Electronic Colloquium on Computational Complexity, Report No. 183 (2023)

# Derandomized Squaring: An Analytical Insight into Its True Behavior

Gil Cohen* Itay Cohen† Gal Maor‡ Yuval Peled§

November 24, 2023

**Abstract**

The notion of the derandomized square of two graphs, denoted as $G \circledS H$, was introduced by Rozenman and Vadhan as they rederived Reingold's Theorem, $\mathbf{SL} = \mathbf{L}$. This pseudorandom primitive, closely related to the Zig-Zag product, plays a crucial role in recent advancements on space-bounded derandomization. For this and other reasons, understanding the spectral expansion $\lambda(G \circledS H)$ becomes paramount. Rozenman and Vadhan derived an upper bound for $\lambda(G \circledS H)$ in terms of the spectral expansions of the individual graphs, $\lambda(G)$ and $\lambda(H)$. They also proved their bound is optimal if the only information incorporated to the bound is the spectral expansion of the two graphs.

The objective of this work is to gain deeper insights into the behavior of derandomized squaring by taking into account the *entire spectrum* of $H$, where we focus on a vertex-transitive $H$. Utilizing deep results from analytic combinatorics, we establish a lower bound on $\lambda(G \circledS H)$ that applies universally to all graphs $G$. Our work reveals that the key information regarding the bound lies within the largest real solution to the polynomial equation

$$(d-1)\chi_x(H)\chi_x''(H) = (d-2)\chi_x'(H)^2,$$

where $\chi_x(H)$ is the characteristic polynomial of the $d$-vertex graph $H$. Empirical evidence suggests that our lower bound is essentially optimal for every graph $H$ and for a typical graph $G$. We support the tightness of our lower bound by showing that the bound is tight for a class of graphs which exhibit local behavior similar to a derandomized squaring operation with $H$. To this end, we make use of finite free probability theory.

In our second result, we establish a lower bound for the spectral expansion of rotating expanders. These graphs, introduced by Cohen and Maor (STOC 2023), are constructed by taking a random walk with vertex permutations occurring after each step. We prove that Cohen and Maor's construction is essentially optimal. Unlike our results on derandomized squaring, the proof in this instance relies solely on combinatorial methods. The key insight lies in establishing a connection between random walks on graph products and the Fuss-Catalan numbers.

*Tel Aviv University. gil@tauex.tau.ac.il. Supported by ERC starting grant 949499 and by the Israel Science Foundation grant 1569/18.

†Tel Aviv University. itay3@mail.tau.ac.il. Supported by ERC starting grant 949499.

‡Tel Aviv University. galmaor@mail.tau.ac.il. Supported by ERC starting grant 949499.

§The Hebrew University. yuval.peled@mail.huji.ac.il.

ISSN 1433-8092

# Contents

# 1 Introduction

Expander graphs have played a crucial role in essentially all areas within theoretical computer science as well as in coding theory, and cryptography, among others. Their utility stems to a large extent from the ability to interpret expansion from various perspectives, be it combinatorial, probabilistic, or linear algebraic. This multifaceted understanding offers a unique advantage: it enables the otherwise challenging inference of combinatorial attributes of graphs by examining the spectral properties of related operators.

We briefly recall the notion of *spectral expansion*. Let $G$ be an undirected $d$-regular graph on $n$ vertices with adjacency matrix $\mathbf{A}$. Since $G$ is undirected, $\mathbf{A}$ is symmetric and so its spectrum is real-valued. We denote the eigenvalues of $\mathbf{A}$ by $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. The spectral expansion of $G$, denoted as $\lambda(G)$, is given by $\max(\lambda_2, |\lambda_n|)$. We further denote the normalized spectral expansion of $G$ by $\omega(G) = \frac{\lambda(G)}{d} \in [0,1]$. We alternate between the two variants–the normalized and the unnormalized–depending on context.

An *expander* is a graph $G$ with a normalized spectral expansion $\omega(G)$ that is bounded away from 1 [1]. However, for a typical application of expander graphs one "pays" a cost that increases with the degree $d$ and has an "error" that vanishes as $\omega(G) \to 0$. This raises the question of what is the lowest possible value of $\omega(G)$ attainable by $d$-regular graphs. From the Alon-Boppana bound [Nil91], which is usually stated in terms of $\lambda(G)$, it follows that for every $\varepsilon > 0$ there are only finitely many $d$-regular graphs $G$ with $\lambda(G) \leq 2\sqrt{d-1} - \varepsilon$. A $d$-regular graph $G$ satisfying $\lambda(G) \leq 2\sqrt{d-1}$ is called a *Ramanujan graph*. Over the past several decades, Ramanujan graphs have been a focal point of research. The constructions of Ramanujan graphs and their variants lean on profound number theoretic results [LPS88, Mar88, Mor94] (see also [Iha66]), or is rooted in deep analytical methods and on the accompanied technique of polynomial interlacing [MSS15a, MSS22, MSS18, Coh16, HPS18].

In their highly influential paper [RVW00], Reingold, Vadhan, and Wigderson introduced the Zig-Zag product which enabled them to obtain a combinatorial construction of expander graphs by elementary means. While the expanders that were constructed were not quite close to Ramanujan, the fact that the construction is combinatorial and highly flexible made the Zig-Zag product extremely useful. Indeed, no long after, Reingold [Rei08] based his breakthrough result, $\mathbf{SL} = \mathbf{L}$, on the Zig-Zag product, not for constructing expanders per se but for the purpose of "transforming" a given graph to an expander while maintaining its connected components structure. In a subsequent work, Ben-Aroya and Ta-Shma [BATS11] put forth an improved variant of the Zig-Zag product, dubbed the *wide-replacement product*, that enabled the combinatorial construction of graphs that come quite close to Ramanujan. That variant was key in a recent breakthrough by Ta-Shma who constructed near-optimal small-bias sets [TS17]. Several other expander construction paradigms have been put forth in the literature, e.g., [BL06, MOP22]. We refer the reader to the excellent survey by Hoory, Linial, and Wigderson [HLW06] for a comprehensive exposition on expander graphs.

[1] To be more precise, it is common to consider a family of graphs in this context. However, we will exclude this technical detail from our discussion for simplicity.

### 1.1 Derandomized squaring

Not long after the work of Reingold [Rei08], Rozenman and Vadhan [RV05] introduced a close sibling to the Zig-Zag product, dubbed *derandomized squaring*, which we describe soon. This operation can be "cleaner" than the Zig-Zag product in some settings, in particular for their rederivation of Reingold's result, though the two operations are tightly connected. In the past few years, derandomized squaring has gained significant traction in the space-bounded derandomization literature (see, e.g., [MRSV21, AKM+20, APP+23, CHL+23]) mostly since it facilitated the adaptation of ideas from the realm of fast Laplacian solvers into the domain of space-bounded derandomization. For these reasons, in this paper we focus on the operation of derandomized squaring though we are confident that our techniques can be extended to other operations such as the Zig-Zag product and the wide-replacement product.

Squaring a graph is an easy way of improving its normalized spectral expansion. The square of a graph $G$, denoted as $G^2$, is the graph on the same vertex set that has an edge between a pair of vertices for every length-2 path in $G$ between the vertices. Clearly, if $\mathbf{A}$ is the adjacency matrix of $G$ then $\mathbf{A}^2$ is the adjacency matrix of $G^2$. Hence, $\omega(G^2) = \omega(G)^2$. However, if $G$ is $d$-regular, $G^2$ is a $d^2$-regular graph. As a result, the degree growth associated with squaring the graph often surpasses the advantages gained from reducing the normalized spectral expansion. The purpose of derandomized squaring is to obtain a comparable improvement to the normalized spectral expansion without blowing up the degree by a quadratic factor.

From the view point of a vertex $v$ of $G$, in the graph $G^2$, the neighbors of $v$ are all connected to each other. That is, $G^2$ is obtained by adding copies of the complete graph with self-loops, one copy for each vertex $v$, where the complete graph associated with $v$ is placed on the neighbors of $v$. Let $H$ be a graph on $d$ vertices, where we focus on the case in which $H$ is vertex-transitive, and denote the degree of a vertex in $H$ by $c$. The derandomized square of $G$ and $H$, denoted as $G \circledS H$, is defined by replacing each such copy of the complete graph with a copy of $H$. Note that $G \circledS H$ is a $D$-regular graph where $D = dc$. Formally, the derandomized squaring, like the Zig-Zag product, requires working with edge-labeled graphs, but we sidestep this technicality (see Section 4.1). For the reader that is familiar with these intricacies, we remark that, for simplicity, in this extended abstract we circumvent labeling issues by assuming that $G$ is given as the union of $d$ perfect matchings, though this condition can be relaxed.

Given that an expander $H$ approximates the complete graph, one is correct to expect that the derandomized square $G \circledS H$ approximates $G^2$ for every graph $G$. Rozenman and Vadhan formalized this intuition with regards to the normalized spectral expansion by establishing the bound

$$\omega(G \circledS H) \le (1 - \omega(H))\,\omega(G)^2 + \omega(H) \le \omega(G)^2 + \omega(H). \tag{1.1}$$

How tight is this bound? This is a somewhat subtle question. Rozenman and Vadhan proved that the bound is tight *as a function of* $\omega(G)$ and $\omega(H)$, however, it is certainly conceivable that a superior bound might be achieved if one incorporates more information about the graphs beyond just their spectral expansions into the bound. In particular, if we fix $H$ and consider the mapping $\lambda(\cdot \circledS H)$ which maps every $d$-regular graph $G$ to $\lambda(G \circledS H)$, then it is interesting to ask how strong a bound can be obtained on this mapping as a function of the entire spectrum of $H$.

Given the significance of the derandomized squaring operation, and the related Zig Zag product as well as the wide-replacement product, a substantial improvement to the bound could profoundly impact our understanding on several fundamental problems, including in space-bounded derandomization and in coding theory. For example, in the context of space-bounded derandomization such a result may reduce the seed length of PRGs or weighted PRGs (see [BCG19, CL20, CHL$^+$23] and references therein). Such a result may also lead to a better construction of small-bias sets in which the wide-replacement product is used for bias-reduction. Therefore, gaining a thorough understanding of derandomized squaring is highly motivated from the theoretical computer science standpoint.

### 1.2 Two case studies

Before presenting our results, which we view as a first step towards the above goal, we wish to highlight the gap between the Rozenman-Vadhan bound, as given in Equation (1.1), and the "true" behavior of the derandomized squaring operation. We do so by considering two case studies, starting with $H = \mathrm{K}_{c,c}$, the complete $c = \frac{d}{2}$-regular bipartite graph on $d$ vertices.

#### 1.2.1 Derandomized squaring with the complete regular bipartite graph

Since $H = \mathrm{K}_{c,c}$ is bipartite, $\omega(H) = 1$, and so the bound given by Equation (1.1) becomes trivial, $\omega(G \circledS H) \leq 1$ for all $d$-regular graphs $G$. For this special case, one can get a nontrivial bound by elementary means by incorporating some information on $G$. To see this, assume that $G$ is the union of two $c$-regular Ramanujan graphs on $n$ vertices, whose adjacency matrices are denoted $\mathbf{B}$ and $\mathbf{R}$, respectively. That is, the adjacency matrix of $G$ is given by $\mathbf{A} = \mathbf{B} + \mathbf{R}$. Thus, it can be shown that the adjacency matrix of $G \circledS H$ can be expressed as $\mathbf{RB} + \mathbf{BR}$ [2], and so by the Courant-Fischer Theorem,

$$\lambda(G \circledS H) = 2 \cdot \max_{x \perp \mathbf{1}} \frac{x^{\mathsf{T}}\mathbf{BR}x}{x^{\mathsf{T}}x} \leq 2\left(2\sqrt{\frac{d}{2} - 1}\right)^2 \leq \sqrt{32}\sqrt{D-1} \approx 5.66\sqrt{D-1},$$

where $D = \frac{d^2}{2}$ is the regularity of $G \circledS H$.

Although the above bound on $\lambda(G \circledS H)$ certainly beats the trivial bound, $D$, it still seems to undersell the typical behavior of $G \circledS H$. In fact, by sampling [3] a random $d$-regular graph $G$ and evaluating $\lambda(G \circledS H)$, one can verify that for a sufficiently large $d$, the value of $\lambda(G \circledS H)$ distributes around $2.35\sqrt{D-1}$. But where does the 2.35 value originate? How can this number be determined based on our selected $H$? Jumping the gun, the analytical tool we introduce *predicts* that the exact value, for this $H$, is

$$\frac{1}{2}\sqrt{11 + 5\sqrt{5}} \approx 2.35. \tag{1.2}$$

[2] With regards to the edge labeling, for the last statement to hold we assume that neighbors $1, \ldots, \frac{d}{2}$ of every vertex are those coming from $\mathbf{B}$ and the remaining neighbors $\frac{d}{2} + 1, \ldots, d$ are coming from $\mathbf{R}$.

[3] Our sampling is done by taking the union of $d$ uniformly random and independent perfect matchings, where edges that are sampled multiple times are counted with the respective multiplicity.

By saying that we "predict" this bound captures the true behavior of derandomized squaring with $H = \mathrm{K}_{c,c}$, we mean the following: First, we prove the aforementioned value to be a lower bound on $\lambda(G \circledS H)$ for *every* $d$-regular graph $G$; Second, we prove the existence of infinitely many graphs that meet this bound. These graphs exhibit a local structure resembling a derandomized square with $H$. Lastly, our predictions align with every experiment we made for every graph $H$ and when $G$ is sampled uniformly at random. We provide further details in Section 2, where our results are formally presented.

#### 1.2.2 Derandomized squaring with a Paley graph

In the aforementioned example, the Rozenman-Vadhan bound was non-informative. It is worth noting that it is not just in these instances where the typical performance of the derandomized square surpasses the predictions of the bound. To give one such example, consider a Paley graph on $d$ vertices, denoted as $\mathrm{Pal}_d$. For a typical $d$-regular graph $G$, the limit behavior as $d \to \infty$ of the spectral expansion $\lambda(G \circledS \mathrm{Pal}_d)$, when properly normalized, is predicted by our analytic tool to equal

$$\lim_{d\to\infty} \frac{\lambda(G \circledS \mathrm{Pal}_d)}{\sqrt{D-1}} = \frac{1+\sqrt{13+16\sqrt{2}}}{\sqrt{8}} \approx 2.46, \tag{1.3}$$

where $D = \frac{d(d-1)}{2}$ is the degree $G \circledS \mathrm{Pal}_d$. This should be compared with a bound of 2, the least possible value given the Alon-Boppana bound. Additionally, it should be compared with Equation (1.1), which, irrespective of the choice of $G$, cannot produce a bound lower than $O(D^{1/4})$.

From the preceding discussion and, in particular, the two case studies, a key question lingers: Is there an exact formula or efficient method that enables us to compute, and more importantly, to gain insight on the spectral expansion of the operation of derandomized squaring with $H$?

## 2 Our Results

As our case studies suggest, the spectral expansion of the graphs $G$ and $H$ might not adequately represent the spectral expansion of their derandomized square. In this paper we initiate the study of the following question:

**Main Question.** What is the "true" behavior of the spectral expansion of derandomized squaring?

We turn to give a brief summary of our results. We elaborate further on each of these results in the subsequent sections, Sections 2.1 to 2.3.

**Limitations of derandomized squaring.** Our first result is a lower bound on $\lambda(G \circledS H)$, factoring in the full spectrum of $H$, which holds for *every* graph $G$. If we encode this spectrum by the characteristic polynomial of $H$, denoted as $\chi_x(H)$, then our work reveals that the key information regarding the bound lies within the largest real solution to the polynomial equation

$$(d-1)\chi_x(H)\chi_x''(H) = (d-2)\chi_x'(H)^2.$$

Our proof leans on deep results from analytic combinatorics and the symbolic method.

**Evidence for the tightness of our lower bound.** Based on our empirical experiments, it appears that our lower bound is tight in a strong sense, namely, for *every* vertex-transitive graph $H$ and for a *typical* graph $G$. However, a definitive proof of the bound's tightness eludes us in general. In spite of this, we have made notable progress by establishing its tightness for a class of graphs, we term $H$-local graphs. This class captures the local structure of graphs obtained by derandomized squaring with $H$, and include all graphs of the form $G \circledS H$. For obtaining this result we make use of finite free probability theory and the accompanied technique of interlacing. These were instrumental in the seminal works of Marcus, Spielman, and Srivastava [MSS15b, MSS18, MSS22] who introduced these techniques for their study of bipartite Ramanujan graphs. We elaborate on this in Section 2.2. It is also worth noting that for some choices of $H$, we are able to prove that our bound is tight.

**A lower bound for rotating expanders.** In the process of establishing our lower bound on the spectral expansion of derandomized squaring, we address an open problem concerning the spectral expansion of *rotating expanders* [CM23]. In this recent paper, random walks on expanders were studied, wherein a permutation is applied to the vertices following each step. The objective of this approach is to mitigate the inherent exponential deterioration of the spectral expansion with respect to the length of the walk. Indeed, the authors proved that by using a carefully chosen permutation sequence, the deterioration can be reduced from exponential to linear. The authors left open the question of whether their construction is optimal.

In this work, we resolve this question by proving the optimality of their construction. More generally, we prove that a graph which is constructed as a graph product is inherently far from Ramanujan. Our key observation lies in relating the problem with the Fuss-Catalan numbers which generalize the Catalan numbers that emerge when bounding the spectral expansion of $d$-regular graphs. We elaborate on this in Section 2.3, where we also give the necessary background on rotating expanders.

**A broader perspective: beyond spectral expansion.** Almost all of the numerous works and applications of spectral expanders in theoretical computer science, indeed, the very definition of a spectral expander $G$, rely on the notion of the spectral expansion, $\lambda(G)$. Only a few instances utilize the entire spectrum of $G$, which holds significantly more, and sometimes vital, information about the graph. In their seminal series of works, Marcus, Spielman, and Srivastava developed finite free probability as a framework to handle the full spectrum of a graph. As mentioned, this enabled them to establish the existence of bipartite Ramanujan graphs of all sizes and degrees.

Our current work serves as a further exploration into analyzing graphs beyond their spectral expansion. Instead of aiming to construct expanders, our objective is to achieve a deeper insight into the derandomized squaring operation. While we primarily target the spectral expansion of the derandomized square $G \circledS H$, our approach involves leveraging the entire spectrum of $H$ for establishing our bounds. In addition to our use of finite free probability, we employ deep results from analytic combinatorics, and the framework offered by the symbolic method. We posit that working with the full spectrum of a graph could yield significant results and improvements for various problems in theoretical computer science, and we believe that the deep results we use could be advantageous in other scenarios where analyzing the full spectrum is desired.

