .*

Proof. Let (v, i) be any vertex in G_2 . Let H be the neighborhood of v in G and let H_2 be the subgraph of G_2 induced by $V(H) \times [2]$. Observe that the distance- r neighborhood of (v, i) is contained in H_2 , and that $\text{exc}(H_2) \leq 0$ since $\text{exc}(H) \leq 0$. If H_2 is disconnected it is isomorphic to a disjoint union of two copies of H and thus the distance- r neighborhood of (v, i) is then isomorphic to H . Otherwise, if H_2 is connected, $\text{exc}(H_2) \leq 0$ implies that it has at most one cycle. \square

It is easy to see that any n -vertex, d -regular graph that is bicycle-free at radius r must have $r \lesssim \log_{d-1} n$. On the other hand, as mentioned earlier, a random d -regular graph achieves this bound up to a constant factor, and we will derandomize the proof of this fact, within the $O(\log n)$ -wise uniform configuration/lift model, in [Section 4.1](#).

In a graph that is bicycle-free at radius r , by definition we have $\text{exc}(H) \leq 0$ for all subgraphs H contained in a single distance- r neighborhood. In fact, this property is enough to guarantee that $\text{exc}(H)$ is small for *any* subgraph H with at most $\exp(r)$ vertices, regardless of whether it's contained in a single distance- r neighborhood:

Theorem 2.13. *Let H be a v -vertex graph that is bicycle-free at radius r . Assume $r \geq 10 \ln v$. Then $\text{exc}(H) \leq \frac{\ln(ev)}{r} v$.*

The rest of this subsection is devoted to the proof of the above theorem of elementary graph theory.

Definition 2.14 ($\text{Cyc}_g(G)$ and girth). Given a graph G , let $\text{Cyc}_g(G)$ denote the collection of all cycles in G of length at most g . Recall that if $\text{Cyc}_g(G)$ is empty then G is said to have *girth* exceeding g .

The following fact is essentially immediate from the definitions:

Fact 2.15. *Suppose G is bicycle-free at radius r . Then the cycles in $\text{Cyc}_{2r}(G)$ are vertex-disjoint.*

Indeed, more generally:

Proposition 2.16. *Suppose G is bicycle-free at radius r . For each $C \in \text{Cyc}_{2r}(G)$, let C^+ denote the collection of vertices within distance $r - \text{len}(C)/2$ of C . Then the sets $\{C^+ : C \in \text{Cyc}_{2r}(G)\}$ are pairwise disjoint.*

Proof. If $u \in C_1^+ \cap C_2^+$, the distance- r neighborhood of u is enough to include both C_1 and C_2 . \square

Next, let us now recall the “Moore bound for irregular graphs”. Suppose H is a graph with v vertices and $\text{exc}(H) = \epsilon v$; hence H has average degree $2 + 2\epsilon$. If we build a breadth-first search tree from some vertex, then after depth t we would “expect” to encounter at least $(1 + 2\epsilon)^t$ vertices. If this exceeds v — roughly, if $t \geq (\ln v)/(2\epsilon)$ — then the breadth-first search must encounter a cycle. Thus we have a heuristic argument that $\text{girth}(H) \lesssim (\ln v)/\epsilon$; i.e., $\epsilon \lesssim (\ln v)/\text{girth}(H)$. Indeed, Alon–Hoory–Linial have precisely established this kind of result; we quote their theorem in a slightly simplified form:

Theorem 2.17. ([\[AHL02\]](#).) *Let H be a graph with v vertices, $\text{exc}(H) = \epsilon v$ (for $\epsilon \geq 0$), and girth g . Then $v \geq (1 + 2\epsilon)^{g/2-3/2}$.*

Corollary 2.18. *Let H be a graph with $v \geq 3$ vertices and girth $g \geq 20 \ln v$. Then $\text{exc}(H) \leq ((2 \ln v)/g)v$.*

We can now prove [Theorem 2.13](#), which replaces “girth” with “bicycle-free radius” in the above with only a small loss in parameters.

Proof of Theorem 2.13. We will show the theorem assuming H is connected (the only case we’ll need). It is an exercise to extend it to the general case by considering H ’s connected components.

Let $c = |\text{Cyc}_{2r}(H)|$. By deleting at most c edges from H we can obtain a v -vertex graph \tilde{H} with girth at least (in fact, exceeding) $2r$. Applying [Corollary 2.18](#) to \tilde{H} , we conclude that $\text{exc}(\tilde{H}) \leq \frac{\ln v}{r} v + c$. Thus it remains to show $c \leq v/r$. This is trivial if $c = 0$, and if $c = 1$ then it can only fail if $r > v$ — but then H is unicyclic and hence has excess 0. Assuming then that $c \geq 2$, choose paths in H

to minimally connect the c cycles of $\text{Cyc}_{2r}(H)$. Now for each $C \in \text{Cyc}_{2r}(H)$, if we “charge” to it the $r - \text{len}(C)/2$ closest path-vertices, then no vertex is charged to multiple cycles, by virtue of [Proposition 2.16](#). If we also charge the vertices of C to itself, then for each $C \in \text{Cyc}_{2r}(H)$ we have charged a batch of $\text{len}(C) + (r - \text{len}(C)/2) > r$ vertices, and these batches are disjoint. Thus $cr \leq v$, i.e. $c \leq v/r$, as required. \square

2.3 Non-backtracking walks and the Ihara–Bass formula

The Friedman/Bordenave theorem ultimately uses the Trace Method to analyze the eigenvalues of random d -regular graphs; this involves counting closed walks in them. As observed in [\[Fri08, Bor19\]](#), it is much easier to count *non-backtracking* walks, and luckily the *Ihara–Bass formula* gives an easy translation between eigenvalues of the adjacency matrix of a graph and the eigenvalues of its *non-backtracking matrix*.

Definition 2.19 (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

$$B_{(u_1, v_1), (u_2, v_2)} = \begin{cases} 1 & \text{if } v_1 = u_2 \text{ and } v_2 \neq u_1, \\ 0 & \text{otherwise.} \end{cases}$$

(Note that this matrix is not symmetric in general.) In case G is an edge-signed graph, the entry 1 above should be replaced by A_{u_2, v_2} , the sign of G on edge $\{u_2, v_2\}$.

In a number-theoretic context, Ihara [\[Iha66\]](#) implicitly showed a relationship between the eigenvalues of A and B when G is regular. Serre [\[Ser77\]](#) and several others suggested the translation to graph theory, and Bass [\[Bas92\]](#) (following [\[Has89\]](#)) explicitly established:

Theorem 2.20. (*Ihara–Bass formula.*) Let G be a d -regular (multi)graph and write $q = d - 1$. Then

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

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 will use the following result, which is immediate from the edge-weighted generalization [\[WF09\]](#) when all weights are ± 1 :

Theorem 2.21. ([\[WF09\]](#).) The Ihara–Bass formula holds as stated above for edge-signed graphs.

The utility of Ihara–Bass is that it gives a direct correspondence between the spectra of A and B . To see this, consider the zeroes of the polynomials (in z) on the left- and right-hand sides. We have that z is a zero of the left-hand side precisely if z^{-1} is an eigenvalue of B . On the other hand, z is a zero of the right-hand side precisely if $z^{-1} = \pm 1$ or if z^{-1} is such that $z^{-1} + q/z^{-1}$ is an eigenvalue of A . Thus if we want to deduce, say, the eigenvalues of B from the eigenvalues of A , we have the following:

Proposition 2.22. (*Consequence of Ihara–Bass.*) Let $G = (V, E)$ be a $(q + 1)$ -regular edge-signed graph with adjacency matrix A and non-backtracking matrix B . Let $\lambda \neq 0, \pm 1$ be a number such that $\lambda + q/\lambda$ is an eigenvalue of A . Then λ is an eigenvalue of B .