**Related work.** Already at this point, prior to delving into the formal details concerning our results, we would like to briefly highlight some related work. Our study of the graph $G \circledS H$ for a $d$-regular graph $G$ is done by considering the graph $\mathcal{T}_d \circledS H$, where $\mathcal{T}_d$ is the $d$-ary infinite tree. The study of graphs, which represent the quotient of a given (typically infinite) graph $X$, has a long history. Of particular interest are the extreme graphs, known as *$X$-Ramanujan graphs*. The reader is referred to [MO20, OW20] and references therein for more details. Our result supporting the tightness of our lower bound mentioned above can also be derived from [MO20]. However, we believe our proof to be simpler and more direct. We discuss this further after presenting the relevant result in Section 2.2.

Regarding our lower bound result, the calculation of the spectral radius of operators associated with infinite graphs has been extensively explored. This is particularly true when these graphs exhibit a well-defined group-theoretic structure. Analytic combinatorics has a well-established presence in this context [Woe00]. Finally, it is noteworthy that the Fuss-Catalan numbers are significant in free probability theory and have known associations with the product of certain random matrices [PŻ11].

### 2.1 Limitations of derandomized squaring

Let $H$ be a vertex-transitive graph on $d$ vertices. Recall that, throughout, $c$ denotes the degree of a vertex in $H$. In this section we state our result regarding the lower bound on $\lambda(G \circledS H)$ which holds for every $d$-regular graph $G$. As previously suggested, our approach integrates the complete spectrum of $H$ into the bound. This integration is accomplished by encoding the spectrum through the characteristic polynomial of $H$-s adjacency matrix, denoted as $\chi_x(H) = \prod_{i=1}^{d} x - \lambda_i$, where, as before, $c = \lambda_1 \geq \cdots \geq \lambda_d$ are the corresponding eigenvalues.

**Theorem 2.1.** *Let $H$ be a vertex-transitive $c$-regular graph on $d \geq 3$ vertices, where $c \geq 1$. Let $x_0$ be the largest real solution to the polynomial equation*

$$(d-1)\chi_x(H)\chi_x''(H) = (d-2)\chi_x'(H)^2. \tag{2.1}$$

*Then, for every $d$-regular graph $G$ on $n$ vertices, $\lambda(G \circledS H) \geq \Lambda_H - o_n(1)$, where*

$$\Lambda_H \triangleq d\left(x_0 - (d-1)\frac{\chi_{x_0}(H)}{\chi_{x_0}'(H)}\right). \tag{2.2}$$

As shown in the proof of Theorem 2.1, despite the polynomial equation from Equation (2.1) usually yielding complex solutions, there is always at least one real solution. Experiments overwhelmingly suggest that the bound accurately reflects the behavior of $\lambda(G \circledS H)$ for a typical graph $G$. Having this in mind, we may posit that the structure of Equations (2.1) and (2.2), namely,

$$(d-1)\Phi\Phi'' = (d-2)(\Phi')^2,$$

and the accompanied expression $d\left(x-(d-1)\frac{\Phi(x)}{\Phi'(x)}\right)$, epitomize the derandomized squaring operation with a typical $d$-regular graph. By setting $\Phi = \chi(H)$, we incorporate details about $H$.

Although the proof of Theorem 2.1 leans on deep results from analytic combinatorics and the symbolic method, employing the theorem remains elementary. However, as perhaps anticipated, it is not as direct as the Rozenman-Vadhan bound from Equation (1.1), but rather it requires finding the largest real solution to a polynomial equation.

Before proceeding further, we introduce the following notation. Recall that $G \circledS H$ is $D$-regular where $D = cd$. We define $\kappa_H = \frac{\Lambda_H}{\sqrt{D-1}}$, and note that, due to the Alon-Boppana bound, $\kappa_H \in \left[2, \frac{D}{\sqrt{D-1}}\right] \approx [2, \sqrt{D}]$.

#### 2.1.1 Equivalent reformulations of Theorem 2.1

One can alternatively recast our procedure for finding a lower bound for $\lambda(G \circledS H)$, as given by Theorem 2.1, in several equivalent ways, as we describe next.

**Recasting the procedure using the Cauchy transform.** The Cauchy transform is a useful analytic tool which we will make an extensive use of in this paper (see Section 4.2). For a graph $H$ on $d$ vertices, the Cauchy transform takes a simple form and is given by

$$\mathcal{G}_H(x) = \frac{1}{d} \cdot \frac{\chi'_x(H)}{\chi_x(H)} = \frac{1}{d}\sum_{i=1}^{d} \frac{1}{x-\lambda_i}. \tag{2.3}$$

Using the Cauchy transform we can reformulate Theorem 2.1 as follows.

**Theorem 2.2** (Recasting Theorem 2.1 in terms of the Cauchy transform)**.** *Let $H$ be a vertex-transitive $c$-regular graph on $d \geq 3$ vertices, where $c \geq 1$. Let $x_0$ be the unique positive real solution to the equation*

$$\frac{d}{d-1}\mathcal{G}_H(x)^2 + \mathcal{G}'_H(x) = 0. \tag{2.4}$$

*Then, for every $d$-regular graph $G$ on $n$ vertices, $\lambda(G \circledS H) \geq \Lambda_H - o_n(1)$, where*

$$\Lambda_H = dx_0 - \frac{d-1}{\mathcal{G}_H(x_0)}. \tag{2.5}$$

We emphasize that, as demonstrated in the proof of Theorem 2.2, there always exists a positive real solution to Equation (2.4) and it is unique.

**Recasting the procedure as a minimization problem.** By defining

$$\psi_H(x) = dx - \frac{d-1}{\mathcal{G}_H(x)},$$

we can recast the procedure outlined in Theorem 2.1 as computing the value $x_0 > c$ that minimizes $\psi_H(x)$, where it can be shown that such $x_0$ exists and is unique. That is, $\Lambda_H = \min_{x>c} \psi_H(x)$ (see Theorem 5.9). As $\lambda(G \circledS H)$ is the solution to a maximization problem (being the largest eigenvalue of $H$ in absolute value, excluding $\lambda_1 = c$), one way to interpret this way of recasting the procedure is as the following min-max result (which, we posit, should hold with equality, but for the vanishing term, for a typical $G$ on $n$ vertices):

$$\lambda(G \circledS H) = \max_{i>1} |\lambda_i(G \circledS H)| \geq \min_{x>c} \psi_H(x) - o_n(1).$$

In Section 8.4, we introduce a fourth approach, characterized by a more combinatorial perspective, to restate Theorem 2.1. This approach serves us in studying derandomized squaring with cycle graphs.

### 2.1.2 Derandomized squaring with bounded-degree graphs

An advantage of the latter formulation of Theorem 2.1 as a minimization problem is that it allows us to find upper bounds on $\Lambda_H$ even in cases where it is too difficult to find the minimum of $\psi_H(x)$. Indeed, $\psi_H(x_0)$ serves as an upper bound on $\Lambda_H$ for any $x_0 > c$. Using this, we prove that our lower bound (which recall, we posit reflects the true behavior of derandomized squaring with a typical $d$-regular graph $G$) on the spectral expansion of $\lambda(G \circledS H)$ gravitates towards the Alon-Boppana bound for every vertex-transitive graph $H$ with bounded degree. Quantitatively, in Theorem 8.1 we prove that for every simple [4] vertex-transitive $c$-regular graph $H$ on $d$ vertices, it holds that

$$\kappa_H \leq 2 + \frac{\sqrt{c}}{\sqrt{d} - \sqrt{c}}. \tag{2.6}$$

Theorem 8.1 further asserts that the bound on $\kappa_H$ gravitates towards 2 at a linear rate, specifically, $\kappa_H = 2 + O(\frac{c}{d})$, assuming $H$ is triangle-free. A noteworthy application of this result concerns the boolean hypercube on $d$ vertices, denoted as $\mathrm{HC}_d$. Although an exact analysis of $\kappa_{\mathrm{HC}_d}$ is challenging, the aforementioned result readily implies that $\kappa_{\mathrm{HC}_d} = 2 + O\left(\frac{\log d}{d}\right)$. We also derive a stronger bound assuming $H$ is a good spectral expander. Specifically, in Proposition 8.2, we establish a bound of the form

$$\kappa_H \leq 2 + \frac{2}{\sqrt{d}} \left(\frac{\lambda(H)}{\sqrt{c}}\right)^3,$$

applicable when $c < \sqrt{d}$, and a stronger bound assuming triangle-freeness.

### 2.1.3 A universal bound on $\kappa$ for simple graphs

The bound presented in Equation (2.6) is particularly effective in the low-degree regime where $c \ll d$. In contrast, for the high-degree regime, we introduce a second bound in Theorem 8.1 which is given by $\kappa_H \leq \frac{2c+d}{\sqrt{cd}}$. Building on this, we establish a universal bound for $\kappa$. Specifically, as demonstrated in Theorem 8.1, for every simple vertex-transitive graph $H$ with at least 11 vertices, $\kappa_H \leq 3$. This bound is proven to be tight using the example of the complete graph without self-loops (see Section 8.1.2). Consequently, the game-play in determining the value of $\kappa_H$ falls within the interval $[2, 3]$.

[4] We adhere to the conventional definition of a *simple graph*, which stipulates the absence of self-loops and parallel edges.

### 2.1.4 The derandomized squaring polynomial

Generally, finding the desired solution to the polynomial equation presented in Theorem 2.1 can be challenging, especially considering that the polynomial's degree is $2d-2$. Upon closer examination, it becomes apparent that the complexity of this task is actually determined by the number $s$ of *distinct* eigenvalues. To see this denote these distinct eigenvalues of $H$ by $c = \mu_1 > \mu_2 > \cdots > \mu_s$, where $m_i$ is the multiplicity of the eigenvalue $\mu_i$. Using this notation, Equation (2.4) can be written as

$$\frac{1}{d}\sum_{i,j=1}^{s} m_i m_j \frac{g(x)^2}{(x-\mu_i)(x-\mu_j)} - \left(1-\frac{1}{d}\right)\sum_{i=1}^{s} m_i \frac{g(x)^2}{(x-\mu_i)^2} = 0,$$

where $g(x) = \prod_{i=1}^{s} x - \mu_i$.

The left-hand side is evidently a polynomial of degree $2s-2$, and it can be verified that it is monic. We refer to this polynomial as the *derandomized squaring polynomial associated with* $H$ and denote it as $\Delta_H(x)$. Note that its degree depends only on the number $s$ of distinct eigenvalues of $H$, which may be much smaller than $d$, the number of vertices. Therefore, applying Theorem 2.1 (or any of its alternatives) is typically simpler when $s$ is small. For instance, strongly regular graphs can be characterized within the family of regular graphs, spectrally, as having $s = 3$ distinct eigenvalues. We analyze the derandomized squaring with strongly regular graphs in Section 8.7.

One interesting class of graphs that is contained within the class of strongly regular graphs are Paley graphs which were already discussed in Section 1.2.2. We illustrate the use of Theorem 2.1 with this example. As we prove in Section 8.6, the derandomized squaring polynomial of the $d$-vertex Paley graph is given by

$$\Delta_{\mathrm{Pal}_d}(x) = x^4 - (d-3)x^3 - \frac{d^2+4d-9}{4}x^2 + \frac{(d+1)(d-1)(d-2)}{4}x - \frac{d(d-1)^2(d-2)}{16}.$$

From this one can compute $\Lambda_{\mathrm{Pal}_d}$ for any particular $d$. The first values (recall $d \equiv_4 1$) are $\kappa_{\mathrm{Pal}_5} \approx 2.026$, $\kappa_{\mathrm{Pal}_9} \approx 2.203$, and $\kappa_{\mathrm{Pal}_{13}} \approx 2.279$. More interestingly, we can study the limit behavior as $d \to \infty$. To this end, it suffices to consider the following simpler polynomial $\Delta_{\mathrm{Pal}_\infty}(x) \triangleq x^4 - dx^3 - \frac{d^2}{4}x^2 + \frac{d^3}{4}x - \frac{d^4}{16}$, or, after homogenizing,

$$x^4 - x^3 - \frac{1}{4}x^2 + \frac{1}{4}x - \frac{1}{16}.$$

Finding the unique positive root of $\Delta_{\mathrm{Pal}_\infty}(x)$ and substituting to Equation (2.5), we get

$$\kappa_{\mathrm{Pal}_\infty} \triangleq \lim_{d\to\infty} \kappa_{\mathrm{Pal}_d} = \frac{1+\sqrt{13+16\sqrt{2}}}{\sqrt{8}} \approx 2.46,$$

which aligns with Equation (1.3).

## 2.2 Matching the lower bound with $H$-local graphs

As previously discussed, we have yet to establish that the lower bound provided by Theorem 2.1 is tight in general. However, empirical results strongly suggest its accuracy. Specifically, we believe this to be true for *every* vertex-transitive graph $H$ on $d$ vertices and for a *typical* $d$-regular graph $G$. In light of the evidence supporting this assertion, as we discuss next, we will formulate it as a conjecture in Section 2.4.

In order to state our analytic evidence for the tightness of our bound, we observe that from the perspective of a vertex $v$ in $G \circledS H$, the vertex $v$ participates in $d$ instances of $H$. This is because each of the $d$ neighbors of $v$ positions it within a copy of $H$. We call a graph that has the above local property an *$H$-local graph* (see Definition 6.1 for the formal definition). The following theorem formalizes the evidence we have gathered for the tightness of our lower bound.

**Theorem 2.3.** *For every vertex-transitive graph $H$ on $d \geq 3$ vertices and for every $n \geq 1$, there exists an $H$-local graph $X_H$ on $nd$ vertices such that $\lambda_2(X_H) \leq \Lambda_H$.*

In addition to Theorem 2.3, we prove the optimality of our lower bound in three specific cases of $H$: the clique with self-loops, which corresponds to the actual squaring operation; the clique without self-loops, which corresponds to a non-backtracking length-2 random walk; and lastly, the graph employed in the Rozenman-Vadhan bound's tightness result. We provide further details on these cases in Section 8.1.

Going back to Theorem 2.3, note that we manage to bound only the second-largest eigenvalue, $\lambda_2(X)$, rather than the spectral expansion $\lambda(X) = \max(\lambda_2(X), |\lambda_n(X)|)$. Graphs with such property are termed *one-sided spectral expanders*. These graphs are suitable for numerous applications, primarily due to the fact that this property alone suffices for the Alon-Chung Lemma [AC88].

The proof of Theorem 2.3 leverages finite free probability and the interlacing technique that were developed by Marcus, Spielman, and Srivastava [MSS15b, MSS18, MSS22]. We provide a high-level overview for the proof of Theorem 2.3 in Section 3.2, however, already here we emphasize that the fact that our lower bound, which is based on results from analytic combinatorics, matches our upper bound which is rooted in tools from free probably theory is an instantiation of a deep connection between the two fields. This has to do with the fact that one combinatorial proof for the Lagrange inversion formula–a tool used under the hood in our lower bound–makes use of Lukasiewicz paths that in turn are tightly connected to the lattice of non-crossing partitions which is at the heart of free probability theory. The reader is referred to Chapter 16 in the excellent book by Nica and Speicher [NS06] to learn more about this connection, though for our purpose, of studying the derandomized squaring operation, we give a direct and self-contained proof.

**Related work.** In their paper, Mohanty and O'Donnell [MO20] proved the existence of $X$-Ramanujan graphs for a wide class of infinite graphs called *additive product graphs*. These can be shown to include the graphs that are obtained by derandomized squaring. As a result, Theorem 2.3 can also be derived from [MO20]. We turn to give a brief comparison between the two proofs. As in our proof, the interlacing technique is used to argue that a particular graph in the family "behaves as well" as the expected characteristic polynomial (the reader who is unfamiliar with this approach by MSS is referred to Section 3.2). Notably, when analyzing the expected characteristic polynomial, Mohanty and O'Donnell adopt a different approach than our own. They consider a generalization of the matching polynomial, which arises in the study of Ramanujan graphs. In contrast, our approach aligns with the later works of MSS and is entirely analytical, departing from the combinatorial method employed in MSS's earlier work [MSS15a]. We believe that our proof, tailored to the case of derandomized squaring, is both simpler and more straightforward. An interesting question we leave open is to generalize our lower bound, given by Theorem 2.1, to the more general setting of additive product graphs.

### 2.3 Lower bound on the spectral expansion of rotating expanders

A "standard" length-$t$ random walk on a graph $G$ is analyzed by considering the power graph, denoted as $G^t$, generalizing the square of the graph $G^2$ which was discussed so far. This graph encodes the number of length-$t$ walks by introducing an edge for each such walk between the two corresponding vertices. It is easy to see that if $\mathbf{A}$ is the adjacency matrix of $G$, then the matrix $\mathbf{A}^t$ is the adjacency matrix of $G^t$. Consequently, the spectral expansion of $G^t$, which is the most pertinent quantity when examining length-$t$ random walks on $G$, is given by $\lambda(G^t) = \lambda(G)^t$. In particular, if $G$ is a $d$-regular Ramanujan graph, then $\lambda(G^t) = 2^{\Omega(t)}\sqrt{D-1}$, where $D = d^t$ is the degree of $G^t$. Therefore, even if $G$ is initially Ramanujan, the power graph is exponentially distant, in $t$, from Ramanujan.

With an eye towards potential applications to theoretical computer science, Cohen and Maor [CM23] proposed that permuting the vertices after each step (in a palindrome fashion to result in an undirected graph) can circumvent this exponential deterioration. More precisely, the authors proved that for every $d$-regular Ramanujan graph $G$ with adjacency matrix $\mathbf{A}$, and for every integer $t \geq 2$, there exists a sequence of permutation matrices $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_{t-1})$ such that the graph $G_{\mathbf{P}}$, whose adjacency matrix is given by

$$\mathbf{A}_{\mathbf{P}} = \mathbf{A}\mathbf{P}_{t-1} \cdots \mathbf{A}\mathbf{P}_1 \mathbf{A}^2 \mathbf{P}_1^\top \mathbf{A} \cdots \mathbf{P}_{t-1}^\top \mathbf{A},$$

has spectral expansion

$$\lambda(G_{\mathbf{P}}) \leq \left(1 + \frac{1}{t}\right)^t (t+1)\sqrt{D} + o(1), \tag{2.7}$$

where $D = d^{2t}$ is the degree of $G_{\mathbf{P}}$ and the $o(1)$ term is a quantity that vanishes exponentially fast with the girth of $G$, and should be ignored in this introductory section. Specifically, by permuting the vertices after each step using suitable permutations, the deterioration is reduced from exponential to linear in $t$.

An open problem left in [CM23] is to establish a lower bound on the spectral expansion of $G_{\mathbf{P}}$ that is applicable for any permutation sequence $\mathbf{P}$. Specifically, the authors left open the question of whether the linear dependence in $t$ is optimal. Experimental results suggest that for a typical $\mathbf{P}$, Equation (2.7) holds with equality, up to the vanishing $o(1)$ term. However, it is entirely plausible that the typical behavior does not accurately represent the behavior of the optimal permutation sequence $\mathbf{P}$. The logic would be that for a graph with substantial structure, such as a Cayley graph, a permutation sequence that takes into account the structure of the underlying group and the set of generators may yield a superior spectral expansion. However, in this work we resolve this open problem by proving that the bound is indeed tight.

**Theorem 2.4.** *For every $d$-regular graph $G$ and for every permutation sequence $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_{t-1})$,*

$$\lambda(G_{\mathbf{P}}) \geq \left(1 + \frac{1}{t}\right)^t (t+1)\sqrt{D} - o(1).$$

In fact, our lower bound applies to the product of any $d$-regular graphs, not just to isomorphic graphs as used in the construction of $G_{\mathbf{P}}$. For $t = 1$, where no actual product is involved, this essentially aligns with the Alon-Boppana bound. As suggested by Theorem 2.4 (ignoring the $o(1)$ term), we have $\lambda(G_{\mathbf{P}}) = \lambda(G^2) \geq 4\sqrt{D}$. However, for $t = 2$, the bound increases to $\lambda(G_{\mathbf{P}}) \geq \frac{3^3}{2^2}\sqrt{D} = 6.75\sqrt{D}$, and for $t = 3$, it further deteriorates to $\lambda(G_{\mathbf{P}}) \geq \frac{4^4}{3^3}\sqrt{D} \approx 9.48\sqrt{D}$. As indicated, the gap for graph products increases linearly with the number of graphs involved, making them inherently far from Ramanujan.

Our proof begins similarly to the proof of our lower bound for the spectral expansion of a derandomized square, by employing the trace method. However, unlike the derandomized square, here we are able to prove our bound by pure combinatorial means, without resorting to analytic tools. Our key observation lies in relating the problem with the Fuss-Catalan numbers which generalize the Catalan numbers that emerge when bounding the spectral expansion of $d$-regular graphs.

### 2.4 Two conjectures and open problems

Given our results and the above discussion, we wish to put forth two conjectures that capture different aspects of the tightness of our lower bound as given by Theorem 2.1. These are analog to fundamental questions on Ramanujan graphs where Theorem 2.1 plays in this analogy the role of the Alon-Boppana bound.

**Conjecture 2.5.** *For every vertex-transitive graph $H$, $\lambda(G \circledS H) \leq \Lambda_H$ holds for infinitely many graphs $G$.*

Conjecture 2.5 is analog to the fundamental question regarding the existence of Ramanujan graphs which has received significant attention in the literature. Resolving Conjecture 2.5 with respect to $\lambda_2(G \circledS H)$ would be interesting as well. Our second conjecture focuses on the typical behavior, and is analogous to Friedman's resolution [Fri08] of Alon's conjecture [Alo86] (see also [Bor20]). We first introduce the following notation: For an even integer $n$ and for an integer $d$, we let $\mathcal{M}_{n,d}$ denote the distribution over $d$-regular graphs on $n$ vertices that are sampled by taking the union of $d$ uniformly random and independent perfect matchings, where edges that are sampled multiple times are counted with the respective multiplicity.

**Conjecture 2.6.** *For every vertex-transitive graph $H$ on $d$ vertices and for every $\varepsilon > 0$,*

$$\mathop{\mathbf{Pr}}_{G \sim \mathcal{M}_{n,d}} [\lambda(G \circledS H) \geq \Lambda_H + \varepsilon] = o_n(1).$$

In addition to the conjectures previously discussed, our research raises several intriguing questions. An obvious open problem is the generalization of our results to non-vertex-transitive graphs. For potential theoretical computer science applications, it would be pertinent to identify conditions that a pair of graphs $G$ and $H$ satisfy so that the spectral expansion $\lambda(G \circledS H)$ is close to our lower bound or, at a minimum, substantially improves upon the Rozenman-Vadhan bound. Once this aspect is clearer, problems regarding the explicitness can be addressed. To give just one additional research question, we believe that the extension of our techniques to additional graph operations, including the Zig-Zag product and the wide-replacement product, is feasible. We defer this exploration to future research.

### Organization of the rest of the paper

In Section 3 we give a high-level proof overview of our results. The proof of Theorem 2.1 that deals with the limitation of derandomized squaring is given in Section 5, where we also derive its different equivalent formulations. In Section 6 we prove Theorem 2.3 which constitutes our analytic evidence for the tightness of Theorem 2.1. Our result on rotating expanders, Theorem 2.4, is given in Section 7. In Section 8 we apply our results to interesting graph families, and prove our universal bound on $\kappa_H$ for simple graphs.

# 3 Proof Overview

In this section, we provide an informal overview of the proofs for our results. We begin with our lower bound for the spectral expansion of derandomized squaring, as given by Theorem 2.1 (outlined in Section 3.1). Our proof relies on the symbolic method and leverages results from analytic combinatorics, both of which we introduce and explain in the respective sections (see Section 3.1.1 and Section 3.1.3 for the necessary background). Additionally, we briefly outline the proof for our evidence regarding the tightness of our lower bound, as stated in Theorem 2.3, in Section 3.2. In that section, we provide the necessary background on finite free probability, which is essential for understanding the proof. Finally, in Section 3.3, we give a sketch of the underlying ideas of the proof for Theorem 2.4, which concerns the lower bound on the spectral expansion of rotating expanders.

## 3.1 Limitations of derandomized squaring

As before, let $G$ be a $d$-regular graph and $H$ a vertex-transitive $c$-regular graph on $d$ vertices. In this section we sketch the proof for our lower bound on $\lambda(G \circledS H)$, as stated in Theorem 2.1. Our starting point is standard, relying on the trace method which asserts that $\lambda(G \circledS H)$ is lower bounded by roughly $c_\ell(G \circledS H)^{1/\ell}$ for every $\ell > 0$, where $c_\ell(G \circledS H)$ is the number of length-$\ell$ cycles that originate at some fixed vertex $v$ of $G \circledS H$ (see Section 4.3). Thus, the task at hand is to compute, or at least lower bound $c_\ell(G \circledS H)$, where we will choose $\ell$ to be sufficiently large. A common strategy for this is to consider a suitable infinite cover of the graph of interest, $G \circledS H$ in our case, which we take to be $\mathcal{T}_d \circledS H$, where $\mathcal{T}_d$ is the $d$-regular infinite tree. Indeed, for every $\ell$, every length-$\ell$ cycle in $\mathcal{T}_d \circledS H$ that originated at some fixed vertex induces a unique cycle in $G \circledS H$, initiated at some fixed vertex, and so $c_\ell(G \circledS H) \geq c_\ell(\mathcal{T}_d \circledS H)$.

We obtain an accurate estimate on $c_\ell(\mathcal{T}_d \circledS H)$ by first expressing the combinatorial class of cycles in $\mathcal{T}_d \circledS H$ using the symbolic method, from which we immediately derive a functional equation that is satisfied by the corresponding generating function. We then use results from analytic combinatorics to get the desired estimate on the coefficients of the latter. The symbolic method, a prominent combinatorial theory, allows one to deduce a functional equation that is satisfied by the class's generating function straight from its specification. Given its lesser prominence in theoretical computer science, we begin with a brief overview of the symbolic method, and as a preliminary exercise, we determine a lower bound for $c_\ell(\mathcal{T}_d)$ (see Section 3.1.1), which explains the familiar $2\sqrt{d-1}$ bound on the spectral expansion of $d$-regular graphs. Following this, in Section 3.1.2, we utilize the symbolic method to define the cycle class in $\mathcal{T}_d \circledS H$ and from there, derive a functional equation that is satisfied by the associated generating function.

With the functional equation in hand, our objective is to deduce estimates of its coefficients. While straightforward for simpler instances like $\mathcal{T}_d$, the task becomes more complex for our graph, $\mathcal{T}_d \circledS H$. To achieve the sought-after estimate, we employ deep results from analytic combinatorics. These treat the functional equation as a meromorphic function, considering its singularities to determine the bound. We provide the essential context and outline our derivation for the estimates in Sections 3.1.3 and 3.1.4. For a comprehensive treatment of the symbolic method and analytic combinatorics, we refer the reader to the excellent book by Flajolet and Sedgewick [FS09], though, our presentation is meant to be self-contained.

### 3.1.1 The symbolic method: a swift overview

The symbolic method provides a technique to convert a specification of a combinatorial class by means of certain combinatorial constructs into a functional equation that is satisfied by its associated generating function. In more technical terms, a *combinatorial class* $\mathcal{A}$ consists of a collection of combinatorial objects paired with a designated *size* function $|\cdot| : \mathcal{A} \to \mathbb{N}$. The associated *(ordinary) generating function* for this class is the formal power series $A(z) = \sum_{a\in\mathcal{A}} z^{|a|} = \sum_{k\in\mathbb{N}} A_k z^k$, where $A_k$ is the number of objects in $\mathcal{A}$ of size $k$, which we always assume is finite.

Set theoretic operators on the combinatorial classes reflect in their associated generating functions. For instance, when two combinatorial classes, $\mathcal{A}$ and $\mathcal{B}$, are combined in a disjoint union, denoted as $\mathcal{A} + \mathcal{B}$, the corresponding generating function becomes the sum of their individual generating functions, $A(z) + B(z)$. When considering the Cartesian product $\mathcal{A} \times \mathcal{B}$, it corresponds to the multiplication of their generating functions. In this context, the size of an element $(a, b)$ from $\mathcal{A} \times \mathcal{B}$ is given by $|a| + |b|$. This concept of the Cartesian product can be extended to multiple classes. Another valuable concept is the *sequence* of a class, denoted as $\mathsf{SEQ}(\mathcal{A})$. This represents the disjoint union of the Cartesian products across all finite lengths $n \geq 0$. The generating function for $\mathsf{SEQ}(\mathcal{A})$ is given by $\frac{1}{1-A(z)}$.

We make use of standard shorthand notations: For an integer $\ell \geq 1$ and a class $\mathcal{A}$, we let $\ell\mathcal{A}$ denote the sum of $\ell$ copies of $\mathcal{A}$. We similarly write $\mathcal{A}^\ell$ for the Cartesian product of $\ell$ copies of $\mathcal{A}$. The class denoted $\mathcal{Z}$ refers to the class containing a single element of size 1. Its generating function is, of course, $z$. The elements of size 1 in a combinatorial class $\mathcal{A}$ are called *atoms*, all of which are considered distinct. An element of size 0, denoted as $\epsilon$, is called a *neutral object*.

For instance, the class of binary strings can be constructed as $\mathsf{SEQ}(\{0\} + \{1\})$ where both elements $0, 1$ in their corresponding sets are atoms. Note that we can also write the class more succinctly as $\mathsf{SEQ}(\mathcal{Z}+\mathcal{Z})$ or $\mathsf{SEQ}(2\mathcal{Z})$ as indeed $2\mathcal{Z}$ is a combinatorial class that consists of two atoms. For the purpose of counting elements, these descriptions are equivalent, or isomorphic, though the second is less informative. From this, the corresponding generating function is immediately obtained, $\frac{1}{1-2z} = \sum_{k=0}^{\infty} 2^k z^k$.

To give another example, consider the class of rooted trees where the sequence order of a node's children matters, meaning they are arranged from left to right. This class can be formulated using the recurrence $\mathcal{A} = \bullet \times \mathsf{SEQ}(\mathcal{A})$, where $\bullet$ symbolizes an atom denoting a node. In this context, the size function corresponds to the number of vertices in the tree. To elaborate, a tree consists of a node, contributing a size of 1, followed by a sequence of trees. The related generating function satisfies the functional equation $A(z) = \frac{z}{1-A(z)}$, or equivalently $A(z)^2 - A(z) + z = 0$. Using basic methods, it can be shown that the coefficients of $A(z)$ are the Catalan numbers.

**A preliminary example: counting cycles in $\mathcal{T}_d$.** To illustrate the symbolic method with a fairly straightforward example which is related to our problem, let us determine the number of cycles in $\mathcal{T}_d$ that originate at the root. Denote the corresponding class by $\mathcal{C}$, where the size function is the cycle's length. To simplify the problem slightly, we truncate one branch from the root. As it turns out, this has no affect on the asymptotic behavior, and is anyhow valid if one aims for proving a lower bound. The recursive specification of a cycle yields

$$\mathcal{C} = \mathsf{SEQ}\left(\{1,2,\ldots,d-1\} \times \mathcal{C} \times \uparrow\right), \tag{3.1}$$

where the elements $1,2,\ldots,d-1$ and $\uparrow$ are atoms.

To see this, observe that within the $\mathsf{SEQ}$ construct, we specify the class of cycles that originate at the root and revisit it only upon cycle completion. Specifically, we have $d-1$ options for the first step, each of length 1. This is followed by a cycle in the infinite $d$-ary tree originating from the node we transitioned to. The concluding atom $\uparrow$ represents the move from that node back to the root. An equivalent, more succinct, formulation is given by $\mathcal{C} = \mathsf{SEQ}\left(((d-1)\mathcal{Z}^2) \times \mathcal{C}\right)$. As an immediate consequence, the associated generating function $C(z)$ satisfies the functional equation

$$C(z) = \frac{1}{1-(d-1)z^2 C(z)}. \tag{3.2}$$

From this point one can proceed to extract the coefficients of $C(z)$ by elementary means especially since the problem's simplicity permits such an approach. However, when applying the symbolic method to analyze the derandomized squaring operation, directly determining the coefficients might be an insurmountable challenge. We thus resort to approximating the coefficients using results from analytic combinatorics. We will also do that for this running example later on, and so for comparison, we briefly recall the standard derivation for the exact coefficients by elementary means: By Equation (3.2), $C(z) = \frac{1-\sqrt{1-4(d-1)z^2}}{2(d-1)z^2}$, and since

$$\sqrt{1-w} = \sum_{n=0}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} w^n = -\sum_{n=0}^{\infty} \frac{2}{4^n n} \binom{2n-2}{n-1} w^n,$$

we have that

$$C(z) = \frac{1}{2(d-1)z^2} \cdot \sum_{n=1}^{\infty} \frac{2}{4^n n} \binom{2n-2}{n-1} (4(d-1)z^2)^n = \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} (d-1)^n z^{2n}.$$

Hence, for an even $k$, the coefficient of $z^k$ in $C(z)$ is given by

$$\left[z^k\right] C(z) \approx k^{-3/2} \cdot (2\sqrt{d-1})^k. \tag{3.3}$$

By using the trace method, which involves taking the $k$-th root of the above expression, we see the (or a) reason for the $2\sqrt{d-1}$ bound on the spectral expansion of $d$-regular graphs.

**Substitutions.** In order to devise the specification of the class of cycles in $\mathcal{T}_d \circledS H$, analog to the derivation in Equation (3.1) for the cycles in $\mathcal{T}_d$, we introduce one more construct of combinatorial classes called *substitution*. For two classes $\mathcal{A}, \mathcal{B}$, the combinatorial class, denoted as $\mathcal{A} \circ \mathcal{B}$, is obtained by replacing in each object of $\mathcal{A}$ each atom by an element of $\mathcal{B}$. For example, we revisit the class of cycles in $\mathcal{T}_d$ and observe that an alternative specification for the one that was obtained in Equation (3.1) is given by

$$\mathcal{C} = (\mathsf{SEQ}\left(\{1, 2, \ldots, d-1\}\right)) \circ (\downarrow \times \mathcal{C} \times \uparrow). \tag{3.4}$$

To see this, observe that for describing a cycle, one first needs to define the order in which the root visits its sons. For each instance of a son $i \in \{1, \ldots, d-1\}$ in the sequence, we substitute it with a step towards the son, symbolized by the atom $\downarrow$. This is followed by a cycle at the tree originating from the son, and then a return step, represented by the atom $\uparrow$. Generally, if the generating functions for two combinatorial classes $\mathcal{A}$ and $\mathcal{B}$ are denoted as $A(z)$ and $B(z)$ respectively, then the generating function for $\mathcal{A} \circ \mathcal{B}$ can be expressed as the composition $A(B(z))$. This offers an alternate validation for Equation (3.2).

### 3.1.2 The functional equation for derandomized squaring

Let $H$ be a vertex-transitive graph on $d$ vertices. Define $\mathcal{C}_{\mathcal{T}_d \circledS H}$ as the combinatorial class of cycles in $\mathcal{T}_d \circledS H$ that originate at the root. As previously mentioned, the size function corresponds to the cycle's length. To prevent double-counting, we exclude the empty cycle from this class. When expressing the class using the symbolic method, we use $\mathcal{S}_H$ to represent the combinatorial class of nonempty cycles in $H$ that only revisit the originating vertex upon completing the cycle. Consequently, as detailed below, after truncating one branch of the root as was done when we studied $\mathcal{T}_d$, the class $\mathcal{C}_{\mathcal{T}_d \circledS H}$ satisfies to the recursive relation

$$\mathcal{C}_{\mathcal{T}_d \circledS H} = \{1, \ldots, d-1\} \times \left(\mathcal{S}_H \circ \left(\rightarrow \times \left(\mathcal{C}_{\mathcal{T}_d \circledS H} + \epsilon\right)\right)\right). \tag{3.5}$$

Here, $\rightarrow$ symbolizes an atom, which we interpret as a step within a cycle in $H$.

To see this, remember that each son of the root positions the root within a copy of $H$. Therefore, when describing a non-empty cycle originating at the root, we first select one of its $d-1$ sons, which determines the copy of $H$ in which the root is involved. Now, consider any cycle within that copy of $H$ starting at the root, $v_1 \to v_2 \to \cdots \to v_\ell = v_1$. This cycle corresponds to a cycle in $\mathcal{T}_d \circledS H$ that begins at the root in the following manner: After each step $v_i \to v_{i+1}$ on the cycle, we examine the copy of $\mathcal{T}_d \circledS H$ rooted at $v_{i+1}$ and attach a cycle from that copy of $\mathcal{T}_d \circledS H$. When we return to $v_{i+1}$, we proceed with $v_{i+1} \to v_{i+2}$. Note that attaching an empty cycle is permissible, even though it is not included in $\mathcal{C}_{\mathcal{T}_d \circledS H}$, leading to the addition of the neutral element $\epsilon$ in Equation (3.5). Furthermore, after the final step $v_{\ell-1} \to v_\ell = v_1$, we attach another (potentially empty) copy of $\mathcal{C}_{\mathcal{T}_d \circledS H}$ to account for cycles that visit the root more than twice. This rationale underpins our definition of $\mathcal{S}_H$, which is designed to prevent over-counting that would have otherwise occur.

Equation (3.5) directly implies that the generating function, $C_{\mathcal{T}_d \circledS H}(z)$, associated with the class $\mathcal{C}_{\mathcal{T}_d \circledS H}$ satisfies

$$C_{\mathcal{T}_d \circledS H}(z) = (d-1)S_H\left(z\left(C_{\mathcal{T}_d \circledS H}(z)+1\right)\right), \tag{3.6}$$

where $S_H(z)$ is the generating function corresponding to the class $\mathcal{S}_H$. On its own, this result does not provide much insight, as the functional equation $u = (d-1)S_H(z(u+1))$ tends to be intricate, hindering our ability to extract the coefficients of $C_{\mathcal{T}_d \circledS H}(z)$. For instance, even in the simple case of a length-4 cycle, $H = C_4$, in which case $S_{C_4}(z) = \frac{2z^2}{1-2z^2}$, Equation (3.6) takes the form

$$2z^2c(z)^3 + 10z^2c(z)^2 + (14z^2-1)c(z) + 6z^2 = 0,$$

where the term $c(z)$ is a shorthand for $C_{\mathcal{T}_d \circledS C_4}(z)$, resulting in a complicated expression for $c(z)$.