In fact, [Proposition 2.22](#) is the only consequence of Ihara–Bass we will need in this paper, and for the convenience of the reader we give a self-contained proof (inspired by [\[AFH15\]](#)):

Proof. Let $f : V \rightarrow \mathbb{C}$ be an eigenvector for A with eigenvalue $\lambda + q/\lambda$. Define $g : \vec{E} \rightarrow \mathbb{C}$ by $g_{vw} = A_{vw}f_v - \lambda f_w$. We claim that $Bg = \lambda g$. It then follows that λ is an eigenvalue of B , given that $g \neq 0$ (a consequence of $f \neq 0$: choose $\{v, w\} \in E$ with f_v, f_w not both 0, and then $g_{vw} = 0 = g_{wv}$ is impossible because $\lambda \neq \pm 1$). To verify the claim, for any $uv \in \vec{E}$ we have

$$(Bg)_{uv} = \sum_{\substack{w \sim v \\ w \neq u}} A_{vw}g_{vw} = \sum_{w \sim v} A_{vw}(A_{vw}f_v - \lambda f_w) - A_{vu}(A_{vu}f_v - \lambda f_u) = -\lambda \sum_{w \sim v} A_{vw}f_w + qf_v + \lambda A_{vu}f_u.$$

But $\sum_{w \sim v} A_{vw}f_w = (Af)_v = (\lambda + q/\lambda)f_v$. Thus $(Bg)_{uv} = -\lambda^2 f_v + \lambda A_{vu}f_u = \lambda g_{uv}$, as needed. \square

When G is unsigned, A has a “trivial” eigenvalue of $d = q + 1$, corresponding to $\lambda = q$; this yields the “trivial” eigenvalue of $q = d - 1$ for B . For general edge-signed G , if $\lambda = \pm\sqrt{q} = \pm\sqrt{d-1}$ in [Proposition 2.22](#), then $\lambda + q/\lambda = \pm 2\sqrt{q} = \pm 2\sqrt{d-1}$. Thus the Ramanujan eigenvalue bound of $2\sqrt{d-1}$ for A is equivalent to the bound $\sqrt{d-1}$ for B . As for the “ $+\epsilon$ ”, a simple calculation (appearing in [\[Bor19\]](#)) shows:

Corollary 2.23. *Let $G = (V, E)$ be a d -regular edge-signed graph ($d \geq 3$) with adjacency matrix A and non-backtracking matrix B . If A has an eigenvalue of magnitude $2\sqrt{d-1} + \epsilon$ (for $\epsilon \geq 0$) then B has an eigenvalue of magnitude $\sqrt{d-1} + \sqrt{\epsilon}\sqrt{\sqrt{q} + \epsilon/4} + \epsilon/2$ (which is $\sqrt{d-1} + \Theta(d^{1/4}\sqrt{\epsilon})$ for fixed d and $\epsilon \rightarrow 0$).*

3 On random edge-signings of fixed base graphs

In this section we will prove [Theorem 1.2](#). In fact, we will prove the following refined version:

Theorem 3.1. *Let $G = (V, E)$ be an arbitrary d -regular n -vertex graph, where $d \leq \text{polylog } n$. Assume that G is bicycle-free at radius $r \gg (\log \log n)^2$. Then for G a uniformly random edge-signing of G , except with probability at most n^{-100} the non-backtracking matrix B of G satisfies the spectral radius bound*

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

and hence (by [Corollary 2.23](#)) the signed adjacency matrix A of G satisfies the bound

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

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

As in [\[Fri08, Bor19\]](#), the proof of [Theorem 3.1](#) will use the Trace Method. In preparation for this, we make some definitions:

Definition 3.2 (Hikes). Let $G = (V, E)$ be an undirected graph. For $\ell \in \mathbb{N}$, we define an ℓ -hike \mathcal{H} to be a closed walk in G of exactly 2ℓ steps which is non-backtracking except possibly between the ℓ th and $(\ell + 1)$ th step. Given an edge-signing $w : E \rightarrow \{\pm 1\}$ we write $w(\mathcal{H})$ for the product of the edge-signs that \mathcal{H} traverses, counted with multiplicity. Finally, we call a hike *even* (respectively, *singleton-free*) if each undirected edge traversed by \mathcal{H} is traversed an even number of times (respectively, at least twice).

A straightforward use of the Trace Method will now imply:

Proposition 3.3. *Let $\ell \in \mathbb{N}^+$ and define $T = \text{tr}(B^\ell (B^\top)^\ell)$ (which is an upper bound on $\rho(B)^{2\ell}$). Then for a uniformly random edge-signing $w : E \rightarrow \{\pm 1\}$,*

$$\mathbb{E}[T] \leq d^2 \cdot \#\{\text{even } (\ell - 1)\text{-hikes } \mathcal{H} \text{ in } G\} \leq d^2 \cdot \#\{\text{singleton-free } (\ell - 1)\text{-hikes } \mathcal{H} \text{ in } G\}.$$

Furthermore, if w is merely $(\delta, 2\ell)$ -wise uniform, the bound holds up to an additive $\delta nd^{2\ell+2}$.

Proof. We have

$$T = \sum_{\vec{e}_0, \vec{e}_1, \dots, \vec{e}_{2\ell-1}, \vec{e}_{2\ell} = \vec{e}_0 \in \vec{E}} B_{\vec{e}_0, \vec{e}_1} B_{\vec{e}_1, \vec{e}_2} \cdots B_{\vec{e}_{\ell-1}, \vec{e}_\ell} B_{\vec{e}_{\ell+1}, \vec{e}_\ell} B_{\vec{e}_{\ell+2}, \vec{e}_{\ell+1}} \cdots B_{\vec{e}_{2\ell}, \vec{e}_{2\ell-1}}. \quad (1)$$

Recalling the definition of B , one immediately sees that T is “something like” the sum of $w(\mathcal{H})$ over all ℓ -hikes in G . But being careful, one sees we precisely have the following:

T is equal to the sum of $w(\mathcal{H})$ over all “special” $(\ell + 1)$ -hikes in G , where we call an $(\ell + 1)$ -hike *special* if its $(\ell + 2)$ th step is the reverse of its $(\ell + 1)$ th step, and the last step is the reverse of the first step.³

Next, we employ the following easy fact:

Fact 3.4. *If $w : E \rightarrow \{\pm 1\}$ is a fully uniformly random edge-signing, then $\mathbb{E}[w(\mathcal{H})]$ will be 1 if \mathcal{H} is an even hike, and will be 0 otherwise.*

Thus

$$\mathbb{E}_{w:E \rightarrow \{\pm 1\}}[T] = \#\{\text{even, special } (\ell + 1)\text{-hikes } \mathcal{H} \text{ in } G\}. \quad (2)$$

Since an $(\ell + 1)$ -hike involves at most 2ℓ undirected edges, a crude upper bound on the number of all $(\ell + 1)$ -hikes in G is $nd^{2\ell}$. Thus for an edge-signing w that is merely $(\delta, 2\ell)$ -wise uniform, Equation (2) holds up to an additive $\delta nd^{2\ell}$. Finally, every even special $(\ell + 1)$ -hike \mathcal{H} can be formed from an even $(\ell - 1)$ -hike \mathcal{H}' by: (i) attaching a step and its reverse to the beginning/end of \mathcal{H} ; (ii) attaching a step and its reverse to the midpoint of \mathcal{H} . As there are at most $(d - 1)^2 \leq d^2$ choices for how to perform (i) and (ii), the inequality in the proposition’s statement follows. \square

At this point, edge-signs are out of the way and we are reduced to counting singleton-free hikes. In aid of this, we borrow some terminology from [MOP19]:

Definition 3.5. Given an $(\ell - 1)$ -hike \mathcal{H} in graph G , we write $G_{\mathcal{H}} = (V_{\mathcal{H}}, E_{\mathcal{H}})$ for the subgraph of G formed by the union of the edges visited by \mathcal{H} . We think of $G_{\mathcal{H}}$ as being “revealed” as the $2(\ell - 1)$ steps of \mathcal{H} are taken in order. We classify each step of \mathcal{H} as either *stale*, *fresh*, or *boundary*. If a step of \mathcal{H} traverses a previously-explored edge in $G_{\mathcal{H}}$ (in either direction), we call the step *stale*; otherwise, if it steps to a previously-unvisited vertex, we call the step *fresh*; otherwise, we call it *boundary*. For the purposes of this definition, at the beginning of \mathcal{H} the initial vertex is considered to be “previously visited”.

We now put bounds on the different kinds of steps. For the fresh steps, we only need the singleton-free property:

³The astute reader will note that the sign of the first/last edge in \mathcal{H} is never counted in Equation (1); however it is okay to count it twice, as $w(\mathcal{H})$ does, since $(\pm 1)^2 = 1$.

Proposition 3.6. *In a singleton-free $(\ell - 1)$ -hike, at least half of all steps must be stale. Thus there are fewer than ℓ fresh steps.*

For the boundary steps of \mathcal{H} , it is easy to see that there are exactly $\text{exc}(G_{\mathcal{H}}) + 1$ of them. Thus we can bound them using only the bicycle-free property. Together with the simple bound $|V_{\mathcal{H}}| \leq 2\ell$, [Theorem 2.13](#) implies

Proposition 3.7. *If \mathcal{H} is an $(\ell - 1)$ -hike in a graph G which is bicycle-free at radius $r \geq 10 \ln(2\ell)$, then \mathcal{H} has at most $O(\frac{\log \ell}{r}) \cdot \ell$ boundary steps.*

Finally, to handle the stale steps we group them into “stretches”.

Proposition 3.8. *In an $(\ell - 1)$ -hike \mathcal{H} , the stale steps may be partitioned into at most $O(\frac{\log \ell}{r}) \cdot \ell$ stretches of consecutive stale steps, each stretch having length at most r , and none straddling the “turnaround” at step ℓ .*

Proof. We begin by partitioning the stale steps into maximal contiguous stretches. It is easy to see that each of these must be preceded in \mathcal{H} by a boundary step (with a single possible exception of the “turnaround” at step ℓ). Thus [Proposition 3.7](#) implies that there are at most $O(\frac{\log \ell}{r}) \cdot \ell$ maximal stretches of stale steps. If a maximal stretch straddles the turnaround, we can split it in two. Finally, if necessary we now subdivide the stretches into length at most r . Since there are fewer than 2ℓ stale steps, this subdivision can be done without increasing the number of stretches by more than $2\ell/r \leq O(\frac{\log \ell}{r}) \cdot \ell$. \square

We may now make our final estimate:

Theorem 3.9. *In a d -regular graph G that is bicycle-free at radius $r \geq 10 \ln(2\ell)$, the number of singleton-free $(\ell - 1)$ -hikes \mathcal{H} is at most $O(\ell^3 n) \cdot (d - 1)^\ell \cdot (dr\ell)^{O(\frac{\log \ell}{r}) \cdot \ell}$.*

Proof. Following [\[Bor19\]](#), we use an encoding argument. To each \mathcal{H} we associate a string $\text{STRUCT}(\mathcal{H})$ over the alphabet $\{F, B, S\}$, where we replace each fresh step with an F , each boundary step with a B , and each stale stretch with an S . Our goal will be to show:

Claim 3.10. *For any string σ with c_f, c_b, c_s occurrences of F, B, S (respectively), there are no more than $2n \cdot (d - 1)^{c_f + c_b} \cdot (2r\ell)^{c_s}$ singleton-free $(\ell - 1)$ -hikes \mathcal{H} with $\text{STRUCT}(\mathcal{H}) = \sigma$.*

Let us complete the proof of the theorem assuming this claim. By [Propositions 3.6](#) to [3.8](#), we have the bounds

$$c_f < \ell, \quad c_b, c_s < m := O(\frac{\log \ell}{r}) \cdot \ell.$$

Crudely, there are at most $O(\ell^3)$ possibilities for the triple (c_f, c_b, c_s) . Also, the following two quantities are increasing in c_f, c_b, c_s :

$$2n \cdot (d - 1)^{c_f + c_b} \cdot (2r\ell)^{c_s}, \quad \Sigma_{c_f, c_b, c_s} := \# \text{ strings of } c_f \text{ F's, } c_b \text{ B's, } c_s \text{ S's.}$$

Thus we can upper-bound the number of all singleton-free $(\ell - 1)$ -hikes by

$$O(\ell^3 n) \cdot (d - 1)^{\ell + m} \cdot (2r\ell)^m \cdot \Sigma_{\ell, m, m} \leq O(\ell^3 n) \cdot (d - 1)^\ell \cdot (dr\ell)^{O(m)},$$

as needed, where we used the simple bound $\Sigma_{\ell, m, m} \leq \ell^{O(m)}$.

It remains to prove the claim. Let σ be as given. We may recover all possible associated \mathcal{H} , in a vertex-by-vertex fashion, by first specifying the initial vertex (n choices) and then proceeding

through the symbols of σ in order. If we are at an F or a B symbol, we can recover the next vertex by specifying one of $d - 1$ neighbors of the current vertex; there are only $d - 1$ possibilities, since \mathcal{H} is non-backtracking. (Exception: there are d choices at the very beginning of the hike; we compensated for this with the factor $2 > \frac{d}{d-1}$.) To complete the proof of the claim, we need to show that for each stale stretch, there are at most $2r\ell$ possibilities. Recall that a stale stretch beginning from a vertex v consists of walking in non-backtracking fashion for at most r steps over the previously seen portion K of $G_{\mathcal{H}}$. This subgraph K has at most 2ℓ vertices, and by the bicycle-free property, this walk is confined to a subgraph of K that is at most unicyclic. It is easy to see this walk is determined by specifying its final vertex (at most 2ℓ possibilities), the number of times the cycle in v 's distance- r neighborhood (should it exist) is traversed (fewer than $r/2$ possibilities), and the direction in which the cycle is traversed (2 possibilities). Thus indeed each stale stretch can be completely determined by specifying one of at most $2\ell \cdot (r/2) \cdot 2 = 2r\ell$ possibilities. \square

Combining this with [Proposition 3.3](#) now yields:

Corollary 3.11. *Let $G = (V, E)$ be an arbitrary d -regular n -vertex graph. Assume that G is bicycle-free at radius r . Let $\ell \in \mathbb{N}^+$ and $0 < \eta < 1$ be parameters. Then for \mathbf{G} a uniformly random edge-signing of G , except with probability at most η the non-backtracking matrix \mathbf{B} of \mathbf{G} has spectral radius bound*

$$\rho(\mathbf{B}) \leq \sqrt{d-1} \cdot (1 + O(\epsilon_1) + O(\epsilon_2)), \quad (3)$$

where

$$\epsilon_1 := \frac{\log(n/\eta)}{\ell}, \quad \epsilon_2 := \frac{\log(d\ell) \log(\ell)}{r},$$

provided $\epsilon_1, \epsilon_2 \leq 1$.

Furthermore, if the random edge-signs of \mathbf{G} are merely $(\delta, 2\ell)$ -wise uniform, the bound holds up to an additional additive $(\delta n / \eta)^{\frac{1}{2\ell}} \cdot O(d)$.

Proof. We have obtained that, for a uniformly random edge-signing $w : E \rightarrow \{\pm 1\}$,

$$\mathbf{E}[T] \leq O(d^2 \ell^3 n) \cdot (d-1)^\ell \cdot (dr\ell)^{O(\frac{\log \ell}{r}) \cdot \ell}.$$

Note that $r \lesssim \log_{d-1} n$ always holds, and hence we must have $\ell \leq n$ (else $\epsilon_2 > 1$). Also we must have $\ell \geq \log n$ (else $\epsilon_1 > 1$). Thus we may coarsen $O(d^2 \ell^3 n)$ in the above to $O(n^5)$, and coarsen $(dr\ell)^{O(\cdot)}$ to $(d\ell)^{O(\cdot)}$. Now since T is a nonnegative random variable, Markov's inequality implies that except with probability at most η ,

$$T \leq O(n^5 / \eta) \cdot (d-1)^\ell \cdot (d\ell)^{O(\frac{\log \ell}{r}) \cdot \ell},$$

and hence

$$\rho(\mathbf{B}) \leq T^{\frac{1}{2\ell}} \leq O(n^5 / \eta)^{\frac{1}{2\ell}} \cdot \sqrt{d-1} \cdot (d\ell)^{O(\frac{\log \ell}{r})},$$

which directly implies [Inequality \(3\)](#).

Finally, in the $(\delta, 2\ell)$ -wise uniform case, we get an additional additive $\delta n d^{2\ell+2}$ in the bound on $\mathbf{E}[T]$; this gets a factor of $1/\eta$ after the application of Markov, and becomes $(\delta n / \eta)^{\frac{1}{2\ell}} \cdot O(d)$ after taking 2ℓ th roots. \square

Finally, the reader may verify that [Theorem 3.1](#) follows from [Corollary 3.11](#) in the fully uniform case by taking $\ell = \Theta(r \log(n) / \log \log n)$, and in the derandomized case by taking $\ell = \Theta(C \log(n/\eta))$.

Remark 3.12. Alternatively, by taking $\eta = \exp(-\exp(r^{49}))$ and $\ell = \exp(r^{49})$ in [Corollary 3.11](#), we may conclude that $\rho(\mathbf{B}) \leq \sqrt{d-1} \cdot (1 + o_r(1))$ holds in the fully uniform case except with probability at most $\exp(-\exp(r^{49}))$.