To address this challenge, we leverage a deep result from analytic combinatorics. We will first provide the essential background in the following section, Section 3.1.3. Subsequently, in Section 3.1.4, we will outline our approach to estimating the coefficients of $C_{\mathcal{T}_d \circledS H}(z)$ using Equation (3.6) as our starting point.

### 3.1.3 A brief introduction to analytic combinatorics

The symbolic method classifies combinatorial classes into *schemes* based on their shared structures. This approach aims to consolidate solutions to these problems and highlight their interrelations. A notable schema within this framework is termed *smooth inverse-function schema*. These are classes whose generating function $\zeta(z)$ satisfies the functional equation $u = z \cdot \phi(u)$, namely, $\zeta(z) = z \cdot \phi(\zeta(z))$, for some "well-behaved" function $\phi(u)$. By manipulating Equation (3.6), we see that $\mathcal{C}_{\mathcal{T}_d \circledS H}$ is tightly connected to this schema. Indeed, letting $\zeta_H(z) = z\big(C_{\mathcal{T}_d \circledS H}(z)+1\big)$, we have that $\zeta_H(z) = z \cdot \phi_H(\zeta_H(z))$, where

$$\phi_H(u) = 1 + (d-1)S_H(u). \tag{3.7}$$

Analytic combinatorics provides a method to estimate the coefficients of the generating function for smooth inverse-function schema. This approach is applicable under certain technical conditions on $\phi(u)$, which we hide under the rug in this informal proof overview. The key requirement though is that there is a real positive solution to the *characteristic equation* $\phi(u) = u \cdot \phi'(u)$ within $\phi$-s analytic domain around the origin (see Definition 5.2). With this, we have the following theorem which is informally stated here (see Theorem 5.6 for the formal statement).

**Theorem 3.1.** *Let $\zeta(z)$ belong to the smooth inverse-function schema. Then, with $\tau$ the positive root of the corresponding characteristic equation $\phi(u) = u \cdot \phi'(u)$, one has*

$$\left(\left[z^k\right] \zeta(z)\right)^{\frac{1}{k}} \approx \phi'(\tau). \tag{3.8}$$

The proof of Theorem 3.1 relies on results from complex analysis though, unfortunately, we are unable to say much about the proof. As mentioned, the reader is referred to the excellent book by Flajolet and Sedgewick [FS09] to learn more about this fascinating topic.

**Back to the example of cycles in $\mathcal{T}_d$.** Let us illustrate Theorem 3.1 using our ongoing example. Given that there are no cycles of odd length in $\mathcal{T}_d$, all coefficients of $C(z)$ corresponding to odd powers of $z$ vanish, and so we can rewrite Equation (3.2) as $D(z) = \frac{1}{1-(d-1)zD(z)}$, where $D(z^2) = C(z)$. By multiplying by $z$ and introducing the generating function $E(z) = zD(z)$, we get $E(z) = z \cdot \phi(E(z))$, with $\phi(z) = \frac{1}{1-(d-1)z}$. It is straightforward to confirm that $\tau = \frac{1}{2(d-1)}$ satisfies the characteristic equation, i.e., $\phi(\tau) = \tau \cdot \phi'(\tau)$. As $\phi'(\tau) = 4(d-1)$, Theorem 3.1 implies that $\left(\left[z^k\right]E(z)\right)^{1/k} \approx 4(d-1)$, leading to the conclusion $\left(\left[z^k\right]C(z)\right)^{1/k} \approx 2\sqrt{d-1}$, which aligns with the result obtained by elementary means, Equation (3.3).

### 3.1.4 Proof sketch of Theorem 2.1

With Theorem 3.1 in hand, and by the discussion above that led us to Equation (3.7), we are ready to sketch the proof of Theorem 2.1. In fact, it will be more convenient to consider the variant using the Cauchy transform as given by Theorem 2.2. Since $\mathcal{C}_H = \mathsf{SEQ}(\mathcal{S}_H)$, we have that $S_H(z) = 1 - \frac{1}{C_H(z)}$. It can also be shown that $C_H(z) = \frac{1}{z}\mathcal{G}_H(\frac{1}{z})$ (see Claim 5.4), and so Equation (3.7) takes on the form

$$\phi_H(z) = d - \frac{(d-1)z}{\mathcal{G}_H\left(\frac{1}{z}\right)}.$$

Through some algebraic manipulations, it becomes evident that the characteristic equation, $\phi_H(u) = u \cdot \phi'_H(u)$, transforms into the form presented in Equation (2.4) from Theorem 2.2 when $z$ is substituted with its reciprocal. Upon further analytical exploration, one can deduce the existence of a unique real positive solution $\tau$ to the characteristic equation within $\phi$-s analytic domain around the origin. This allows us to apply Theorem 3.1 and derive the sought-after estimate.

## 3.2 Matching the lower bound with $H$-local graphs

As briefly discussed in Section 2.2, the proof of Theorem 2.3 makes use of finite free probability. Thus, to start with, in Section 3.2.1 we give a brief account of this elegant theory. Then, in Section 3.2.2 we sketch the proof of Theorem 2.3.

### 3.2.1 Finite free probability

Free probability is a branch of mathematics, initiated by Voiculescu, that extends classical probability theory into the non-commutative setting. In classical probability, random variables are analyzed using their joint distribution, which encodes the correlations or lack of between them. In contrast, free probability introduces the abstract notion of "freeness" to represent the absence of correlations, appropriately defined, among non-commutative random variables. Free probability theory provides, in particular, tools to analyze the spectrum of the sum and product of two operators, given that these operators are free, using knowledge of their individual spectra. Freeness is an infinite-dimensional phenomena in the sense that a pair of finite-dimensional operators can only be free from one another if one of them is constant. As a result, operators associated with finite graphs cannot be studied directly by free probability theory.

In response to this limitation, Marcus, Spielman, and Srivastava, in their groundbreaking series of works [MSS15b, MSS18, MSS22], introduced the theory of *finite free probability* along with the associated technique of interlacing. This enabled them to extend some results of free probability to the finite-dimensional setting, especially regarding the spectra of matrix sums and products. While finite free probability may not capture all details of the latter spectra, it provides a one-sided bound on its support. Finite free probability does not depend on the abstract concept of freeness or any analogous notion. Rather, it demonstrates that conjugating a finite operator, $\mathbf{A}$, with an orthogonal matrix—sampled according to the Haar measure on this group—effectively "frees" $\mathbf{A}$ from other operators. We consider a specific application of this principle in the context of operator addition.

**Definition 3.2** (Definition 2.4 in [MSS18])**.** Let $\mathbf{A}, \mathbf{B}$ be $d \times d$ real symmetric matrices, with characteristic polynomials $a(x)$ and $b(x)$, respectively. The *additive convolution* of $a(x)$ and $b(x)$ is defined as

$$a(x) \boxplus_d b(x) = \mathop{\mathbf{E}}_{\mathbf{Q}} \chi_x \left(\mathbf{A} + \mathbf{Q}\mathbf{B}\mathbf{Q}^{\mathsf{T}}\right), \tag{3.9}$$

where the expectation is taken over random orthogonal matrices $\mathbf{Q}$ sampled according to the Haar measure on the group of $n$-dimensional orthogonal matrices.

We note that, while it may not be immediately apparent, the right-hand side of Equation (3.9) depends only on the spectra of $\mathbf{A}$ and $\mathbf{B}$. Consequently, the additive convolution is well-defined. It was also proved in [MSS22] that $a(x) \boxplus_d b(x)$ is real-rooted itself, hence a discussion of bounding its roots is sensible. When $d$ is clear from context, we omit the subscript $d$ in $\boxplus_d$.

The analytic machinery that will allow us to study the additive convolution is the Cauchy transform and its max-inverse (see Section 4.2 for details). More precisely, the Cauchy transform of a real-rooted degree $d$ polynomial $p(t) \in \mathbb{R}[t]$, whose roots are $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$, is defined as $\mathcal{G}_p(x) = \frac{1}{d}\sum_{i=1}^{d} \frac{1}{x-\lambda_i}$. Clearly, for an undirected graph $H$, the Cauchy transform $\mathcal{G}_H(x)$ as defined in Equation (2.3) can be expressed as $\mathcal{G}_p(x)$ where $p(t) = \chi_t(H)$ is the characteristic polynomial of $H$.

Note that when the Cauchy transform of a polynomial $p(t)$ is restricted to the domain to the right of its rightmost pole, $(\lambda_1, \infty)$, its range is $(0, \infty)$. Additionally, $\mathcal{G}_p(x)$ is monotonically decreasing within this domain. With this in mind, one can define $\mathcal{K}_p : (0, \infty) \to (\lambda_1, \infty)$ to be the inverse of $\mathcal{G}_p(x)$ when restricted to the latter domain. In other words, $\mathcal{K}_p$ is the max-inverse of $\mathcal{G}_p$. Particularly, for every $y \in (0, \infty)$, $\mathcal{K}_p(y)$ provides an upper bound on the largest root, $\lambda_1$, of $p(t)$. The key feature of the $\mathcal{K}$-transform is that it behaves very-well under additive convolution.

**Theorem 3.3** (Theorem 1.12 in [MSS22])**.** *For all $d \times d$ real symmetric matrices $\mathbf{A}, \mathbf{B}$ with characteristic polynomials $a(x), b(x)$, respectively, and for every $y > 0$, it holds that*

$$\mathcal{K}_{a \boxplus b}(y) \leq \mathcal{K}_a(y) + \mathcal{K}_b(y) - \frac{1}{y}.$$

It is worth noting that in free probability, the analog statement to Theorem 3.3 in the infinite dimensional case holds with equality.

### 3.2.2 Proof sketch of Theorem 2.3

The main idea in proving Theorem 2.3 is to randomly construct an $H$-local graph in a very intuitive way: since we want each vertex $v$ to appear in $d$ instances of $H$, we place $v$ in $d$ such instances, choosing the neighbors uniformly at random. Formally, we define a matrix $\mathcal{H}$ consisting of disjoint copies of $H$, and sum $d$ random permutations of this matrix. This results in the matrix

$$X_{\mathbf{P}}(H) = \sum_{i=1}^{d} \mathbf{P}_i \mathcal{H} \mathbf{P}_i^{\mathsf{T}},$$

where $\mathbf{P} = \mathbf{P}_1, \ldots, \mathbf{P}_d$ are permutation matrices. The proof for the existence of an $H$-local graph whose second largest eigenvalue meet our lower bound incorporates two parts:

1. Bounding the second largest root of the *expected characteristic polynomial*, $\mathbf{E}_{\mathbf{P}} \, \chi_x \left( X_{\mathbf{P}}(H) \right)$, where the permutations are sampled uniformly and independently at random.

2. Relating the roots of $\mathbf{E}_{\mathbf{P}} \, \chi_x \left( X_{\mathbf{P}}(H) \right)$ to roots of a particular choice for $\mathbf{P}$, resulting in finding a *good* permutation, which induces a graph.

On first sight, it is not clear how to relate the expectation polynomial from Part 1 with the aforementioned tools of finite free probability. Definition 3.2 uses an expectation over the Haar measure, and together with Theorem 3.3 (applied $d-1$ times) enables us to establish an upper bound on the largest root of the expected characteristic polynomial, derived as the "free sum" of $d$ of identical matrices. More precisely, a corollary from Theorem 3.3, together with the above discussion, yields

$$\mathsf{maxroot}\left( \chi_x(\mathbf{A})^{\boxplus d} \right) \leq \min_{x > \lambda_1} \left( dx - \frac{d-1}{\mathcal{G}_{\mathbf{A}}(x)} \right), \tag{3.10}$$

where $\lambda_1$ is the largest eigenvalue of $\mathbf{A}$. When taking $\mathbf{A}$ to be the matrix $\mathcal{H}$, the RHS of Equation (3.10) resembles Equation (2.5) from Theorem 2.2. However, the relevance of the LHS of the above equation remains unclear, as the expectation hidden in the $\boxplus$ operation is over the Haar measure and not over permutations. For bridging this gap, as well as for establishing Part 2, we follow MSS and proceed in two steps: quadrature and interlacing. While our proof makes a black-box use of these techniques we believe that the unfamiliar reader will benefit from this short account.

**Quadrature.** Quadrature refers to a general technique by which an integral is written as a finite sum. In our context, we make use of the result showing that finite free additive convolution can be expressed using the finite subgroup of permutation matrices of the unitary group. Specifically,

**Theorem 3.4** (Theorem 4.1 in [MSS18]). *Let $\mathbf{A}, \mathbf{B}$ be symmetric $d \times d$ matrices with $\mathbf{A1} = a\mathbf{1}$ and $\mathbf{B1} = b\mathbf{1}$. Let $\chi_x(\mathbf{A}) = (x-a)a(x)$ and $\chi_x(\mathbf{B}) = (x-b)b(x)$. Then,*

$$\mathop{\mathbf{E}}_{\mathbf{P}} \chi_x\left(\mathbf{A} + \mathbf{PBP}^\intercal\right) = (x - (a+b)) \cdot a(x) \boxplus_{d-1} b(x),$$

*where $\mathbf{P}$ is a uniformly random permutation matrix.*

Assume that $\mathbf{A}$ is the adjacency matrix of a $c$-regular graph, and let $p(x) = \frac{\chi_x(\mathbf{A})}{x-c}$. As a direct corollary of Theorem 3.4, we get that

$$\mathop{\mathbf{E}}_{\mathbf{P}_1,\ldots,\mathbf{P}_d} \chi_x\left(\sum_{i=1}^{d} \mathbf{P}_i\mathbf{A}\mathbf{P}_i^\intercal\right) = (x - dc) \cdot p^{\boxplus d}(x).$$

Consequently, by taking $\mathbf{A} = \mathcal{H}$, the upper bound on the max-root of the convolution polynomial, derived using Equation (3.10), directly establishes a bound on the max-root of the expected characteristic polynomial appearing on the LHS. The advantage is that we are now considering an expectation over a finite distribution, and more importantly, each element in the support of the distribution is an $H$-local graph. The final step of interlacing permits us to conclude that an element exists within this distribution for which the same upper bound holds.

**Interlacing.** So far, we have discussed how to obtain a bound on the largest root of the expected characteristic polynomial (excluding the trivial root), where the expectation is over the group of permutation matrices. It is generally incorrect to assert that a bound on the largest root of the expectation of polynomials can be utilized to infer a bound on the largest root of one of the polynomials involved in the expectation. A key observation by MSS concerning this issue is that such an result holds if the polynomials participating in the expectation form an *interlacing family*. In fact, for any choice of $k$, this structure suffices to deduce a bound on the $k$-th largest root of at least one polynomial in the family, given that we are able to bound the $k$-th largest root of the expected characteristic polynomial.

### 3.3 Lower bound on the spectral expansion of rotating expanders

In this section we sketch the ideas underlying the proof of Theorem 2.4. For simplicity, we focus on the simplest case, $t = 2$. Specifically, suppose we have two $d$-regular graphs, denoted as $G_1$ and $G_2$, on the same vertex set with adjacency matrices $\mathbf{A}_1$ and $\mathbf{A}_2$, respectively. It is possible to construct a $d^4$-regular graph whose adjacency matrix is $\mathbf{A}_1\mathbf{A}_2^2\mathbf{A}_1$. Recall that the symmetrization is necessary to ensure that the resulting product remains an undirected graph. Combinatorially, this is the graph that encodes length-4 walks, where the first and last steps are according to $G_1$ and the two middle steps are done according to $G_2$. As before, for proving a lower bound on the spectral expansion of the above product graph, we employ the trace method. Consequently, we will need to argue about the number of cycles in the graph product. Interestingly, the number of such cycles is closely tied to the Fuss-Catalan numbers.

A length-$k$ cycle in the product graph can be divided into $4k$ steps, $2k$ of which are from $G_1$ and the rest are from $G_2$. In this walk, step 1 occurs in $G_1$, steps 2 and 3 occur in $G_2$, steps 4 and 5 take place in $G_1$, and so on, until the last step, which is in $G_1$. Let us assume that such a length-$k$ walk from a vertex $v$ forms a cycle $c$, where $m$ denotes the first step (out of a total of $4k$ steps) at which the walk revisits vertex $v$. In other words, the length-$m$ prefix of $c$ takes the form $v \to v_1 \to \cdots \to v_{m-1} \to v_m = v$.

If we assume that there are only tree-like cycles in $G_1$ and $G_2$ (meaning there are no cycles in $G$ with a length smaller than $2k$), and no nontrivial "relations" between the two graphs, it becomes evident that $v_{m-1} = v_1$. This implies that $v_1 \to \cdots \to v_{m-1}$ forms a cycle (which may not necessarily close only once), with the first and last edges originating from $G_2$. This condition holds recursively, meaning that such cycles are embedded within each other, and do not *cross*. By saying that there are no "relations" between the two graphs, we mean that we assume nothing about the edge sets of the two graphs, and so a backwards step in one graph cannot correspond to a forward step in the other. These two assumptions are, of course, perfectly valid for the purpose of proving a lower bound.

To calculate the number of such cycles, similarly to the approach in Equation (3.1), where we either moved away from or returned toward the root of the tree, we consider each step as either an opening or a closing bracket, with an associated color representing the graph. Figure 1 illustrates the three possible options for opening and closing such colored brackets, without any "crossings", representing the assumption regarding no nontrivial relations between the two graphs.

Before delving into the number of options for each forward step, we describe the permissible combinations of non-crossing steps away from and back toward the root in a recursive manner. We refer to such a combination as a *configuration*. We start by selecting the position of the backward step corresponding to the first forward step, and then proceed to fill in the gaps in between (which may be empty). In Figure 1, for instance, the choices for returning to the root corresponding to step 1 are either at step 4, as depicted in the first illustration, or at step 8, as depicted in the second and third ones. Our key observation is that calculating the options for this recursive process can be achieved using the recursive formula

$$B_k = \sum_{a+b+c=k-1} B_a B_b B_c, \tag{3.11}$$

where $B_0 = 1$, and $a, b, c \geq 0$ are the gaps to be filled after the choices of backward steps: $a$ is the one between the opening and the closing of the first $G_2$ step, $b$ is the gap between *closing* $G_2$ and closing $G_1$, and $c$ is the remaining walk after returning to the root. It is important to observe a subtlety in the correctness of Equation (3.11): the structure of the smaller instance to be solved might not resemble the original structure, as exemplified in $B_b$ of the second illustration in Figure 1. However, following a cyclic rotation, it appears identical, and the non-crossing nature of the pairings remains unaffected by such rotations.