4 Weakly derandomizing Bordenave’s theorem

In this section we give a weak derandomization of Bordenave’s proof of [Theorem 1.8](#), using “off-the-shelf” tools; the derandomization is “weak” in the sense that it only yields a quasipoly(n)-time deterministic construction. As discussed in [Section 2.2.1](#), we will derandomize both the configuration model version and the random lift version. Specifically, we show the conclusion of [Theorem 1.8](#) holds even for the “almost k -wise uniform” versions of these models, $k = O(\log n)$.

Definition 4.1 ((δ, k) -wise uniform configuration/lift models). When the permutation $\pi \in S_{nd}$ used in the configuration model is not uniformly random but is merely (δ, k) -wise uniform, we will say that G is drawn from the (δ, k) -wise uniform configuration model. Similarly, when the $\pi_{uv} \in S_n$ used in the random lift model are independent but merely (δ, k) -wise uniform, we will say that G is a (δ, k) -wise uniform random n -lift of base graph \underline{G} .

(For simplicity, in the lift model we will henceforth only concern ourselves with $\underline{G} = K_{d+1}$.)

We will not fully recap Bordenave’s proof of [Theorem 1.8](#) in this work, although the reader unfamiliar with it will get some insight knowing that our proof of [Theorem 3.1](#) is modeled on it. Bordenave employs two twists on the Trace Method to show that a random d -regular graph G has spectral radius at most $2\sqrt{d-1} + \epsilon$ (when the trivial eigenvalue of d is ignored). The less important (but still challenging) twist involves replacing the non-backtracking matrix B by a centered variant, \underline{B} , that enables one to ignore the trivial eigenvalue. The more conceptually important twist comes from the fact, originally recognized by Friedman, that even after passing to \underline{B} , the Trace Method still fails. The reason, in brief, is as follows: A successful use of the Trace Method would have to consider walks of length ℓ for ℓ at least a large multiple of $\log n$, in order to overcome the factor of n arising from the n different walk starting points (cf. the error term ϵ_1 just after [Inequality \(3\)](#)). But for walks of this long length, one can show that the expected trace of $\underline{B}^\ell (\underline{B}^\top)^\ell$ is simply too large — much larger than the target $\text{poly}(n) \cdot (d-1)^\ell$ needed to get the “correct” final bound.

However, as first demonstrated by Friedman, the expectation is too large only because of certain low-probability events. Bordenave’s way of handling things is to show that: (i) a random d -regular graph G is, with high probability, bicycle-free at large radius r ; (ii) when G is so bicycle-free, the r th power of its non-backtracking matrix, B^r , coincides with a certain “bicycle-discarding” variant $B^{(r)}$; (iii) the usual Trace Method *can* be successfully applied to $B^{(r)}$; i.e., the expected trace of powers of $\underline{B}^{(r)}$ is suitably small.

Thus our weak derandomization of Bordenave’s proof has two ingredients, corresponding to (i) and (iii) above. In [Section 4.1](#) we derandomize a standard proof that a random d -regular graph is bicycle-free at large radius (in either the configuration model or the random lift model). In [Section 4.2](#) we examine the key probabilistic ingredient in Bordenave’s use of the Trace Method, [[Bor19](#), Prop. 11], which encapsulates the fact that for a centered version \underline{M} of the configuration model matching matrix, the random variables $\underline{M}_{(v,i),(v',i')}$ are close to k -wise independent for $k \ll \sqrt{dn}$.

(In [Appendix A](#), we also show a derandomization of the most basic fact about the configuration model, that G is simple with probability $\Omega_d(1)$. This is just a “bonus” for the reader who prefers the configuration model; it will be more convenient to use the random lift model for our explicit near-Ramanujan graphs, due to its guaranteed simplicity.)

4.1 Bicycle-freeness

The following relatively straightforward fact about d -regular n -vertex graphs is crucial for Bordenave’s proof: with high probability they are bicycle-free at radius r , provided $r \lesssim c \log_{d-1} n$ for some constant $c < 1/4$. This fact is proved for completeness by Bordenave [Bor19, Lem. 9] (and in [Bor19, Lem. 27] for random lifts); another proof appears earlier in, e.g., [LS10, Lem. 2.1]. We would like a derandomized version of this fact for the k -wise uniform configuration model, $k = O(r)$. This motivates looking for a moments-based proof, such as the one suggested by Wormald [Wor99, Lem. 2.7] and carried out for Erdős–Rényi $\mathcal{G}(n, m)$ graphs in [JLR00, Thm. 5.5]. The essential point will be that minimal witnesses to failure have only $O(r)$ edges.

Definition 4.2 (Minimal bicycle). We say a connected multigraph is a *minimal bicycle* if it is bicyclic but has no proper subgraph that is bicyclic. It is easy to see (cf. [JLR00, Proof of Thm. 5.5]) that any minimal bicycle is either a “handcuffs graph” (two cycles joined by a path), a “figure-eight graph” (two cycles attached at a vertex), or a “theta graph” (a cycle with a “diagonal”).

We now prove:

Proposition 4.3. Fix $d \geq 3$ and $k \geq 1$. Let G be drawn from the d -regular n -vertex configuration model using a $2k$ -wise uniform permutation. Then G is bicycle-free at radius $k/4$, except with probability at most $O(k^3(d-1)^k/n)$.

As a corollary, the failure probability is at most $1/n^{.99}$ provided $k < c \log_{d-1} n$ for a certain universal $c > 0$. This statement remains true if G is instead a $2k$ -wise uniform random n -lift of K_{d+1} . Finally, by [Theorem 2.5](#), these statements remain true in the $(\delta, 2k)$ -wise uniform versions of the models, $\delta \leq 1/n^{8k+2}$.

Proof. We first consider the configuration model. Fix a minimal bicycle H with h vertices and hence $h+1$ edges, where $h < k$. Let the random variable X_H denote the number of times that H appears in G . This is a polynomial of degree at most $h+1 \leq k$ in the entries of G ’s adjacency matrix and hence a polynomial of degree at most $2k$ in the permutation indicators $1[\pi(j) = (v, i)]$. Thus to compute $\mathbb{E}[X_H]$ we may assume G is drawn from the usual configuration model (with a truly random permutation). In this case, it is elementary to compute an exact formula for $\mathbb{E}[X_H]$; as per [Bor16, eqn. (2.4)], it is

$$\mathbb{E}[X_H] = \frac{1}{bc} \frac{n(n-1)(n-2) \cdots (n-h+1)}{(nd-1)(nd-3)(nd-5) \cdots (nd-2h-1)} \prod_{u \in V(H)} d(d-1) \cdots (d - \deg_H(u) + 1), \quad (4)$$

where b (respectively, c) is the number of edge- (respectively, vertex-)isomorphisms of H . For any minimal bicycle H we have $b \geq 1$, $c \geq 2$, and $\deg_H(u) \geq 2$ for all $u \in V(H)$. The last of these facts implies the product on the right in [Equation \(4\)](#) is at most $(d(d-1))^{h+1}$. Also, the large fraction in the middle is asymptotic to $(d^{h+1}n)^{-1}$, and it is not hard to check it is always at most twice that. Hence we conclude $\mathbb{E}[X_H] \leq (d-1)^{h+1}/n \leq (d-1)^k/n$. Finally, it is easy to see that, up to isomorphism, the number of minimal bicycles with fewer than k vertices is at most $O(k^3)$. Thus by Markov’s inequality we conclude that the probability of having any minimal bicycle on fewer than k vertices is at most $k^3(d-1)^k/n$. The claim about the configuration model now follows because any bicyclic radius- $k/4$ vertex neighborhood in G must contain a minimal bicycle with fewer than k vertices. (The “worst case” is a figure-eight graph.)

As for the model where G is a $2k$ -wise uniformly random n -lift of K_{d+1} , the proof is nearly identical. The only difference arises in the computation of $\mathbb{E}[X_H]$ — instead of using an exact closed form expression for the quantity, one can elementarily upper bound $\mathbb{E}[X_H]$ by $O((d+1)^h/n)$ (assuming, say, $k \leq \sqrt{n}$). From this slightly weaker bound, one can still draw the same conclusion that the failure probability is at most $1/n^{.99}$ for $k < c \log_{d-1} n$ (possibly with slightly smaller c). \square

4.2 Bordenave's key probabilistic proposition

In this section we examine the last place in Bordenave's argument that uses randomness of the underlying graph G ; namely, [Bor19, Prop. 11] for the configuration model and [Bor19, Prop. 28] for the random lift model. These nearly-identical propositions give an upper bound on a certain moment arising in his use of the Trace Method. Unfortunately, the propositions are not as self-contained as the ones covered in Section 4.1. Rather than trying to give a complete summary of how Bordenave's argument works, we will proceed in a "black-box" fashion, only giving the bare minimum needed to verify derandomizability. We refer the reader to [Bor19] for the complete picture. As in [Bor19], we will focus on the configuration model, and then describe the modifications necessary for the random lift model.

Here is the key probabilistic proposition (which can be viewed as a far more sophisticated version of Fact 3.4):

Proposition 4.4. ([Bor19, Prop. 11].) *Let $\vec{E} = [n] \times [d]$, and let \mathbf{M} be a uniformly random matching on \vec{E} as in the configuration model Definition 2.7. Also let $\underline{\mathbf{M}}$ be the matrix obtained from \mathbf{M} by subtracting $\frac{1}{n'}$ from each entry, where $n' := dn$. Then for any $\gamma \in \vec{E}^{2k}$ with $1 \leq k \leq \sqrt{m}$ and any $0 \leq k_0 \leq k$, we have*

$$\left| \mathbb{E} \left[\prod_{t=1}^{k_0} \underline{\mathbf{M}}_{\gamma_{2t-1}, \gamma_{2t}} \prod_{t=k_0+1}^k \mathbf{M}_{\gamma_{2t-1}, \gamma_{2t}} \right] \right| \leq O \left(2^b \cdot \left(\frac{1}{n'} \right)^a \cdot \left(\frac{3k}{\sqrt{n'}} \right)^{a_1} \right). \quad (5)$$

Here a , b , and a_1 on the right-hand side of Inequality (5) are certain quantities relating to the multiplicities of half-edges in γ and to k_0 . We omit these definitions here, as they won't be relevant for us.

Note that when \mathbf{M} is formed from a random permutation π on $[nd]$ as in Definition 2.7, each entry $M_{e,f}$ is a polynomial of degree 2 in the indicators $1[\pi(j) = (v, i)]$. It follows that the quantity inside the expectation in Inequality (5) is a polynomial of degree at most $2k$ in these indicators. We conclude:

Corollary 4.5. *Let G be drawn from the d -regular n -vertex configuration model using a $2k$ -wise uniform permutation, and write \mathbf{M} for the matching matrix inducing G . Then Inequality (5) continues to hold.*

Bordenave also proved an analogue of Proposition 4.4 for the random lift model. The statement is extremely similar to Proposition 4.4, with " n " being n , and with the rows/columns of " \mathbf{M} " being the potential "half-edges" in the lifted graph; for the exact statement we refer the reader to [Bor19, Prop. 28]. Further, Corollary 4.5 is true when G is drawn from a $2k$ -wise uniform lift model.

With Proposition 4.4 in hand, Bordenave does some intricate — but entirely non-probabilistic — path-counting to complete his use of the Trace Method. (This is like a much more sophisticated version of the part of Section 3 beginning with Definition 3.2.) This part of his proof involves considering paths of length $2\ell m$, where " ℓ " and " m " are parameters he selects (with ℓ being at least the bicycle-free radius, and m being large enough so that $\ell m \gg \log n$). The crucial observation for us is that Bordenave *only* employs Proposition 4.4 with its parameter " k " set to $2\ell m$ (and the same is true in the random lift model).

Bordenave directly sets $\ell = \Theta(\log_{d-1}(n))$ and $m = \Theta(\log(n)/\log \log(n))$ to obtain best parameters, but we will work more generally, since we may be interested in minimizing $k = 2\ell m$ to save on random bits. Carefully examining [Bor19, Proofs of Prop. 14, 18], one may extract the below proposition. The random matrices $\underline{\mathbf{B}}^{(\ell)}$ and $\mathbf{R}_1^{(\ell)}, \dots, \mathbf{R}_\ell^{(\ell)}$ mentioned in it are derived from the randomness of the configuration model; again, see [Bor19] for details.

Proposition 4.6. Assuming d, ℓ, m satisfy $\text{poly}(d\ell m)^m \ll n$, it holds that

$$\mathbb{E} \left[\|\underline{\mathbf{B}}^{(\ell)}\|^{2m} \right] \leq \text{poly}(n) \cdot (d-1)^{\ell m}, \quad \mathbb{E} \left[\sum_{i=1}^{\ell} \|\underline{\mathbf{R}}_i^{(\ell)}\|^{2m} \right] \leq \text{poly}(d\ell m)^m \cdot (d-1)^{2\ell m},$$

Furthermore, this only relies on [Inequality \(5\)](#) with $k = 2\ell m$, and therefore by [Corollary 4.5](#) it continues to hold even in the $4\ell m$ -wise independent configuration model. Thus in this model, Markov's inequality implies that except with probability at most n^{-100} ,

$$\|\underline{\mathbf{B}}^{(\ell)}\| \leq \text{poly}(n)^{\frac{1}{2m}} \cdot \sqrt{d-1}^{\ell}, \quad \sum_{i=1}^{\ell} \|\underline{\mathbf{R}}_i^{(\ell)}\| \leq \text{poly}(n)^{\frac{1}{2m}} \cdot (d-1)^{\ell}.$$

This proposition holds just the same in the random lift model with base graph $\underline{G} = K_{d+1}$ (indeed, with any d -regular base graph). One simply has to follow through the analogous propositions, [[Bor19](#), Proofs of Prop. 29, 33], in the same way.⁴

Finally, [[Bor19](#), Prop. 8] is the following:

Proposition 4.7. Suppose \mathbf{G} drawn from the d -regular configuration model is bicycle-free at radius ℓ . Let $n' = dn$. Then the largest magnitude eigenvalue of the associated non-backtracking matrix \mathbf{B} , excluding the trivial eigenvalue of d , is at most

$$\left(\|\underline{\mathbf{B}}^{(\ell)}\| + \frac{1}{n'} \cdot \sum_{i=1}^{\ell} \|\underline{\mathbf{R}}_i^{(\ell)}\| \right)^{1/\ell}.$$

Again, Bordenave has a very similar analogue [[Bor19](#), Prop. 26] in the random lift model, with “ n' ” equal to n , and with the quantity bounding the largest-in-magnitude “new” eigenvalue of the lifted graph (which is precisely what one needs to bound to show the near-Ramanujan property, assuming the base graph is itself d -regular Ramanujan).

We can now finish the proof as Bordenave does (in either the configuration or random lift model), combining [Corollary 2.23](#), [Propositions 4.3, 4.6](#) and [4.7](#), and also [Proposition A.1](#) (if desired). Using the parameter settings $\ell = c \log_{d-1} n$ and $m = (C/c) \log(d-1)/\sqrt{\epsilon}$ where c is the constant from [Proposition 4.3](#) and C is a large enough universal constant, we get the following:

Theorem 4.8. Fix $3 \leq d \leq C^{-1} \sqrt{\log n}$ and let $\epsilon \leq 1$ and k satisfy

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

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

- \mathbf{G} is bicycle-free at radius $c \log_{d-1} n$;
- $\lambda(\mathbf{G}) \leq 2\sqrt{d-1} \cdot (1 + \epsilon)$.

Additionally, in the configuration model case, \mathbf{G} is simple with probability at least $e^{-(d-1)^2/4}/2$. Finally, by [Theorem 2.5](#), these statements remains true in the (δ, k) -wise uniform configuration model, $\delta \leq 1/n^{8k+1}$.

⁴Bordenave carries these propositions out for not-necessarily-regular base graphs of maximum degree d . His computations depend on the base graph through the Perron eigenvalue ρ_1 of its non-backtracking operator B , which in the d -regular case is just $d-1$. In [[Bor19](#), (67)] Bordenave selects $\rho > \rho_1$ and $c_\rho \geq 1$ such that $\|(B^\top)^k \mathbf{1}_e\|_1 \leq c_\rho \rho^k$ holds for all k and all edges in the base graph. In our d -regular case, we can simply take $c_\rho = 1$ and $\rho = \rho_1 = d-1$ when carrying through his computations.

5 Explicit near-Ramanujan graphs

With the tools developed in [Section 3](#) and [Section 4](#) we are now ready to establish our explicit near-Ramanujan graph constructions. For ease of reading, in this section we will merely prove [Theorem 1.1](#), the deterministic polynomial-time (“weakly explicit”) construction, with d and ϵ assumed to be constant. We leave the slightly more technical proof of the “probabilistically poly $\log n$ -time computable” construction ([Theorem 1.13](#)), with worked out dependence on $d = d(n)$ and $\epsilon = \epsilon(n)$, for [Appendix B](#).

Recall we want to show there is a deterministic algorithm that on input $N, d \geq 3$ and $\epsilon > 0$, outputs in $\text{poly}(N)$ -time a d -regular graph G on $N' \sim N$ vertices with $\lambda(G) \leq 2\sqrt{d-1} + \epsilon$.