The formula mentioned above bears a resemblance to the recursive formula for the Catalan

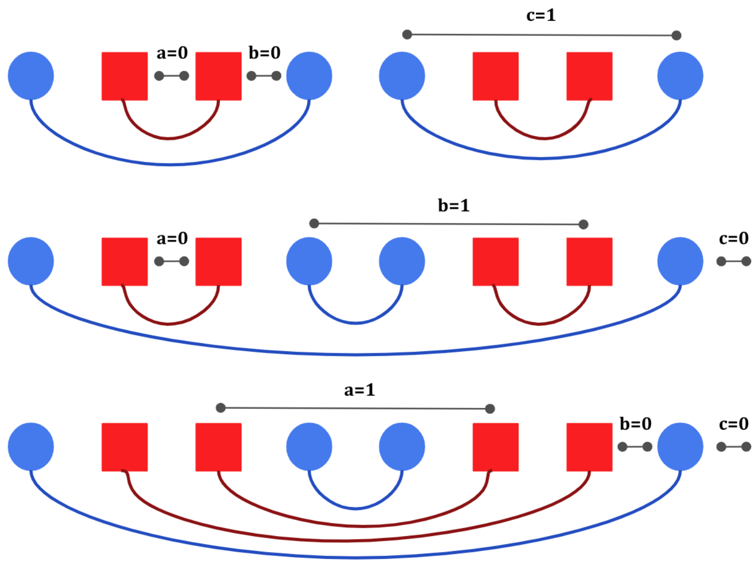


Figure 1: All configurations for length $k = 2$ closed walks in the graph $G = G_1 G_2^2 G_1$. The blue circles represent the steps from $G_1$, and the red squares represent $G_2$. Each *opening* of a pair is a step away from the root, where a closing is a step back towards it. The first 4 steps are the first step in $G$ split into steps in the original graphs, and similarly for the second step. The numbers $a, b, c$ correspond to the ones in Equation (3.11).

numbers, $C_k = \sum_{a+b=k-1} C_a C_b$. In fact, the sequence $(B_k)_k$ corresponds to a generalized version of the Catalan numbers, known as the *Fuss-Catalan numbers*. While the well-known closed form for the $k$-th Catalan number is typically expressed as $C_k = \frac{1}{k+1}\binom{2k}{k}$, we can write it in a slightly unorthodox manner as $C_k = \frac{1}{2k+1}\binom{2k+1}{k}$ to emphasize the connection with the generalization. Specifically, the closed form for $B_k$ is given by $B_k = \frac{1}{3k+1}\binom{3k+1}{k}$. In general, for values of $t$ greater than 2, the analysis of rotating expanders, and graph products in general, is intimately linked to the Fuss-Catalan numbers with an appropriate parameter $t$, and can be expressed as $\frac{1}{pk+1}\binom{pk+1}{k}$, where $p = t + 1$.

Having determined the number of configurations, our attention now shifts to the analysis of the number of cycles corresponding to any given configuration. The relationship between the number of cycles and the specific configuration is complex, rendering an exact count challenging. This complexity is reminiscent of the difficulties encountered when counting the number of cycles in $\mathcal{T}_d$ (see Section 3), although there it was to a lesser extent. To manage this in our previous discussion, we presumed the possibility of $d-1$ forward steps, disregarding instances—such as when tracing back to the root—where $d$ options are actually available. This approximation introduced a negligible error in the asymptotic analysis.

In a similar vein, for the current analysis, we posit a lower bound on the choices available at each recursive step. Given that the graphs are $d$-regular, typically one would have $d$ options to choose a forward neighbor. However, if two consecutive steps occur within the same graph (as depicted in the third configuration in Figure 1), the number of options is reduced to $d-1$.

Therefore, at each recursive step, we consider a product of $d(d-1)$, leading to an overall lower bound of $(d(d-1))^k$ for the number of cycles per configuration. This lower bound, combined with a precise estimate of the Fuss-Catalan numbers, culminates in the proof of Theorem 7.1.

# 4 Preliminaries

In this short section we give a formal treatment for the operation of derandomized squaring (see Section 4.1), and cover the essential background on the Cauchy transform (see Section 4.2). Finally, in Section 4.3 we discuss the trace method.

## 4.1 Derandomized squaring

Consider an edge-labeled $d$-regular graph $G$ on $n$ vertices, and let $H$ be a $c$-regular graph over the vertex set $\{1, 2, \dots, d\}$. The *derandomized square* of $G$ and $H$, denoted $G \circledS H$, is a $cd$-regular graph on the same vertex set as $G$. It is defined as follows: let $u$, $v$, and $w$ be vertices in $G$. If $u$ is the $i$-th neighbor of $v$, and $w$ is the $j$-th neighbor of $u$, then the edge $(v, w)$ exists in $G \circledS H$ if and only if $\{i, j\}$ is an edge in $H$. In simpler terms, the edges in $G \circledS H$ represent length-2 walks in $G$, where the first step is arbitrary, but the second step is constrained by the first step and the structure of $H$. This results in the edges being a subset of those in $G^2$, with $G \circledS H$ equal to $G^2$ when $H$ is $\mathrm{J}_d$, the complete graph on $d$ vertices with self-loops.

Is should be noted that $G \circledS H$ is not necessarily undirected. This depends on how the edges in $G$ are labeled. By an "edge-labeled graph", we simply mean that each vertex in $G$ assigns numbers $\{1, 2, \dots, d\}$ to its neighbors. For instance, a vertex $v$ might be the first neighbor for all its connecting vertices. This leads to the concept of *consistent* labeling, where each vertex receives $d$ distinct incoming labels. Under consistent labeling, $G \circledS H$ is in-regular. On the other hand, *undirected* labeling occurs when the labels for an edge $\{u, v\}$ are identical from both $u$ and $v$'s perspectives. In this case, $G \circledS H$ forms an undirected graph. This paper assumes undirected labeling for all graphs, though our results can extend to the consistent labeling scenario. We conclude by noting that $G$ has an undirected labeling exactly when it is the union of $d$ perfect matchings, each uniquely labeled.

## 4.2 The Cauchy transform

Let $p(x)$ be a degree $n$ real-rooted polynomial with roots $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. The *Cauchy transform* of $p(x)$ is defined as the function

$$\mathcal{G}_p(x) = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{x - \alpha_i} = \frac{1}{n} \cdot \frac{p'(x)}{p(x)}.$$

In many settings it is instructive to study the Cauchy transform as a function whose domain is $\mathbb{C}^+$. However, we will consider the Cauchy transform as a function on $\mathbb{R}$, where we evaluate the Cauchy transform to the right of its rightmost pole, at $x > \alpha_1$.

With $p(x)$ we associate the distribution $\mu_p$ that is uniform over its roots, namely, to sample from $\mu_p$ one first samples $i \in [n]$ uniformly at random and then returns $\alpha_i$. The Cauchy transform is closely related to the moments of this distribution. Indeed, it is easy to see that if $m_r(p)$ is the $r$-th moment of $\mu_p$, then for every $x > \alpha_1$ we have

$$\mathcal{G}_p(x) = \sum_{r=0}^{\infty} \frac{m_r(p)}{x^{r+1}}. \tag{4.1}$$

The reader is referred to Remark 2.19 in [NS06] for more details. Note that the Cauchy transform is defined for general distributions and not only for polynomials, but we will not need the general definition in this paper.

For a real symmetric matrix $\mathbf{A}$, we denote by $\mathcal{G}_{\mathbf{A}}(x)$ the Cauchy transform of the characteristic polynomial $\chi_x(\mathbf{A})$. In case where $\mathbf{A}_G$ is the adjacency matrix of a graph $G$, we write $\mathcal{G}_G(x)$ for $\mathcal{G}_{\mathbf{A}_G}(x)$. In this context, the roots of $\chi_x(\mathbf{A})$ are the eigenvalues of $\mathbf{A}$, and we may write

$$\mathcal{G}_{\mathbf{A}}(x) = \sum_{r=0}^{\infty} \frac{m_r(\mathbf{A})}{x^{r+1}}, \tag{4.2}$$

where $m_r(\mathbf{A}) = \frac{1}{d}\mathsf{Tr}(\mathbf{A}^r)$.

### 4.3 The trace method

In this short section, for completeness, we give a self-contained proof of the trace method, as used in our proofs. This is a standard tool that has numerous applications, including in the proofs of Friedman's theorem ([Fri08], [Bor20]). Our presentation closely follows the proof of the Alon-Boppana Theorem in Chapter 5 of [HLW06].

**Lemma 4.1.** *Let $G$ be a regular graph on $n$ vertices with diameter $\Delta(G)$, and let $k < \frac{\Delta(G)}{2}$. Assume that for every vertex $v$ in $G$ there are $C_k(G)$ cycles of length $k$ originating at $v$. Then,*

$$\lambda(G) \geq C_{2k}(G)^{\frac{1}{2k}}. \tag{4.3}$$

*Proof.* Let $\mathbf{A}$ be the adjacency matrix of $G$, and let $u$ and $v$ be vertices in $G$ of distance $D = \Delta(G)$. Denote $x = \frac{e_v - e_u}{\sqrt{2}}$, where $e_i$ is the vector with 1 at the $i$-th entry and is otherwise 0. Note that $x$ has unit length and is orthogonal to the all 1-s vector, denoted as $\mathbf{1}$. Therefore, the spectral theorem implies that

$$\lambda(G^{2k}) \geq x^{\mathsf{T}}\mathbf{A}^{2k}x = \frac{1}{2}\left((\mathbf{A}^{2k})_{uu} + (\mathbf{A}^{2k})_{vv} - 2(\mathbf{A}^{2k})_{uv}\right).$$

Since $k < \frac{\Delta(G)}{2}$ the last summand is 0. Note that $(\mathbf{A}^{2k})_{ww}$ counts the number of cycles of length $2k$ in $G$ which start and end at a vertex $w$, so we conclude that $\lambda(G^{2k}) \geq C_{2k}(G)$. The proof then follows as $\lambda(G^{2k}) = \lambda(G)^{2k}$. □

For an application of the above, we will assume that a lower bound on $C_k(G)$ is known, and that it has a specific form, dominated by an exponential component, which will turn out to be the most crucial ingredient for lower bounding the spectral expansion.

**Lemma 4.2.** *Let $F$ be a family of $d$-regular graphs such that for every graph $G \in F$ and every $k \geq 0$ we have that $(C_{2k}(G))^{\frac{1}{2k}} \geq \rho\,(1 - o_k(1))$ for some constant $\rho > 0$ that is independent of $G$ and $k$. Then, for every $G \in F$,*

$$\lambda(G) \geq (1 - o_n(1))\,\rho, \tag{4.4}$$

*where $n$ is the number of vertices of the graph $G$.*

*Proof.* By Lemma 4.1, we have that for $k = \frac{\Delta(G)-1}{2}$,

$$\lambda(G) \geq (C_{2k}(G))^{\frac{1}{2k}} \geq (1 - o_k(1))\,\rho.$$

We know that for an $n$-vertex graph, the diameter is at least $\log_d n$. Hence $\Delta(G) \to \infty$ as $n \to \infty$, which means that by picking $k(G) = \frac{\Delta(G)-1}{2}$ we get $\lambda(G) \geq (1 - o_n(1))\,\rho$. □

Using Lemma 4.2, one can lower bound the spectral expansion of the general family of $d$-regular graphs. Indeed, since the infinite $d$-ary tree $\mathcal{T}_d$ is a universal cover for any such graph, the number of cycles originating at any vertex is lower bounded by the number of cycles originating at the root in $\mathcal{T}_d$. Using our analysis from Section 3.1.1, in particular Equation (3.3), one gets the Alon-Boppana bound, as $\rho = 2\sqrt{d-1}$.

# 5 Limitations of Derandomized Squaring

In this section we prove our lower bound result for derandomized squaring, as presented in Theorem 2.1. In fact, we will prove its equivalent form, which is stated using the Cauchy transform, Theorem 2.2. From this, we will deduce the former as well as the recasting of the theorem as a minimization problem. The proof of Theorem 2.2 is structured around two primary components: Initially, in Section 5.1, we deduce the symbolic relation, paving the way to a functional equation that the associated generating function satisfies. Subsequently, in Section 5.2, we apply analytic combinatorics to approximate the generating function's coefficients. Finally, in Section 5.3, we establish the theorem's equivalent reformulations.

## 5.1 Deriving the symbolic relation

Recall that throughout, $H$ is a $c$-regular vertex-transitive graph on $d$ vertices, where $c \geq 1$ and $d \geq 3$. In order to formulate the symbolic construction, we start by considering the combinatorial class $\mathcal{S}_H$ of cycles in $H$ originating in some fixed vertex $v$ of $H$ that only revisit $v$ upon completing a cycle. We exclude the empty cycle from the class.

As discussed in Section 3.1.1, where we counted cycles in $\mathcal{T}_d$, the symbolic method handles the infinite tree with one pruned branch more straightforwardly than it does the full infinite tree. Let us designate a root, denoted as $v$, for $\mathcal{T}_d$. To specify a symbolic construction of cycles from $v$ to itself, we want each vertex to have $d-1$ options for moving away from the root. This holds true for all vertices except the root itself, which has $d$ such options. Therefore, we remove a single edge adjacent to the root, disconnecting the infinite tree but merely reducing the number of cycles from

$v$ to itself. The class of cycles in this graph can be characterized using the symbolic constructions outlined in Equation (3.1) and Equation (3.4).

In our graph $\mathcal{T}_d \circledS H$, we employ a similar technique. We designate a root, also denoted as $v$, for $\mathcal{T}_d \circledS H$, where, like all vertices, it participates in $d$ copies of $H$. We initiate the process by removing the edges from a single copy of $H$ that are connected to $v$, disconnecting the graph $\mathcal{T}_d \circledS H$ and reducing the number of cycles from $v$ to itself (Similar to the case of $\mathcal{T}_d$, we expect this change to be negligible as the cycle lengths increase. Indeed, our bound will prove to be asymptotically tight, as shown in Section 6). We abuse notation slightly and use the notation $\mathcal{T}_d \circledS H$ for both the derandomized squaring of $\mathcal{T}_d$ and $H$, as well as for the truncated version described above, where the correct interpretation will always be clear from context. We count cycles in the truncated version and subsequently derive our lower bound for the non-truncated version. With the truncated version of $\mathcal{T}_d \circledS H$ and the generating function of $\mathcal{S}_H$ at hand, we have all we need for the description of the class $\mathcal{C}_{\mathcal{T}_d \circledS H}$ of non-empty cycles in $\mathcal{T}_d \circledS H$.

**Lemma 5.1.** *The class $\mathcal{C}_{\mathcal{T}_d \circledS H}$ of non-empty cycles originate at the root of $\mathcal{T}_d \circledS H$ satisfies the symbolic relation*

$$\mathcal{C}_{\mathcal{T}_d \circledS H} = \{1, \ldots, d-1\} \times \left(\mathcal{S}_H \circ \left(\rightarrow \times \left(\mathcal{C}_{\mathcal{T}_d \circledS H} + \epsilon\right)\right)\right).$$

*Proof.* En route to the symbolic relation, one needs the following observation: for every non-empty cycle in $\mathcal{T}_d \circledS H$ starting at $v$, one can identify uniquely a neighbor $u_i$ of $v$ in $\mathcal{T}_d$, and a cycle in $H$, from which the cycle begins (see example in Figure 2). That is, if the first step is $v \to w$, it means that there exists a vertex $u_i \in \mathcal{T}_d$ such that the edges $\{v, u_i\}$ and $\{u_i, w\}$ are in $\mathcal{T}_d$. Moreover, in order to get back to $v$ for the first time, one has to complete a cycle in the copy of $H$ which is induced by the vertex $u_i$. In order to identify this cycle uniquely, this has to be a cycle returning to its root exactly once.

There are $d-1$ choices to pick the vertex $u_i$ (and the copy of $H$ surrounding it), and the class $\mathcal{S}_H$ described at the beginning of this section represents the cycles returning to the root only upon completion. Once $u_i$ and the cycle $c$ in $H$ were chosen, there are still many options for closing cycles in $\mathcal{T}_d \circledS H$: after each step in $c$, which is represented by the atom $\rightarrow$, there is an option to start a nested cycle from the vertex within the copy of $H$. As we have truncated one copy of $H$ from the original vetrex when defining $\mathcal{C}_{\mathcal{T}_d \circledS H}$, and due to vertex transitivity, the nested cycle can also be described as $\mathcal{C}_{\mathcal{T}_d \circledS H}$. Therefore, the composition of $\mathcal{S}_H$ is with either $\mathcal{C}_{\mathcal{T}_d \circledS H}$, which is defined to be non-empty, or with $\epsilon$, representing the choice of not going through a nested cycle. $\square$

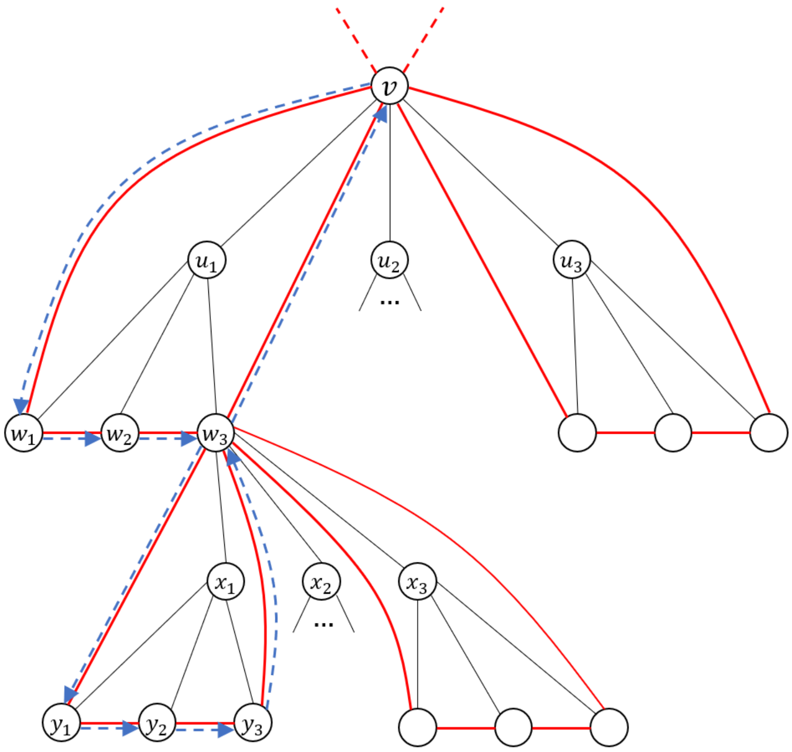


Figure 2: Cycles in $\mathcal{T}_4 \circledS C_4$. The black edges represent the edges of $\mathcal{T}_4$, while the red edges represent those of $\mathcal{T}_4 \circledS C_4$. Dashed red edges indicate the truncated edges. Edges that are irrelevant to the cycles of $v$ (e.g., $(u_1, x_1)$) have not been included in the figure. The blue cycle within $\mathcal{T}_4 \circledS C_4$ corresponds to the cycle $(v \to w_1 \to w_2 \to w_3 \to v)$ within the copy of $H$ centered around vertex $u_1$. In this cycle, the first, second, and last steps are substituted with the pair $(\to, \epsilon)$, while the third step is substituted with the pair $\left(\to, c\right)$, where $c$ represents a nested cycle from $\mathcal{C}_{\mathcal{T}_d \circledS H}$ (specifically, $c = (w_3 \to y_1 \to y_2 \to y_3 \to w_3)$).

### 5.2 Coefficients approximation via analytic combinatorics

Using the symbolic construction in Lemma 5.1, we immediately derive a functional equation that is satisfied by the generating function of $\mathcal{C}_{\mathcal{T}_d \circledS H}$, namely,

$$C_{\mathcal{T}_d \circledS H}(z) = (d-1)S_H\left(z\left(C_{\mathcal{T}_d \circledS H}(z) + 1\right)\right). \tag{5.1}$$

By introducing the functions

$$\zeta_H(z) = z\left(C_{\mathcal{T}_d \circledS H}(z) + 1\right),$$
$$\phi_H(z) = 1 + (d-1)S_H(z),$$

we can write Equation (5.1) as

$$\zeta_H(z) = z \cdot \phi_H(\zeta_H(z)). \tag{5.2}$$

The next step in the proof goes through asymptotic coefficients estimation of $\zeta_H(z)$, and hence of $C_{\mathcal{T}_d \circledS H}(z)$. For this, we introduce a deep result from analytic combinatorics. We start by giving the formal definition of smooth inverse-function schema which was informally discussed in Section 3.1.3.

**Definition 5.2** (Definition VII.3 in [FS09])**.** A function $\zeta(z)$ that is analytic at 0 is said to belong to the *smooth inverse-function schema* if there exists a function $\phi(u)$ analytic at 0 such that in the neighborhood of 0 one has $\zeta(z) = z \cdot \phi(\zeta(z))$, and $\phi(u)$ satisfies the following conditions:

1. The function $\phi(u)$ is such that $\phi(0) \neq 0$, $[u^n]\ \phi(u) \geq 0$ for all $n \in \mathbb{N}$, and $\phi(u)$ is not of the form $\phi_0 + \phi_1 u$.

2. Within the open disc of convergence of $\phi$ at 0, $|z| < R$, there exists (a necessarily unique [5]) positive solution to the *characteristic equation*, $\phi(u) = u \cdot \phi'(u)$.

A combinatorial class whose generating function satisfies these conditions is also said to belong to the *smooth inverse-function schema*.

Our main technical work, captured by Claim 5.3 below, is in establishing that $\zeta_H(z)$ belongs to the above schema.

**Claim 5.3.** *The function $\zeta_H(z)$ belongs to the smooth inverse-function schema.*

To prove Claim 5.3 we first establish the following claim which relates the Cauchy transform of $H$ with the generating function of $\mathcal{S}_H$.

**Claim 5.4.** *The generating function of $\mathcal{S}_H$, denoted as $S_H(z)$, satisfies*

$$S_H(z) = 1 - \frac{1}{\frac{1}{z}\mathcal{G}_H(\frac{1}{z})}.$$

*Proof.* The combinatorial class $\mathcal{C}_H$ of arbitrary cycles originate at some fixed vertex $v$ of $H$ is related to the class $\mathcal{S}_H$ by $\mathcal{C}_H = \mathsf{SEQ}(\mathcal{S}_H)$. Indeed, any nonempty cycle is a sequence of cycles returning to $v$ exactly once, and the empty cycle is correctly captured by the $\mathsf{SEQ}$ construct. The relation between the generating functions of $\mathcal{C}_H$ and $\mathcal{S}_H$ is thus given by $C_H(z) = \frac{1}{1-S_H(z)}$, or equivalently, $S_H(z) = 1 - \frac{1}{C_H(z)}$. Therefore, it suffices to prove that $C_H(z) = \frac{1}{z}\mathcal{G}_H(\frac{1}{z})$. To this end, note that $C_H(z)$ can also be written as

$$C_H(z) = e_v^{\mathsf{T}}(\mathbf{I} - z\mathbf{H})^{-1}e_v = \frac{1}{d}\,\mathsf{Tr}\left((\mathbf{I} - z\mathbf{H})^{-1}\right),$$

where $e_v$ denotes the vector satisfying $(e_v)_u = 0$ for all $u \neq v$ and $(e_v)_v = 1$. Now,

$$\mathcal{G}_H(x) = \frac{1}{d}\sum_{i=1}^{d}\frac{1}{x-\lambda_i} = \frac{1}{d}\,\mathsf{Tr}\left((x\mathbf{I} - \mathbf{H})^{-1}\right) = \frac{1}{xd}\,\mathsf{Tr}\left((\mathbf{I} - x^{-1}\mathbf{H})^{-1}\right).$$

Substituting $x = \frac{1}{z}$, we see that $C_H(z) = \frac{1}{z}\mathcal{G}_H(\frac{1}{z})$, which completes the proof. ☐

[5]The uniqueness of the solution to the characteristic equation, if it at all exists, can be proven in general and the definition we state here utilizes this result. We also make use of this general result, which "hides" under the definition (or more accurately, definition-theorem). It should be noted that in our specific case, the uniqueness can be directly proven with some effort.

*Proof of Claim 5.3.* For condition (2), we need to show that $\phi_H(u)$ is analytic at a neighborhood of 0, and has a convergence radius, denoted $R$, in which the characteristic equation, $\phi_H(u) = u \cdot \phi'_H(u)$ has a solution. To do so, we combine the definition of $\phi_H(u)$ with Claim 5.4 to get

$$\phi_H(u) = 1 + (d-1) \cdot \left(1 - \frac{1}{\frac{1}{u}\mathcal{G}_H(\frac{1}{u})}\right) = d - \frac{d(d-1)}{\sum_{i=1}^{d} \frac{1}{1-u\lambda_i}}.$$

Observe that the radius of convergence of $\phi_H(u)$ hinges on the poles and zeros of the denominator's expression appearing on the RHS, $f(u) = \sum_{i=1}^{d} \frac{1}{1-u\lambda_i}$. Starting with the poles, by the Perron–Frobenius Theorem, and since $H$ is $c$-regular, $\max_i(|\lambda_i|) = \lambda_1 = c$. Consequently, $f(u)$ has no poles in $(-\frac{1}{c}, \frac{1}{c})$. As for the zeros of $f(u)$, note that $f$ vanishes at a point $u_0$ if and only if $\mathcal{G}_H(\frac{1}{u_0}) = 0$. Since $\mathcal{G}_H(w) = \frac{1}{d} \cdot \frac{\chi'_H(w)}{\chi_H(w)}$ and as the zeros of the derivative $\chi'_H(w)$ interlace with the zeros of $\chi_H(w)$, all zeros of $\mathcal{G}_H(w)$ are in the interval $[\lambda_d, \lambda_1] \subseteq [-c, c]$. Therefore, if $\mathcal{G}_H(\frac{1}{u_0}) = 0$ then $\left|\frac{1}{u_0}\right| \le c$, hence $|u_0| \ge \frac{1}{c}$, and so $f(u)$ does not vanish in $(-\frac{1}{c}, \frac{1}{c})$. The above leads to the conclusion that $\phi_H(u)$-s radius of converges is $R = \frac{1}{c}$.

We wish now to prove that there exists a positive solution to the characteristic equation $\phi_H(u) = u \cdot \phi'_H(u)$ within this radius of convergence, namely, a solution in $(0, \frac{1}{c})$. Working out the derivatives, the characteristic equation takes the form

$$d - \frac{(d-1)u}{\mathcal{G}_H(\frac{1}{u})} = -(d-1)\frac{u\mathcal{G}_H(\frac{1}{u}) + \mathcal{G}'_H(\frac{1}{u})}{\mathcal{G}_H(\frac{1}{u})^2}.$$

As we wish to find a solution $u \in (0, \frac{1}{c})$ to the above equation, and since it has been established that $\mathcal{G}_H(\frac{1}{u})$ does not vanish within this interval, an equivalent task is to find a value $u$ in this interval such that

$$d\mathcal{G}_H\left(\frac{1}{u}\right)^2 + (d-1)\mathcal{G}'_H\left(\frac{1}{u}\right) = 0.$$

Substituting $x = \frac{1}{u}$, it suffices to find a solution $x_0 \in (c, \infty)$ to the equation

$$\frac{d}{d-1}\mathcal{G}_H(x)^2 + \mathcal{G}'_H(x) = 0. \tag{5.3}$$

Rewriting Equation (5.3) using the definition of the Cauchy transform, we get

$$\left(\sum_{i=1}^{d} \frac{1}{x-\lambda_i}\right)^2 = (d-1)\sum_{i=1}^{d} \frac{1}{(x-\lambda_i)^2}. \tag{5.4}$$

Assume that the eigenvalue $\lambda_1 = c$ appears in the spectrum of $H$ with multiplicity $r$. For every $\varepsilon \ge 0$ define

$$\Delta_1(\varepsilon) = \sum_{i=r+1}^{d} \frac{1}{c+\varepsilon-\lambda_i},$$

$$\Delta_2(\varepsilon) = \sum_{i=r+1}^{d} \frac{1}{(c+\varepsilon-\lambda_i)^2},$$

and denote $\Delta_1 = \Delta_1(0)$ and $\Delta_2 = \Delta_2(0)$. With this, scaling Equation (5.4) by $\varepsilon^2$ and substituting $x = c + \varepsilon$, we have that

$$\varepsilon^2 \left( \sum_{i=1}^{d} \frac{1}{c + \varepsilon - \lambda_i} \right)^2 = \left( r + \varepsilon \Delta_1(\varepsilon) \right)^2,$$

and

$$\varepsilon^2 (d-1) \sum_{i=1}^{d} \frac{1}{(c + \varepsilon - \lambda_i)^2} = (d-1) \left( r + \varepsilon^2 \Delta_2(\varepsilon) \right).$$

Now,

$$\lim_{\varepsilon \to 0^+} \left( r + \varepsilon \Delta_1(\varepsilon) \right)^2 = r^2,$$

and

$$\lim_{\varepsilon \to 0^+} (d-1) \left( r + \varepsilon^2 \Delta_2(\varepsilon) \right) = (d-1) r.$$

We will argue next that $r < d - 1$. With this in mind, for a sufficiently small $\varepsilon > 0$, the LHS of Equation (5.4) is strictly smaller than the RHS.

On the other hand, using a similar argument it can be shown that as $x \to \infty$, the LHS of Equation (5.4) is strictly larger than the RHS. Indeed, for a large $x$, the LHS is roughly $(\frac{d}{x})^2$ whereas the RHS is roughly $\frac{d(d-1)}{x^2}$. Thus, as the functions that appear on both sides of Equation (5.4) are continuous in the domain $(c, \infty)$, there exists $x_0 \in (c, \infty)$ satisfying Equation (5.3).

To complete the proof, we show that $r < d - 1$. To see this note that per our assumption $c \geq 1$, the graph $H$ contains at least one edge and so, due to the additional assumption of vertex transitivity, the number of connected components is at most $\frac{d}{2}$. It is well-known that the number of connected components equals to the multiplicity $r$ of the largest eigenvalue, $c$. Hence, $r \leq \frac{d}{2}$. The proof then follows as the latter is bounded by $d - 1$ per our assumption $d \geq 3$. □

**Remark.** We record here the fact that, by the above proof, the solution $x_0$ to Equation (5.3) satisfies $x_0 > c$. This will be used when we will come to deduce Theorem 2.1 in Section 5.3.

Now that we have established that $\zeta_H(z)$ conforms to the smooth inverse-function schema, we are almost ready to invoke Theorem 5.6 which is stated below. There is only one additional technical assumption regarding the periodicity of $\phi_H(u)$ which we need to handle.

**Definition 5.5** (Definition IV.5 in [FS09])**.** *For a sequence $(f_n)$ with a generating function $f(z)$, the* support *of $f$, denote* Supp$(f)$*, is the set of all integers $n \geq 0$ such that $f_n \neq 0$. The sequence $(f_n)$ as well as its generating function $f(z)$, is said to admit a* span *$d$ if for some $r$, it holds that*

$$\mathrm{Supp}(f) \subseteq r + d\mathbb{N} = \{r, r + d, r + 2d, \ldots\}.$$

*The largest span, $p$, is the* period*, all other spans being divisors of $p$. If the period is equal 1, the sequence and its generating function are said to be* aperiodic*.*

**Theorem 5.6** (Theorem VII.2 in [FS09])**.** Let $\zeta(z)$ belong to the smooth inverse-function schema and the associated $\phi(u)$ be aperiodic. Then, with $\tau$ the positive root of the characteristic equation $\phi(u) = u \cdot \phi'(u)$, one has

$$\left[z^k\right] \zeta(z) = \left( 1 + O\left( \frac{1}{k} \right) \right) \sqrt{\frac{\phi(\tau)}{2\pi \cdot \phi''(\tau)}} \cdot \frac{\phi'(\tau)^k}{\sqrt{k^3}}. \tag{5.5}$$

The issue with applying Theorem 5.6 to our situation arises from the possibility that our function $\phi_H(u)$ might exhibit periodic behavior. Recall that $\phi_H(u) = 1+(d-1)S_H(u)$, where the coefficients of $S_H(u)$ enumerate cycles of $H$. Consequently, the only nontrivial periodicity that $\phi_H(u)$ could possess is 2, which occurs whenever the graph $H$ is bipartite. In Corollary 5.7 below, we demonstrate a method to circumvent this issue specifically for functions with a period of 2. Nevertheless, the provided proof can be easily extended to any period $p \geq 2$.

**Corollary 5.7.** *Let $\zeta(z)$ belong to the smooth inverse-function schema with respect to a function $\phi(u)$. Assume that $\phi(u)$ has periodicity at most 2. Let $\tau$ be the positive solution to the characteristic equation $\phi(u) = u \cdot \phi'(u)$. Then,*

$$\left(\left[z^k\right] \zeta(z)\right)^{\frac{1}{k}} = (1 - o_k(1))\, \phi'(\tau). \tag{5.6}$$

*Proof.* If $\phi(u)$ is aperiodic, this is a direct implication of Theorem 5.6. Hence we are left with the case of periodicity 2. According to Definition 5.5, a function with period 2 can be written as $\phi(u) = u^r \cdot \psi(u^2)$, for some aperiodic function $\psi(u)$ and integer $r \geq 0$. Taking into account our additional condition $\phi(0) \neq 0$, we have that $\phi(u) = \psi(u^2)$.

Define $\Phi(u) = \psi(u)^2$ and let $Z = z^2$. We wish to look at the functional equation

$$U = Z \cdot \Phi(U) \tag{5.7}$$

in the undetermined $U$. Recall that $\zeta(z)$ is a solution to the function equation $u = z \cdot \phi(u)$, and so $U = \zeta(z)^2$ is a solution to the functional equation given by Equation (5.7). Indeed,

$$\zeta(z)^2 = z^2 \cdot \phi\left(\zeta(z)\right)^2 = Z \cdot \psi\left(\zeta(z)^2\right)^2 = Z \cdot \Phi\left(\zeta(z)^2\right).$$

Since Equation (5.7) is a functional equation of power series in the variable $Z$, we conclude that $\zeta(z)^2$ can be written as a power series in $Z$. We denote this power series by $Y(Z) = \zeta(z)^2$.

As $\psi(u)$ is aperiodic and since it has non-negative coefficients and a non-zero constant term, we have that $\Phi(U)$ is also aperiodic. Our next step is to invoke Theorem 5.6, while using the pair of functions $Y(Z)$ and $\Phi(U)$ rather than $\zeta(z)$ and $\phi(u)$. For doing so, we need to assert that the pair $Y(Z)$, $\Phi(U)$ satisfies the conditions for the smooth inverse-function schema as well. Asserting that $\Phi(U)$ has only non-negative coefficients, does not vanish at 0 and is not of the form $\Phi_0 + \Phi_1 U$, is immediate from its definition and the fact that $\phi(u)$ satisfies the same conditions. Hence, we are left with showing that there exists a solution $\rho > 0$ to the characteristic equation

$$\Phi(U) = U \cdot \Phi'(U) \tag{5.8}$$

within $\Phi(U)$-s radius of convergence. Given that $\tau > 0$ is a solution for the original characteristic equation $\phi(u) = u \cdot \phi'(u)$, we claim that $\rho = \tau^2$ solves Equation (5.8). Before proceeding to showing that, we note that since $\tau$ is within $\phi(u)$-s radius of convergence, then $\rho$ is within $\Phi(U)$-s radius of convergence. Now, using the definition of $\Phi(U)$ we have that solving Equation (5.8) is equivalent to solving

$$\psi(u) = 2u \cdot \psi'(u). \tag{5.9}$$

Since $\tau$ solves the original characteristic equation, and

$$\phi'(\tau) = \frac{d}{du}\psi(u^2)\Big|_{\tau} = 2\tau \cdot \psi'(\tau^2), \tag{5.10}$$

we have that

$$\psi(\tau^2) = \phi(\tau) = \tau \cdot \phi'(\tau) = \tau \cdot 2\tau \cdot \psi'(\tau^2) = 2\tau^2 \cdot \psi'(\tau^2), \tag{5.11}$$

namely, $\tau^2$ is a solution to Equation (5.9).

We can now proceed by invoking Theorem 5.6 to conclude that

$$\left[Z^k\right] Y(Z) = \left(1 + O\left(\frac{1}{k}\right)\right) \sqrt{\frac{\Phi(\rho)}{2\pi \cdot \Phi''(\rho)}} \cdot \frac{\Phi'(\rho)^k}{\sqrt{k^3}}, \tag{5.12}$$

where $\rho = \tau^2$. Following a similar argument, we get that $\Phi'(\rho) = \phi'(\tau)^2$. Indeed,

$$\Phi'(\rho) = 2\psi(\rho)\psi'(\rho) = 4\rho \cdot \psi'(\rho)^2 = \phi'(\tau)^2,$$

where the penultimate equality follows by Equation (5.9) and the last equality follows by Equation (5.10). Thus, we can rewrite Equation (5.12) as

$$\left[Z^k\right] Y(Z) = \Theta\left(\frac{1}{\sqrt{k^3}}\right) \cdot \phi'(\tau)^{2k}.$$

As $Y(Z) = \zeta(z)^2$ and since $Z = z^2$, we have that $\left[z^{2k}\right] \zeta(z)^2 = c_{2k} \cdot \phi'(\tau)^{2k}$, where $c_{2k} = \Theta\left(\frac{1}{\sqrt{k^3}}\right)$. Furthermore, as $\zeta(z)^2 = Y(Z) = Y(z^2)$, the coefficient of every odd power, $c_{2k+1}$, in $\zeta(z)^2$ vanishes.

To conclude the proof, we need to argue about the coefficients of $\zeta(z)$ given our knowledge on the coefficients of $\zeta(z)^2$. This calls for the application of a (discrete) Fourier transform. The somewhat technical Claim 5.8 that follows will finalize our proof.