Before getting into the details, we recap the construction as outlined in [Section 1.4](#):

1. Using [Theorem 4.8](#) 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 $\lambda(G_0) \leq 2\sqrt{d-1} + \epsilon$. The quantity n_0 should satisfy

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

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 $\text{poly}(N)$ time. We have a wide range of allowable possibilities here; for concreteness we will take n_0 near the upper limit to allow for slightly better dependence on non-constant d, ϵ in [Appendix B](#).

2. Next we repeatedly use [Theorem 3.1](#) (roughly $\log(N/n_0) \sim \log N$ times) to double the number of vertices in our construction from Step 1, while keeping $\lambda \leq 2\sqrt{d-1} + \epsilon$ and also retaining that the graph is bicycle-free at radius $\Omega(\log n_0)$ ([Proposition 2.12](#)). Importantly, since [Theorem 3.1](#) is a high-probability result, we will be able to reuse the seed for each of the $\log N$ pseudorandom edge-signings.

Step 1 details. Here the algorithm will select n_0 to be an even integer on the order of $2^{\Theta(\sqrt{\log N})}$. [Theorem 4.8](#) tells us that for a sufficiently large $k = O(\log n_0) = O(\sqrt{\log N})$, and for sufficiently small $\delta = n_0^{-\Theta(k)} = 1/\text{poly}(N)$, a random d -regular n_0 -vertex graph G_0 chosen from the (δ, k) -wise uniform configuration/random-lift-of- K_{d+1} model will with high probability satisfy:

$$G_0 \text{ is bicycle-free at radius } \Omega(\log n_0) = \Omega(\sqrt{\log N}); \quad \lambda(G_0) \leq 2\sqrt{d-1} + \epsilon. \quad (6)$$

(Recall we are treating d and ϵ as constant here.) G_0 will also be simple with $\Omega(1)$ probability in the configuration model case, and with probability 1 in the random lift case. In the former case, we need a (δ, k) -wise permutation in S_{nd} ; in the latter case, we need $\binom{d+1}{2}$ independent (δ, k) -wise permutations in S_n . Either way, [Theorem 2.4](#) tells us that a deterministic algorithm can enumerate all possibilities for G_0 in $\text{poly}(N)$ time and pick out any fixed simple one G_0 satisfying (6).

Step 2 details. Here the algorithm will be applying [Theorem 3.1](#) some $t \sim \log_2 N$ times, starting with G_0 , and each time interpreting the edge-signing produced as a 2-lift as discussed in [Section 1.4](#). This produces a sequence of pseudorandom d -regular simple graphs G_1, \dots, G_t , where G_i has $n_0 2^i$ vertices. The parameter t is chosen to be least possible such that the final number of vertices, $N' = n_0 2^t$, is at least N . It is not hard to check that by adjusting n_0 by a factor of at most 2, we can ensure that $N'/N = 1 + o_N(1)$, where the $o_N(1)$ term is $O(1/n_0) = 1/2^{\Theta(\sqrt{\log N})}$.

For simplicity, we will use the same values for the parameters r , k , and δ in each application of [Theorem 3.1](#); only the value of n will change (ranging from n_0 up to N'). We may take $r = \Omega(\sqrt{\log N})$, the bicycle-free radius from [Equation \(6\)](#) (observe that the bicycle-free radius cannot decrease for *any* 2-lift of a graph). Note that the failure probability of any single 2-lift is at most $1/2^{\Theta(\sqrt{\log N})}$, and hence a union bound tells us that the probability of *any* of the 2-lifts “failing” is low, $\frac{\log N}{2^{\Theta(\sqrt{\log N})}}$. We take the parameter “ k ” to be $\Theta\left(\frac{\log N}{\sqrt{\epsilon}}\right)$ (the hidden constant sufficiently large depending on d). Finally, we take $\delta = 1/N^{\Theta(1/\sqrt{\epsilon})}$ (again with the hidden constant sufficiently large depending on d). By plugging these parameters into [Theorem 3.1](#) we conclude that with high probability, all “new” eigenvalues arising in the 2-lifted adjacency matrices A_1, \dots, A_t are at most $2\sqrt{d-1} + \epsilon$ in magnitude, and hence G_t is ϵ -near Ramanujan.

It remains to observe that with these parameter settings, using [Theorem 2.2](#), a deterministic algorithm can in $\text{poly}(N/\delta) = \text{poly}(N)$ time do the following: First, produce a single $(\delta, 2\ell)$ -wise uniform multiset of strings $Y \subseteq \{\pm 1\}^{N'd/4}$; here $N'd/4$ bits are sufficient to edge-sign/2-lift any of the graphs G_i . Then, for $i = 1, \dots, t$ the algorithm can search Y for a “good” string $y_i \in Y$, meaning one with the property that using it to do an edge-signing/2-lift of G_i yields graph G_{i+1} which is ϵ -near Ramanujan. As argued in the previous paragraph, a $1 - O\left(\frac{\log N}{2^{\Theta(\sqrt{\log N})}}\right)$ fraction of strings in Y have this property. We can check the goodness of any string y in $\text{poly}(N)$ time using the following fact.

Fact 5.1. *For any rational approximation ρ of $2\sqrt{d-1} + \epsilon$, one can decide in $\text{poly}(n)$ time whether $\lambda(G) \leq \rho$.*

This concludes the proof of [Theorem 1.1](#).

Acknowledgments

We would like to thank Michael Forbes and Zander Kelley for pointing out an error in an earlier version of the paper.

References

- [AFH15] Omer Angel, Joel Friedman, and Shlomo Hoory. The non-backtracking spectrum of the universal cover of a graph. *Transactions of the American Mathematical Society*, 367(6):4287–4318, 2015. [2.3](#)
- [AGHP92] Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple constructions of almost k -wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992. [2.1](#)
- [AHL02] Noga Alon, Shlomo Hoory, and Nathan Linial. The Moore bound for irregular graphs. *Graphs and Combinatorics*, 18(1):53–57, 2002. [2.17](#)
- [AL13] Noga Alon and Shachar Lovett. Almost k -wise vs. k -wise independent permutations, and uniformity for general group actions. *Theory of Computing*, 9:559–577, 2013. [2.1](#), [2.5](#), [2.6](#)
- [Alo86] Noga Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986. [1.1](#), [1.1](#), [1.5](#), [1.2](#)

- [Bas92] Hyman Bass. The Ihara–Selberg zeta function of a tree lattice. *International Journal of Mathematics*, 3(6):717–797, 1992. 2.3
- [BC78] Edward Bender and Rodney Canfield. The asymptotic number of labeled graphs with given degree sequences. *Journal of Combinatorial Theory. Series A*, 24(3):296–307, 1978. 2.2.1, A
- [BK67] Jānis Bārzdiņš and Andrey Kolmogorov. On the realization of networks in three-dimensional space. *Problemy Kibernetiki*, 19:261–268, 1967. 1.1
- [BL06] Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap. *Combinatorica*, 26(5):495–519, 2006. 1, 1.2, 1.10, 1, 1.2, 1.2, 1.3, 1.4
- [Bol80] Béla Bollobás. A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. *European Journal of Combinatorics*, 1(4):311–316, 1980. 2.2.1, A, A
- [Bol01] Béla Bollobás. *Random Graphs*. Cambridge University Press, second edition edition, 2001. 2.2.1
- [Bor16] Charles Bordenave. Lecture notes on random graphs and probabilistic combinatorial optimization. Retrieved from <https://www.math.univ-toulouse.fr/~bordenave/coursRG.pdf>, 2016. 4.1
- [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*. 1.2, 1.8, 1.3, 2.2.1, 2.11, 2.3, 2.3, 3, 3, 4, 4.1, 4.2, 4.4, 4.2, 4.2, 4
- [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. 1.9, 1
- [Chi92] Patrick Chiu. Cubic Ramanujan graphs. *Combinatorica*, 12(3):275–285, 1992. 1.2, 1
- [Cla06] Pete Clark. Ramanujan graphs and Shimura curves. Retrieved from <http://alpha.math.uga.edu/~pete/ramanujanrevisited.pdf>, 2006. 1.2, 1
- [CM08] Sebastian M. Cioabă and M. Ram Murty. Expander graphs and gaps between primes. *Forum Mathematicum*, 20(4):745–756, 2008. 1.2, 1.11, 1.2, 1
- [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. 1.2, 1.12, 1
- [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. 1.2, 1
- [DMO⁺19] Yash Deshpande, Andrea Montanari, Ryan O’Donnell, Tselil Schramm, and Subhabrata Sen. The threshold for SDP-refutation of random regular NAE-3SAT. In *Proceedings of the 30th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2305–2321, 2019. 1.3