**Claim 5.8.** $[z^k]\,\zeta(z) = \Theta(\phi'(\tau)^k)$.

*Proof.* We start by recalling some basic results on discrete Fourier transform. Given an integer $N$ and a sequence $t_0, t_1, \ldots, t_N$ we define, for $k = 0, 1, \ldots, N$,

$$\widehat{t}_k = \sum_{n=0}^{N} t_n \cdot e^{-\frac{2\pi i}{N+1}kn}. \tag{5.13}$$

It is well-known that for every $n = 0, 1, \ldots, N$,

$$t_n = \frac{1}{N+1}\sum_{k=0}^{N} \widehat{t}_k \cdot e^{\frac{2\pi i}{N+1}kn}. \tag{5.14}$$

Moreover, one has the convolution theorem which when applied to the same sequence $t$ as above yields $\widehat{t * t} = \widehat{t}^2$. Returning to our proof, let $f_k = [z^k]\,\zeta(z)$ and write $f_k$ as $x_k \cdot \phi'(\tau)^k$. With this, it suffices to prove that $x_k = \Theta(1)$. We have that for every $N \geq 0$,

$$c_N \cdot \phi'(\tau)^N = [z^N]\,\zeta(z)^2 = \sum_{k=0}^{N} (x_k \cdot \phi'(\tau)^k) \cdot (x_{N-k}\phi'(\tau)^{N-k}),$$

and so, as $\phi'(\tau) \neq 0$, $c_N = \sum_{k=0}^{N} x_k x_{N-k}$. Put differently, the sequences $c = (c_0, c_1, \ldots, c_N)$ and $x = (x_0, x_1, \ldots, x_N)$ satisfy $c = x * x$, therefore $\widehat{c} = \widehat{x}^2$. By Equation (5.13), for every $N \geq 0$,

$$\widehat{c}_N = \sum_{n=0}^{N} c_n \cdot e^{-\frac{2\pi i}{N+1} nN} = \sum_{n=0}^{N} c_n \cdot e^{\frac{2\pi i}{N+1} n} = \Theta\left(\sum_{n=1}^{N} \frac{1}{\sqrt{n^3}} \cdot e^{\frac{2\pi i}{N+1} n}\right).$$

As the RHS, thought of as a sequence indexed by $N$, converge absolutely, it approaches some universal constant as $N \to \infty$, and so in particular, $\widehat{x}_N = \sqrt{\widehat{c}_N} = \Theta(1)$. This, together with Equation (5.14), implies that $x_N = \Theta(1)$, completing the proof.

□

This concludes the proof of Corollary 5.7 for the case of $\phi(z)$ with period 2.

□

Now that we have the symbolic characterization of cycles in the derandomized squaring operation (Section 5.1), as well as the analytic tools to analyze them (Section 5.2 so far), we are ready to tie it all together and prove Theorem 2.2.

*Proof of Theorem 2.2.* As shown in Lemma 5.1, the generating function $C_{\mathcal{T}_d \circledS H}(z)$ describing the cycles in $\mathcal{T}_d \circledS H$ is the one satisfying Equation (5.1). Its coefficients lower bound the number of cycles in $G \circledS H$ for every $d$-regular graph $G$. Let $x_0$ be the solution to Equation (5.3), and recall that $z_0 = \frac{1}{x_0}$. By Corollary 5.7, and noting that by definition $C_{\mathcal{T}_d \circledS H}(z) = \frac{\zeta_H(z)}{z} - 1$, the $k$-th root of the number of cycles of length-$k$ is bounded from below by $(1 - o_k(1))\,\Lambda_H$, where

$$\Lambda_H = \phi_H'(z_0) = \frac{\phi_H(z_0)}{z_0} = x_0 \cdot \phi_H\left(\frac{1}{x_0}\right) = dx_0 - \frac{d-1}{\mathcal{G}_H(x_0)}.$$

Applying the trace method as given in Lemma 4.2 we have that $\lambda(G \circledS H) > \Lambda_H - o_n(1)$, $n$ being the number of vertices in $G$. □

### 5.3 Proof of the statements equivalent to Theorem 2.1

We conclude this section by deriving Theorem 2.1 and our reformulation of that theorem as a minimization problem, which is formally stated in Theorem 5.9 below.

*Proof of Theorem 2.1.* Recall that $\mathcal{G}_H(x) = \frac{1}{d} \frac{\chi_x'(H)}{\chi_x(H)}$. Working out the derivatives, Equation (2.4) takes the form

$$\frac{(d-1)\chi_x''(H)\chi_x(H) - (d-2)\chi_x'(H)^2}{\chi_x(H)^2} = 0.$$

By the remark following the proof of Claim 5.3, the above equation has a solution $x_0 > c$. Since $\chi_x(H)$ does not vanish in the domain $(c, \infty)$, we have that $x_0$ is a real positive root of the polynomial appearing in the enumerator, namely, it is a solution to Equation (2.1). The proof then follows since $\Lambda_H$ as given in Equation (2.2) is equal to its definition as given in Equation (2.5). □

**Theorem 5.9** (Recasting Theorem 2.1 as a minimization problem)**.** *Let $H$ be a vertex-transitive $c$-regular graph on $d \geq 3$ vertices, where $c \geq 1$. Then,*

$$\Lambda_H = \min_{x>c} dx - \frac{d-1}{\mathcal{G}_H(x)}.$$

*Proof.* Letting $\psi_H(x) = dx - \frac{d-1}{\mathcal{G}_H(x)}$, we have that

$$\psi'_H(x) = d + (d-1)\frac{\mathcal{G}'_H(x)}{\mathcal{G}_H(x)^2}.$$

Using the fact that $\mathcal{G}_H(x)$ does not vanish in $(c, \infty)$, which was established in the proof of Claim 5.3, this expression vanishes exactly at the solutions of Equation (2.4). Hence, by Theorem 2.2, there is a unique positive solution $x_0$ to the equation $\psi'_H(x) = 0$. By the remark following the proof of Claim 5.3, we have that $x_0 > c$. To see that $x_0$ is in fact a minimizer of $\psi_H(x)$ note that $\mathcal{G}_H(x)$ and its first two derivatives are continuous in the domain $(c, \infty)$ and that $\mathcal{G}'_H(x)$ strictly increases in the interval $(c, \infty)$. On the other hand, $\mathcal{G}_H(x)^2$ strictly decreases in that interval, hence $\psi'_H(x)$ strictly increases in $(c, \infty)$ and so $\psi''_H(x_0) > 0$. ☐

# 6 Matching the Lower Bound with $H$-Local Graphs

Let $H$ be a $c$-regular graph on $d \geq 3$ vertices, where $c \geq 1$. In this section, we prove Theorem 2.3, which establishes the existence of an infinite family of $cd$-regular $H$-local graphs. The spectra of these graphs are upper bounded by the same bound as outlined in Theorem 2.1.

**Definition 6.1.** *Let $H$ be a $c$-regular graph on $d \geq 3$ vertices, where $c \geq 1$. A $cd$-regular graph $G = (V, E)$ is said to be $H$-local if for every vertex $v \in V$, there exist subgraphs $\{G_i^v = (V_i^v, E_i^v)\}_{i=1}^d$ of $G$ such that for every $i \in [d]$, $v \in V_i^v$ and $G_i^v$ is isomorphic to $H$, and for every $i \neq j \in [d]$, $E_i^v \cap E_j^v = \emptyset$.*

Informally, this definition can be thought of as saying that every vertex participating in a *local view* of $d$ instances of $H$. As mentioned in Section 2, all graphs of the form $G \circledS H$ are $H$-local, however there are $H$-local graphs which are not a result of a derandomized square operation.

**Theorem 6.2** (Restatement of Theorem 2.3)**.** *Let $c \geq 1$ and $d \geq 3$ be integers. For every $c$-regular vertex-transitive graph $H$ on $d$ vertices, and for every integer $n \geq 1$, there exists an $H$-local graph $X_n$ on $nd$ vertices such that*

$$\lambda_2(X_n) \leq \min_{x>c}\left(dx - \frac{d-1}{\mathcal{G}_H(x)}\right). \tag{6.1}$$

To prove Theorem 6.2, we introduce a suitable distribution over $dc$-regular graphs. This distribution allows us to apply finite free probability techniques, as outlined in Section 3.2, along with the method of polynomial interlacing. Our approach is inspired by [MSS18], where these techniques were initially developed to establish the existence of bipartite Ramanujan graphs of every size and every degree. Our proof can be viewed as a fairly straightforward generalization of this earlier result. To prove Theorem 6.2, we define the graph $\mathcal{H}$, which is constructed from disjoint copies of the graph $H$. This serves an analogous role to the perfect matching graph used in [MSS18]. The latter can be considered a special case when $H$ is a single-edge graph, corresponding to $d = 2$ and $c = 1$.

### 6.1 Bounding the roots of the expected characteristic polynomial

We recall some general tools for the analysis of the Cauchy transform $\mathcal{G}_p(x)$ and its max-inverse, $\mathcal{K}_p(x)$ as defined in Section 3.2. With the definitions and notations from that section, we state the following theorem which generalizes Theorem 3.3 slightly to general polynomials.

**Theorem 6.3** (Theorem 1.12 in [MSS22])**.** *For real-rooted polynomials $p$ and $q$ of the same degree, and for any $y > 0$,*

$$\mathcal{K}_{p \boxplus q}(y) \leq \mathcal{K}_p(y) + \mathcal{K}_q(y) - \frac{1}{y}.$$

We deduce the following corollary which slightly generalizes a technique used in Chapter 5 of [MSS18].

**Corollary 6.4.** *Let $p$ be a degree $d$ real-rooted polynomial with largest root $\lambda_1$. Assume that the multiplicity of $\lambda_1$ in $p$ is at most $\frac{d}{2}$. For an integer $r \geq 3$ let $p^{\boxplus r}$ be the additive convolution of $p$ with itself $r$ times. Then,*

$$\mathsf{maxroot}\left(p^{\boxplus r}\right) \leq \min_{x > \lambda_1} \left(rx - \frac{r-1}{\mathcal{G}_p(x)}\right).$$

*Proof.* By invoking Theorem 6.3 for $r - 1$ times we get that for every $y > 0$,

$$\mathcal{K}_{p^{\boxplus r}}(y) \leq r\mathcal{K}_p(y) - \frac{r-1}{y}.$$

Since any value of $\mathcal{K}_{p^{\boxplus r}}(y)$ is an upper bound on the roots of $p$, we have that

$$\mathsf{maxroot}\left(p^{\boxplus r}\right) \leq \inf_{y>0} \left(r\mathcal{K}_p(y) - \frac{r-1}{y}\right).$$

Recall that $\mathcal{K}_p : (0, \infty) \to (\lambda_1, \infty)$ is the max-inverse, under composition, of $\mathcal{G}_p$, and observe it is onto. Thus, given $y > 0$ there is an $x > \lambda_1$ such that $y = \mathcal{G}_p(x)$, and so we can write the above equation as

$$\mathsf{maxroot}\left(p^{\boxplus r}\right) \leq \inf_{x>\lambda_1} \left(r\mathcal{K}_p(\mathcal{G}_p(x)) - \frac{r-1}{\mathcal{G}_p(x)}\right) = \inf_{x>\lambda_1} \left(rx - \frac{r-1}{\mathcal{G}_p(x)}\right).$$

To complete the proof, we show that the infimum appearing on the RHS is in fact a minimum. Let $f(x) = rx - \frac{r-1}{\mathcal{G}_p(x)}$ be the function appearing in the infimum. Since $f(x)$ is continuous in $(\lambda_1, \infty)$, it suffices to show that in a small right-neighborhood of $\lambda_1$, the function $f(x)$ decreases, and that $\lim_{x\to\infty} f(x) = \infty$. We provide only a sketch of the proof here, though the details can be completed in a manner similar to the formal argument presented in the proof of Claim 5.3.

In a small neighborhood to the right of $\lambda_1$, $\mathcal{G}_p(x)$ is approximated by $\frac{m}{d}\frac{1}{x-\lambda_1}$, where $m$ denotes the multiplicity of $\lambda_1$ as a root of $p$. Thus, $f(x)$ is approximated by

$$\left(r - \frac{(r-1)d}{m}\right)x + \frac{(r-1)\lambda_1 d}{m}.$$

Per our assumption, $m \leq \frac{d}{2}$ and so, together with the hypothesis $r \geq 3$, the coefficient of $x$ in the above expression is negative, and so in a sufficiently small right-neighborhood of $\lambda_1$, the function $f(x)$ decreases. On the other extreme, as $x \to \infty$, the Cauchy transform $\mathcal{G}_p(x)$ is approximated by $\frac{1}{x}$ and so $f(x)$ is approximated by $x$, establishing that $\lim_{x\to\infty} f(x) = \infty$. $\square$

As previously mentioned, we make use of a graph denoted as $\mathcal{H}$, which we define next. Let $H$ be a $c$-regular graph with $d$ vertices. The graph $\mathcal{H}$ is formed by taking $n$ disjoint copies of $H$, one on each of the vertex sets $id + \{1, \ldots, d\}$ for $i = 0, 1, \ldots, n-1$. The final graph that we construct is obtained by taking the summation of $d$ copies of $\mathcal{H}$ where in each copy the vertex labels are shuffled according to some permutation. In matrix form,

$$X_{\mathbf{P}}(H) = \sum_{i=1}^{d} \mathbf{P}_i \mathcal{H} \mathbf{P}_i^{\mathsf{T}},$$

where $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_d)$ is a sequence of $(nd) \times (nd)$ permutation matrices. We will now use a result from [MSS18] to express the *expected characteristic polynomial* of $X_{\mathbf{P}}(H)$ using the finite free additive convolution, where the sequence $\mathbf{P}$ is chosen uniformly at random.

**Theorem 6.5** (Corollary 4.9 from [MSS18])**.** *Let $\mathbf{A}_1, \ldots, \mathbf{A}_d$ be symmetric $m \times m$ matrices satisfying $\mathbf{A}_i \mathbf{1} = \alpha_i \mathbf{1}$. For $i \in [d]$, let $p_i(x)$ be the polynomial satisfying $\chi_x(\mathbf{A}_i) = (x - \alpha_i) p_i(x)$. Let $\mathbf{P}_1, \ldots, \mathbf{P}_d$ be independent and uniformly chosen random $m \times m$ permutation matrices. Then,*

$$\mathop{\mathbf{E}}_{\mathbf{P}_1,\ldots,\mathbf{P}_d} \chi_x\left(\sum_{i=1}^{d} \mathbf{P}_i \mathbf{A}_i \mathbf{P}_i^{\mathsf{T}}\right) = \left(x - \sum_{i=1}^{d} \alpha_i\right) p_1(x) \boxplus \cdots \boxplus p_d(x).$$

As briefly mentioned in Section 3.2, a key ingredient in the proof for Theorem 6.5 is the *quadrature* result. We utilize this result as a black-box and refer readers interested in further details to the original paper. Additionally, the corresponding result for the multiplicative convolution can be found in Chapter 5 of [CM23]. The following is an immediate application of Theorem 6.5, applied with all instances of $\mathbf{A}_i$ being the adjacency matrix of the graph $\mathcal{H}$.

**Corollary 6.6.** *Let $p(x)$ be the polynomial satisfying $\chi_x(\mathcal{H}) = (x - c)p(x)$, and let $\mathbf{P}_1, \ldots, \mathbf{P}_d$ be independent and uniformly chosen random $nd \times nd$ permutation matrices. Then,*

$$\mathop{\mathbf{E}}_{\mathbf{P}_1,\ldots,\mathbf{P}_d} \chi_x\left(X_{\mathbf{P}}(H)\right) = (x - dc)\, p^{\boxplus d}(x).$$

The combination of the results above give us our desired bound, which at this point will apply only to the expected characteristic polynomial.

**Corollary 6.7.** *Let $d \geq 3$ and $c \geq 1$ be integers. Then, for every $c$-regular graph $H$ on $d$ vertices,*

$$\lambda_2\left(\mathop{\mathbf{E}}_{\mathbf{P}} \chi_x(X_{\mathbf{P}}(H))\right) \leq \min_{x > c}\left(dx - \frac{d-1}{\mathcal{G}_H(x)}\right),$$

*where $\mathbf{P}$ is a uniformly chosen length-$d$ sequence of $nd \times nd$ permutation matrices.*

*Proof.* Let $p(x)$ be the polynomial satisfying $\chi_x(\mathcal{H}) = (x-c)p(x)$. By Corollary 6.6, it is enough to bound the largest root of $p^{\boxplus d}(x)$. Per our assumption $c \geq 1$, the graph $H$ contains at least one edge and so, due to the additional assumption of vertex transitivity, the number of connected components is at most $\frac{d}{2}$. It is well-known that the number of connected components equals to the multiplicity of the largest eigenvalue, $c$. Thus, we may invoke Corollary 6.4 with $r = d$ to conclude that the largest root of $p^{\boxplus d}(x)$ is upper bounded by

$$\min_{x>c}\left(dx - \frac{d-1}{\mathcal{G}_p(x)}\right).$$

To complete the proof we observe that $\mathcal{G}_H(x) > \mathcal{G}_p(x)$ for every $x > c$. To see this note that both $\mathcal{G}_{\mathcal{H}}(x)$ and $\mathcal{G}_p(x)$ are averages of terms of the form $\frac{1}{x-\alpha_i}$, where the $\alpha_i$-s are the roots of the respective polynomials, and $\mathcal{G}_{\mathcal{H}}(x)$ is averaging over one additional term compared to $\mathcal{G}_p(x)$, that term being $\frac{1}{x-c}$ which is the largest. Therefore $\mathcal{G}_{\mathcal{H}}(x) > \mathcal{G}_p(x)$ for every $x > c$. As $\mathcal{H}$ was constructed of $n$ disjoint copies of $H$, clearly $\chi_x(\mathcal{H}) = \chi_x(H)^n$, thus $\mathcal{G}_H(x) = \mathcal{G}_{\mathcal{H}}(x)$, completing the proof. $\square$

### 6.2 Interlacing: from random permutations to a concrete graph

In the previous section we analyzed the expected characteristic polynomial of $X_{\mathbf{P}}(H)$, where the expectation is taken over a uniform choice of the permutation matrix sequence $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_d)$. In order to show that there is a specific graph satisfying the same bound as the expectation, we cite the following theorem from [MSS18].