- [Fri93] Joel Friedman. Some geometric aspects of graphs and their eigenfunctions. *Duke Mathematical Journal*, 69(3):487–525, 1993. 1.5
- [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. 1.2, 1.8, 2.3, 3
- [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. 1.2
- [Hås84] Johan Håstad. An NP-complete problem – some aspects of its solution and some possible applications. Master’s thesis, Uppsala University, 1984. 1.3
- [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 *Advanced Studies in Pure Mathematics*, pages 211–280. Elsevier, 1989. 2.19, 2.3
- [HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *American Mathematical Society Bulletin*, 43(4):439–561, 2006. 1.1, 1.2
- [Iha66] Yasutaka Ihara. On discrete subgroups of the two by two projective linear group over p -adic fields. *Journal of the Mathematical Society of Japan*, 18:219–235, 1966. 1.2, 1, 2.3
- [JŁR00] Svante Janson, Tomasz Łuczak, and Andrzej Ruciński. *Random graphs*. John Wiley & Sons, 2000. 4.1, 4.2
- [Kas07] Martin Kassabov. Symmetric groups and expander graphs. *Inventiones Mathematicae*, 170(2):327–354, 2007. 2.1, 2.4, 2.6
- [KNR09] Eyal Kaplan, Moni Naor, and Omer Reingold. Derandomized constructions of k -wise (almost) independent permutations. *Algorithmica. An International Journal in Computer Science*, 55(1):113–133, 2009. 2.1, 2.4, 2.6
- [LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261—277, 1988. 1.2, 1.2, 1
- [LS10] Eyal Lubetzky and Allan Sly. Cutoff phenomena for random walks on random regular graphs. *Duke Mathematical Journal*, 153(3):475–510, 2010. 4.1
- [Mar73a] Grigory Margulis. Complexity of an optimum nonblocking switching network without reconstructions. *Problemy Peredachi Informatsii*, 9(1):84–87, 1973. 1.1
- [Mar73b] Grigory Margulis. Explicit construction of concentrators. *Problemy Peredachi Informatsii*, 9(4):71–80, 1973. 1.2
- [Mar88] Grigory 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. 1.2, 1
- [MOP19] Sidhanth Mohanty, Ryan O’Donnell, and Pedro Paredes. The SDP value for random two-eigenvalue CSPs. Technical Report 1906.06732, arXiv, 2019. 1.3, 3

- [Mor94] Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q . *Journal of Combinatorial Theory. Series B*, 62(1):44–62, 1994. [1.2](#), [1.7](#), [1](#)
- [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. [1.2](#), [1.12](#), [1](#)
- [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. [1.2](#), [1.12](#), [1](#)
- [Nil91] A. Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991. [1.5](#)
- [NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, 1993. [2.1](#), [2.2](#)
- [Pin73] Mark Pinsker. On the complexity of a concentrator. In *Proceedings of the 7th International Teletraffic Congress*, pages 318/1–318/4, 1973. [1.1](#)
- [Piz90] Arnold Pizer. Ramanujan graphs and Hecke operators. *American Mathematical Society. Bulletin. New Series*, 23(1):127–137, 1990. [1.2](#), [1](#)
- [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. [1.2](#), [1.9](#), [1](#)
- [Ser77] Jean-Pierre Serre. *Arbres, amalgames, SL_2* . Société Mathématique de France, Paris, 1977. Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46. [2.3](#)
- [Sho90] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990. [2.1](#)
- [WF09] Yusuke Watanabe and Kenji Fukumizu. Graph zeta function in the Bethe free energy and loopy belief propagation. In *Proceedings of the 23rd Annual Conference on Neural Information Processing Systems*, pages 2017–2025, 2009. [2.3](#), [2.21](#)
- [Wor99] Nicholas Wormald. Models of random regular graphs. In *Surveys in combinatorics, 1999 (Canterbury)*, volume 267 of *London Mathematical Society Lecture Note Series*, pages 239–298. Cambridge Univ. Press, Cambridge, 1999. [4.1](#)

A Simplicity

In the fully uniform configuration model, the probability of G being simple (i.e., being an ordinary graph with no self-loops or parallel edges) is known [[BC78](#), [Bol80](#)] to tend to the constant $\exp(-(d^2 - 1)/4)$, as $n \rightarrow \infty$. We establish that the $O(d^2)$ -wise uniform configuration model suffices for this:

Proposition A.1. Let $3 \leq d \ll \sqrt{\log n}$ and let $k \geq Cd^2$, where C is a certain universal constant. Let G be drawn from the d -regular n -vertex configuration model using a k -wise uniform permutation. Then

$$\Pr[G \text{ is simple}] = e^{-(d^2-1)/4} (1 \pm e^{-100d^2}).$$

By [Theorem 2.5](#), this remains true if the permutation is merely (δ, k) -wise uniform, $\delta \leq n^{-C'd^2}$.

The proof is a straightforward derandomization of Bollobás's original analysis of simplicity in the configuration model [\[Bol80\]](#). Unlike several later refinements that used the Chen–Stein method, Bollobás's proof uses the method of moments, making it particularly convenient to derandomize using k -wise uniform permutations.

Proof of [Proposition A.1](#). Let us recap Bollobás's proof concerning an n -vertex d -regular configuration model graph G formed from a truly random permutation $\pi \sim S_{nd}$. He defines X_1 to be the number of self-loops in G (i.e., $\frac{1}{2} \text{tr}(A)$), X_2 to be the number of 2-cycles (i.e., $\sum_{v < v'} \binom{A_{v,v'}}{2}$), and $X = X_1 + X_2$. Note that G is simple if and only if $X = 0$. The idea of the proof is that it is nearly the case that X_1, X_2 are independent Poisson random variables with respective means

$$\lambda_1 = \lambda \cdot \frac{nd}{nd-1} = \lambda \cdot (1 \pm O(1/n)), \quad \lambda_2 = \lambda^2 \cdot \frac{nd \cdot (nd-d)}{(nd-1) \cdot (nd-3)} = \lambda^2 \cdot (1 \pm O(1/n)),$$

where $\lambda := (d-1)/2$. Thus X should be nearly Poisson with mean $\lambda_1 + \lambda_2 \sim \lambda + \lambda^2 = (d^2-1)/4$, and hence we should have $\Pr[X=0] \sim e^{-(d^2-1)/4}$.

More precisely, Bollobás first establishes [\[Bol80, ineq. \(11\)\]](#) the following estimate for all integers $0 \leq r \leq 8 \log n$:

$$E_r := \mathbb{E} \left[\binom{X}{r} \right] \text{ satisfies } \left| E_r - \frac{(\lambda_1 + \lambda_2)^r}{r!} \right| \leq \frac{(\lambda_1 + \lambda_2)^r}{r!} \cdot O(r^2/n). \quad (7)$$

(Actually, Bollobás has $O((\log n)^2/n)$ on the right-hand side rather than $O(r^2/n)$, but inspection of his proof confirms the above.) The key point for our proof of [Proposition A.1](#) is that [Inequality \(7\)](#) continues to hold when the permutation $\pi \in S_{nd}$ defining G is merely $4r$ -wise uniform. This is simply because $\binom{X}{r}$ is a polynomial of degree at most $4r$ in the indicators $1[\pi(j) = (v, i)]$. Thus to complete the proof, it suffices to derive the conclusion

$$\Pr[X=0] = e^{-(d^2-1)/4} (1 \pm e^{-100d^2}) \quad (8)$$

from the estimates in [Inequality \(7\)](#) with $r = O(d^2)$. This can be done exactly as in Bollobás's work. He uses the following inclusion-exclusion-type inequality, which holds (for any $u \in \mathbb{N}$) due to X being \mathbb{N} -valued:

$$\sum_{r=0}^{2u+1} (-1)^r E_r \leq \Pr[X=0] \leq \sum_{r=0}^{2u} (-1)^r E_r. \quad (9)$$

Notice that $E_r \approx \frac{(\lambda_1 + \lambda_2)^r}{r!}$, and

$$\sum_{r=0}^{\infty} (-1)^r \frac{(\lambda_1 + \lambda_2)^r}{r!} = e^{-(\lambda_1 + \lambda_2)} = e^{-(\lambda + \lambda^2) \cdot (1 \pm O(1/n))} = e^{-(d^2-1)/4} \cdot (1 \pm O(d^2/n)); \quad (10)$$

also, $O(d^2/n) \ll e^{-100d^2}$ since $d \ll \sqrt{\log n}$. Thus we can establish [Equation \(8\)](#) by bounding the two errors distinguishing the infinite sum in [Equation \(10\)](#) from the sums on the left- and right-hand side of [Inequality \(9\)](#). The two distinctions are: the error in $E_r \approx \frac{(\lambda_1 + \lambda_2)^r}{r!}$, boundable using

Inequality (7); and, the tail of the infinite sum from $2u$ or $2u + 1$ onward. In absolute value, these two errors are boundable by:

$$O(1/n) \cdot \sum_{r=0}^{2u \text{ or } 2u+1} \frac{(\lambda_1 + \lambda_2)^r}{r!} \cdot r^2, \quad \text{and} \quad \sum_{r=2u+1 \text{ or } 2u+2}^{\infty} \frac{(\lambda_1 + \lambda_2)^r}{r!}.$$

The first quantity above can be bounded by $O(u^2/n) \cdot e^{\lambda_1 + \lambda_2}$, and the second quantity can be bounded by $O((\lambda_1 + \lambda_2)^{2u+1}/(2u+1)!)$ provided $u \geq \lambda_1 + \lambda_2$. Recalling $\lambda_1 + \lambda_2 = \Theta(d^2)$ and $d \ll \sqrt{\log n}$, we see that by taking $u = O(d^2)$ sufficiently large, both errors can be made much smaller than e^{-100d^2} , and we obtain **Equation (8)** with $r = O(d^2)$ as needed. \square

B The probabilistically poly log n -time computable construction

We now walk through the steps of **Section 5** giving precise parameter details along the way, and extract a probabilistically poly log n -time computable construction of near-Ramanujan graphs.

Assume we are given N , $3 \leq d \leq \frac{(\log N)^{1/8}}{C}$ and $\epsilon \gg \frac{(\log \log N)^4}{\log N} \cdot \sqrt{d}$ where C is the constant from the statement of **Theorem 4.8**.

Revisiting Step 1. Choose parameters as follows: $\alpha = 1/\sqrt{\binom{d+1}{2}}$; n_0 as the largest multiple of $d+1$ smaller than $2^{\alpha\sqrt{\log N}}$; $k = C\alpha\sqrt{\log N} \cdot d^{1/4}/\sqrt{\epsilon}$ (which is $\approx \log n_0$); and $\delta = 1/N^{8k+1}$. Recall that the key result used in this step is that by **Theorem 4.8**, G_0 drawn from the n_0 -vertex (δ, k) -wise random-lift-of- K_{d+1} model is a simple graph that with high probability satisfies:

$$G_0 \text{ is bicycle-free at radius } \Omega\left(\frac{\alpha\sqrt{\log N}}{\log(d-1)}\right); \quad \lambda(G_0) \leq 2\sqrt{d-1} + \epsilon. \quad (11)$$

As an upshot of **Theorem 2.4**, G_0 can be sampled using s , a uniform binary string of length $O\left(\frac{\log N \cdot d^{1/4}}{\sqrt{\epsilon}}\right)$ as a seed. In particular, s is divided into $\binom{d+1}{2}$ disjoint substrings $s_{e_1}, \dots, s_{e_{\binom{d+1}{2}}}$ each of length $\ell_1 = O\left(\frac{\alpha^2 \log N \cdot d^{1/4}}{\sqrt{\epsilon}}\right)$ indexed by edges of K_{d+1} ; the (δ, k) -wise uniform permutation π_{uv} corresponding to edge (u, v) is taken to be the s_{uv} th permutation in the multiset of permutations Π from the statement of **Theorem 2.4**. Additionally, given s and a vertex $(u, i) \in V(G_0)$, it is possible to return a list of its neighbors in time $T_1 = O\left(d \cdot \text{poly}\left(\frac{\alpha^2 \log N \cdot d^{1/4}}{\sqrt{\epsilon}}\right)\right)$.

Revisiting Step 2. Let $t = \left\lceil \log\left(\frac{N}{n_0}\right) \right\rceil$; let β be a large enough constant; let $k = \frac{2\beta d^{1/4}}{\sqrt{\epsilon}} \log N$; and let $\delta = N^{-O(\beta d^{1/4} \log d / \sqrt{\epsilon})}$. The main result used in Step 2 is that from **Theorem 3.1** the graphs G_1, \dots, G_t where G_i is obtained via a 2-lift of G_{i-1} induced by a (δ, k) -wise uniform signing have their nontrivial eigenvalues bounded by $2\sqrt{d-1} + \epsilon$ in magnitude, except with probability $O(t/n_0^{100})$. From **Theorem 2.2**, a (δ, k) -wise uniform signing of any G_i can be obtained by first sampling a random binary string s' of length $\ell_2 = O\left(\frac{d^{1/4} \log d \cdot \log N}{\sqrt{\epsilon}}\right)$ and choosing the s th string in the multiset of signings Y from the theorem statement. In fact, given s' and edge $e \in G_i$ one can also output the sign assigned to edge e in time $T_2 = \text{poly}(\beta d^{1/4} \log d \log N / \sqrt{\epsilon})$. Finally, by the union bound, the bound of $O(t/n_0^{100})$ on the probability that G_t is not ϵ -near Ramanujan holds if we use independently chosen seeds s_1, \dots, s_t to perform the 2-lifts. Note that $t < \log N$ and $n_0 \geq 2^{(\log N)^{1/4}}$ and hence the failure probability is $o_N(1)$.

Probabilistically strongly explicit near-Ramanujan graphs. Given a uniform binary string s of length $\ell_1 + t \cdot \ell_2$ as a random seed, call the substring given by the first ℓ_1 bits s_1 and the substring given by the next $t \cdot \ell_2$ bits s_2 . Let G_0 be sampled from s_1 as described in Step 1, and let G_t be the “final graph” obtained by the sequence of 2-lifts in Step 2 from s_2 . Each vertex in G_i can be naturally identified with a tuple $(v, a, x) \in [d] \times [n_0] \times \{0, 1\}^i$. Let x be a string in $\{0, 1\}^t$, let $x^{\leq i}$ denote its i -bit prefix. Given a vertex (v, a, x) in G_t and seeds s_1 and s_2 , we describe an algorithm to output a list of its d neighbors in $\tilde{O}(T_1 + dT_2)$ -time where the $\tilde{O}(\cdot)$ hides factors of $\text{polylog } N$. From Step 1, we know that there is an T_1 -time algorithm to output a list of d neighbors of $(v, a, x^{\leq 0})$ in G_0 .

Next, given a list of neighbors of $(v, a, x^{\leq i-1})$ in G_{i-1} it is possible to output a list of neighbors of $(v, a, x^{\leq i})$ in G_i in $\tilde{O}(dT_2)$ -time in the following way. Let (w, b, y) be a neighbor of $(v, a, x^{\leq i-1})$. Then exactly one of $(w, b, y \wedge 0)$ and $(w, b, y \wedge 1)$ is a neighbor of $(v, a, x^{\leq i})$ where \wedge denotes concatenation. It is possible to obtain the sign on edge $\{(v, a, x^{\leq i-1}), (w, b, y)\}$ in the 2-lift from G_{i-1} to G_i in T_2 time from s_2 . If the sign is a -1 , then $(w, b, y \wedge (1 - x_i))$ is a neighbor of $(v, a, x^{\leq i})$; otherwise $(w, b, y \wedge x_i)$ is a neighbor. Thus, in $\tilde{O}(dT_2)$ time, we can obtain a length- d (and hence complete) list of neighbors of $(v, a, x^{\leq i})$.

As a result, after spending T_1 time generating a list of neighbors of $(v, a, x^{\leq 0})$, we can use the above routine t times to obtain a list of neighbors of (v, a, x) in G_t in $T_1 + t \cdot \tilde{O}(dT_2) \leq \tilde{O}(T_1 + dT_2)$. From the upper and lower bounds on d and ϵ , this quantity is always $O(\text{polylog } N)$.

To summarize, we have an algorithm that takes in a random seed of length $O\left(\frac{d^{1/4} \log d \cdot \log^2 N}{\sqrt{\epsilon}}\right)$ and implements the adjacency matrix of a corresponding random graph G such that:

- Given any vertex v of G , its list of neighbors can be generated in $O(\text{polylog } N)$ time.
- G is ϵ -near Ramanujan with probability $1 - o_N(1)$.

This yields the conclusion of [Theorem 1.13](#).