**Theorem 6.8** (Theorem 3.4 in [MSS18])**.** *Suppose $\mathbf{A}_1, \ldots, \mathbf{A}_d$ are symmetric $m \times m$ matrices and $\mathbf{P}_1, \ldots, \mathbf{P}_d$ are independent uniform random $m \times m$ permutation matrices. Then, for every $k \leq m$ there exists a specific choice of permutations $\Pi_1, \ldots, \Pi_d$ such that*

$$\lambda_k\left(\chi_x\left(\sum_{i=1}^{d}\Pi_i\mathbf{A}_i\Pi_i^{\intercal}\right)\right) \leq \lambda_k\left(\mathop{\mathbf{E}}_{\mathbf{P}_1,\ldots,\mathbf{P}_d}\chi_x\left(\sum_{i=1}^{d}\mathbf{P}_i\mathbf{A}_i\mathbf{P}_i^{\intercal}\right)\right). \tag{6.2}$$

Theorem 6.8 is a deep result which skillfully leverages the structure of permutation matrices to recursively construct a tree of polynomials. Each polynomial in this tree represents a partial expectation over the space of permutation matrices. These polynomials collectively form what is known as an *interlacing family of polynomials.*

*Proof of Theorem 6.2.* For proving the existence of the graph stated, we first observe that $X_{\mathbf{P}}(H)$ is $H$-local for every choice of $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_d)$, hence it is enough to show that there exists a permutation sequence $\Pi = (\Pi_1, \ldots, \Pi_d)$ such that $X_\Pi(H)$ satisfies the desired property. By applying Theorem 6.8 with $k = 2$, and plugging the result from Corollary 6.7 to the RHS of Equation (6.2), we get that there exists a sequence $\Pi$ such that

$$\lambda_2\left(X_\Pi(H)\right) \leq \min_{x>c}\left(dx - \frac{d-1}{\mathcal{G}_H(x)}\right).$$

$\square$

# 7 Lower Bound for the Spectral Expansion of Rotating Expanders

In this section, we address the following question

**Question.** How good can the spectral expansion of a graph product be?

Specifically, one can ask whether a graph product can be Ramanujan. We prove that the answer to the latter question is negative. In fact, our result implies that the construction of rotating expanders [CM23] achieves optimal expansion among graph products. We start by stating the main result of this section, which is the full and formal version of Theorem 2.4.

**Theorem 7.1.** *For every sequence of $n$-vertex $d$-regular graphs $G_1, \ldots, G_t$, the product graph $G = G_1 G_2 \cdots G_t^2 \cdots G_2 G_1$ satisfies*

$$\lambda(G) \geq \frac{(t+1)^{t+1}}{t^t} \cdot (d-1)d^{t-1} - o_n(1).$$

As discussed in Section 3.3, the proof of Theorem 7.1 makes use of the Fuss-Catalan numbers.

**Definition 7.2** (Fuss-Catalan numbers)**.** *For integers $p \geq 2$ and $k \geq 0$, the $(p,k)$* Fuss-Catalan number*, denoted as $C_k^{(p)}$, is given by*

$$C_k^{(p)} = \frac{1}{pk+1}\binom{pk+1}{k}.$$

Note that the ordinary Catalan numbers are obtained by setting $p = 2$. As for Catalan numbers, for every $p \geq 2$, Fuss-Catalan numbers also satisfy a recurrence relation which is given by

$$C_{k+1}^{(p)} = \sum_{a_1+a_2+\cdots+a_p=k} \prod_{i=1}^{p} C_{a_i}^{(p)}.$$

As in Section 5, we employ the trace method to establish our lower bound on the spectral expansion. Consequently, we will need to argue about the number of cycles in a graph product. Let $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_t$ be the adjacency matrices of $d$-regular graphs, and let

$$\mathbf{B}_t = \mathbf{A}_1\mathbf{A}_2 \cdots \mathbf{A}_{t-1}\mathbf{A}_t^2\mathbf{A}_{t-1} \cdots \mathbf{A}_2\mathbf{A}_1$$

be the adjacency matrix of the corresponding product graph, denoted as $G_t$. Note that $G_t$ is $D$-regular for $D = d^{2t}$. The following is the main technical result underlying the proof of Theorem 7.1.

**Proposition 7.3.** *Let $v$ be any vertex in $G_t$ as defined above. Then, for every $k \geq 0$, the number of length-$k$ cycles that originate at $v$ is at least $C_k^{(t+1)} \cdot \left((d-1)d^{t-1}\right)^k$.*

*Proof.* As was done for the case of two graphs in Section 3.3, we consider a length-$k$ cycle in $G_t$ and partition it into $\ell = 2kt$ steps, $2k$ in each of the graphs $G_i$ taking part in the product, according to their order. Let $m \leq \ell$ be the first time the cycle revisits $v$, so that there is a prefix of the cycle of the form $v \to v_1 \to \cdots \to v_{m-1} \to v_m = v$.

For the purpose of proving a lower bound on the number of cycles, we do not assume any nontrivial relations between the graphs, and do not assume cycles of any length within the graphs (as discussed in Section 3.3, such relations or cycles can only increase the count). This leads to the conclusion that in order to return to the origin $v$ at step $m$, the first and last edges in this prefix have to come from $G_1$, and therefore $v_1 = v_{m-1}$. We apply the same approach from counting cycles in $\mathcal{T}_d$ in Section 3.1.1, of moving away from or returning towards $v$. Hence, there are two sub-cycles already induced: one starting at $v_1$ and ending at $v_{m-1}$, in which the first and last edges are from $G_2$, and the second is the cycle from $v_m = v$ back to $v_\ell = v$ (which may be an empty cycle, if $m = \ell$), and these induce more such smaller cycles recursively.

The key observation is that the above process has a clear bijection with *alternating colors non-crossing pairing* in the length $2kt$ sequence

$$a_1^{(1)} \cdots a_t^{(1)} a_t^{(2)} \cdots a_1^{(2)} \cdots\cdots\cdots a_1^{(2k-1)} \cdots a_t^{(2k-1)} a_t^{(2k)} \cdots a_1^{(2k)},$$

where each $a_i^{(j)}$ can only be paired with a letter having the same color, namely $a_i^{(j')}$ for some $j'$. By non-crossing, we mean that there are no four indices $i_1 < i_2 < i_3 < i_4$ such that both $(i_1, i_3)$ and $(i_2, i_4)$ are paired. In this bijection, every *opening* of a pair represents a step forward in the corresponding graph, where the *closing* represents a backward step. The non-crossing condition ensures that a cycle is actually closed under no assumption of non-trivial relations between the different graphs. We also note that non-crossing partitions are closed under cyclic rotations, that is, a non-crossing partition of a sequence $(c_1, c_2, \ldots, c_{m-1}, c_m)$ is also non-crossing as a partition of $(c_m, c_1, \ldots, c_{m-1})$.

We observe that if $a_1^{(1)}$ is paired with $a_1^{(j)}$ then $j$ must be even, otherwise there will be an odd number of $a_1$-s between them and no non-crossing pairing will be possible. Moreover, for ensuring that the pairing remains non-crossing, $a_2^{(1)}$ has to be paired with $a_2^{(j')}$ for some $j' \le j$. Applying these observations recursively, we can look at the first instances of $a_1, \ldots, a_t$ and where they are paired, and construct a non-crossing pairing using the following algorithm (see Figure 3):

1. Pick integers $l_1, l_2, \ldots, l_t$ such that $k \ge l_1 \ge l_2 \ge \cdots \ge l_t \ge 1$.
2. Pair each $a_i$ to the $a_i$ at location $m_i = 2t \cdot l_i - i + 1$.
3. Continue recursively from step 1 for the gaps $g_1, g_2, \ldots, g_{t+1}$ between the $m_i$-s.

Notice that the choice of integers in steps 1 and 2 ensures that the pairings do not cross. Moreover, every non-crossing pairing induces the choice of integers in step 1 by looking at which indices were matched to the first $t$ elements. The gaps are of sizes $g_i = m_{i-1} - m_i - 1 = 2t(l_{i-1} - l_i)$, with $g_1 = 2t(k - l_1)$ is the gap between the last paired $a_1$ and the end of the sequence and $g_{t+1} = m_t - t - 1 = 2t(l_t - 1)$ is the gap between the first instance of $a_t$ and its paired element.

By the choices for the $l_i$-s, it is clear that $g_1 + g_2 + \cdots + g_{t+1} = 2t(k-1)$ and each is a multiple of $2t$. Recall that the opening of a pairing represents a step *away* from $v$, and we have $d$ possible steps for each such graph, with the exception of the first: had the previous step been an opening as well, in order to not close the pair there are just $d - 1$ options. Therefore we can write the

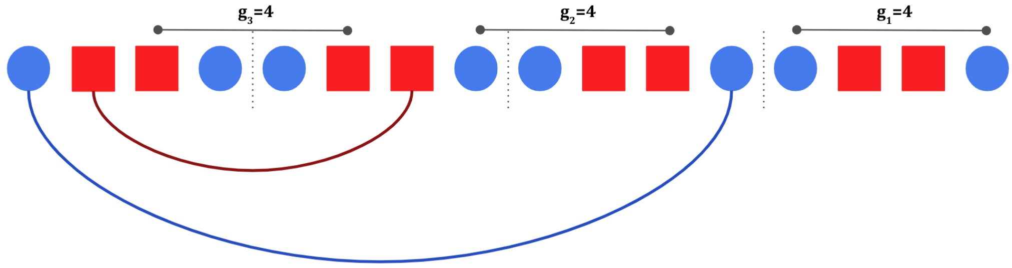


Figure 3: Recursively finding a non-crossing pairing for the case $t = 2$ and $k = 4$. The blue circles represent the graph $G_1$, and the red squares represent $G_2$. In the notations of the proof of Proposition 7.3, we have $l_1 = 3$, $l_2 = 2$, representing the relevant copy of $G_t$ picked for closing the pair.

recursive formula for the number of closed walks $W_k^{(t)}$ as

$$W_k^{(t)} = (d-1)d^{t-1} \sum_{a_1+\cdots+a_{t+1}=k-1} W_{a_1}^{(t)} \cdots W_{a_{t+1}}^{(t)},$$

which matches the recursive formula for $\left((d-1)d^{t-1}\right)^k C_k^{(t+1)}$, given that $W_0^{(t)} = 1$. □

*Proof of Theorem 7.1.* It can be easily verified that

$$C_k^{(p)} = \left(\frac{1}{k}\right)^{\Theta(1)} \left(\frac{p^p}{(p-1)^{p-1}}\right)^k.$$

Combining this with Proposition 7.3 and with Lemma 4.2, we have that for every graph $G_t$ with $n$ vertices constructed as a product of $t$ $d$-regular graphs,

$$\lambda(G_t) \geq \frac{(t+1)^{t+1}}{t^t}(d-1)d^{t-1} - o_n(1).$$

□

As mentioned in Section 2.3, Cohen and Maor [CM23] proved that for every $d$-regular Ramanujan graph $G$ with adjacency matrix $\mathbf{A}$, and for every integer $t \geq 2$, there exists a sequence of permutation matrices $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_{t-1})$ such that the graph $G_{\mathbf{P}}$, whose adjacency matrix is given by

$$\mathbf{A}_{\mathbf{P}} = \mathbf{A}\mathbf{P}_{t-1} \cdots \mathbf{A}\mathbf{P}_1 \mathbf{A}^2 \mathbf{P}_1^\intercal \mathbf{A} \cdots \mathbf{P}_{t-1}^\intercal \mathbf{A},$$

has spectral expansion

$$\lambda(G_{\mathbf{P}}) \leq \frac{(t+1)^{t+1}}{t^t}(d-1)d^{t-1} + o(1) < e(t+1)\sqrt{D-1} + o(1), \tag{7.1}$$

where the $o(1)$ term is a quantity that vanishes exponentially fast with the girth of $G$. The main motivation of [CM23] was to reduce the deterioration of the expansion from exponential in $t$, which is the case when considering the graph $G^t$, to linear. In our current context it is clear that the upper bound on the spectral expansion shown in Equation (7.1) matches, up to a vanishing term, the lower bound of Theorem 7.1. The immediate conclusion is that the lower bound is tight up to an $o(1)$ additive term, and that the construction of [CM23] is essentially optimal. It is worth noting that our lower bound holds in a more general form, where the graphs $G_1, \ldots, G_t$ can be arbitrary, whereas in Equation (7.1) they are all isomorphic.

# 8 Derandomized Squaring with Interesting Graphs

In this section we apply our results to some interesting graph families, starting with graphs which demonstrate the tightness of our lower bound (see Section 8.1). Our general bound on bounded-degree graphs is given in Section 8.2 and the stronger bound assuming good spectral expansion is given in Section 8.3. Cycle graphs are analyzed using the symbolic method in Section 8.4, and the complete bipartite graph is studied in Section 8.5. The remaining sections deal with Paley graphs (see Section 8.6) and, more generally, strongly regular graphs (see Section 8.7), as well as some specific interesting graphs in Section 8.8.

## 8.1 Three tight examples

In this short section we analyze some basic choices for the graph $H$, for which we know what behavior to expect and compare against our bound. We prove that for these instances, our lower bound given by Theorem 2.2 is tight, up to an additive vanishing term, for every Ramanujan graph $G$.

### 8.1.1 The true square

Let $G$ be a $d$-regular graph, where $d \geq 3$, and let $\mathrm{J}_d$ denote the complete graph on $d$ vertices, self-loops included. That is, $\mathrm{J}_d$ is the graph whose adjacency matrix is the all-ones $d \times d$ matrix, typically denoted as $\mathbf{J}$. Note that $G \circledS \mathrm{J}_d = G^2$. Our lower bound on $\lambda(G \circledS \mathrm{J}_d)$ obtained in Theorem 2.2 holds for all graphs $G$ in the sense that $\Lambda_{\mathrm{J}_d}$ is independent of $G$. Therefore, it is sensible to expect that if the lower bound is tight for this choice of $H = \mathrm{J}_d$ then it is matched by taking $G$ to be a $d$-regular Ramanujan graph. In such case, the spectral expansion $\lambda(G \circledS \mathrm{J}_d) = \lambda(G^2)$ can be computed directly and is equal to $\lambda(G)^2 = \left(2\sqrt{d-1}\right)^2 = 4(d-1)$. As we will now show, it is indeed the case that $\Lambda_{\mathrm{J}_d} = 4(d-1)$, establishing that our lower bound is tight for this choice of $H$.

The Cauchy transform of $\mathrm{J}_d$ is given by

$$\mathcal{G}_{\mathrm{J}_d}(x) = \frac{1}{d}\left(\frac{d-1}{x} + \frac{1}{x-d}\right) = \frac{x-d+1}{x(x-d)}.$$

Substituting to Equation (2.4) and simplifying, we see that the derandomized squaring polynomial associated with $\mathrm{J}_d$ is given by $\Delta_{\mathrm{J}_d}(x) = x^2 + (2-2d)x$. The unique real positive root of $\Delta_{\mathrm{J}_d}(x)$ is, of course $x_0 = 2d-2$. Substituting to Equation (2.5) yields $\Lambda_{\mathrm{J}_d} = 4(d-1)$.

### 8.1.2 Non-backtracking random walks

A second example for the tightness of our bound is given by the clique, denoted as $\mathrm{K}_d$, namely the complete graph without self-loops. It is easily seen combinatorially that $G \circledS \mathrm{K}_d$ corresponds to the graph of non-backtracking length-2 walks in $G$, which we denote by $G^{(2)}$. The corresponding adjacency matrix is given by $\mathbf{A}^{(2)} = \mathbf{A}^2 - d\mathbf{I}$. Hence, for a Ramanujan graph $G$, the best value we can hope for coming from the analysis is

$$\lambda(\mathbf{A}^{(2)}) = \lambda(\mathbf{A}^2) - d = 4(d-1) - d = 3d - 4.$$

This bound is indeed what results from our analysis. To see this, note that the Cauchy transform of $\mathrm{K}_d$ is

$$\mathcal{G}_{\mathrm{K}_d}(x) = \frac{1}{d}\left(\frac{d-1}{x+1} + \frac{1}{x-d+1}\right) = \frac{x-d+2}{(x+1)(x-d+1)}.$$

Substituting to Equation (2.4) and simplifying, we see that the derandomized squaring polynomial associated with $\mathrm{K}_d$ is given by

$$\Delta_{\mathrm{K}_d}(x) = x^2 + (4-2d)x + 3 - 2d.$$

The unique real positive root of $\Delta_{\mathrm{K}_d}(x)$ is $x_0 = 2d - 3$. Substituting to Equation (2.5) yields the desired bound, $\Lambda_{\mathrm{K}_d} = 3d - 4$.

It is instructive to compare our bound with the upper bound obtained by the Rozenman-Vadhan bound, Equation (1.1) for a Ramanujan graph $G$. The second largest (normalized) eigenvalue of $\mathrm{K}_d$ in absolute value is $\frac{1}{d-1}$, leading to an overall bound of $\approx 5d$ compared to the true behavior of $\approx 3d$.

### 8.1.3 The graph achieving the Rozenman-Vadhan bound

In [RV05], Rozenman and Vadhan proved that the bound that is given in Equation (1.1) is tight in a strong sense, namely, for every rational $\mu$, there exists a graph $\mathrm{RV}_\mu$ with $\omega(\mathrm{RV}_\mu) = \mu$, such that for every graph $G$ it holds that $\omega(G \circledS \mathrm{RV}_\mu) = (1-\mu)\omega(G^2) + \mu$. For ease of notation, we write RV instead of $\mathrm{RV}_\mu$ from hereon. The graph RV is constructed as follows: assume $\mu = \frac{s}{r}$ for some integers $r, s \geq 1$, then RV is a graph on $d$ vertices which is $rd$-regular, consisting of $r - s$ copies of the complete graph $\mathrm{J}_d$, and additional $sd$ self-loops on each vertex. The combinatorial analysis shows that a step in the $rd^2$-regular graph $G \circledS \mathrm{RV}$ amounts to staying at the same vertex with probability $\mu$ or taking a step in $G^2$ with probability $1 - \mu$, leading directly to the tightness of the bound.

Assume once again that $G$ is Ramanujan, hence $\lambda(G) \leq 2\sqrt{d-1}$. In this case, by Equation (1.1), we get that

$$\begin{aligned}\lambda(G \circledS \mathrm{RV}) &= \omega(G \circledS \mathrm{RV}) \cdot rd^2 \\ &= \left(\left(1 - \frac{s}{r}\right)\frac{4(d-1)}{d^2} + \frac{s}{r}\right) \cdot rd^2 \\ &= 4(d-1)r + (d-2)^2 s.\end{aligned}$$

As in the above two examples, we use the Cauchy transform of RV which is given by

$$\mathcal{G}_{\mathrm{RV}}(x) = \frac{1}{d}\left(\frac{d-1}{x-sd} + \frac{1}{x-rd}\right) = \frac{x-(d-1)r-s}{(x-dr)(x-ds)}.$$

Applying Theorem 5.9, we get

$$\psi_{\mathrm{RV}}(x) = \frac{d^3rs - d^2rs - d^2sx + 2dsx - x^2}{dr - r + s - x},$$

which has a minimum at $x_0 = 2(d-1)r - (d-2)s$, resulting in

$$\Lambda_{\mathrm{RV}} = \psi_{\mathrm{RV}}(x_0) = 4(d-1)r + (d-2)^2 s,$$

as in the Rozenman-Vadhan bound.

### 8.2 Bounded-degree graphs and a universal bound on $\kappa$

In this section we prove that derandomized squaring with a simple vertex-transitive graph of bounded degree results with a graph that gravitates towards Ramanujan as the number of vertices in $H$ increases. Moreover, we establish a universal bound on $\kappa_H$ which holds for all simple vertex-transitive graphs.

**Theorem 8.1.** *Let $H$ be a simple vertex-transitive $c$-regular graph on $d$ vertices, where $d \geq 3$ and $c \geq 1$. Then,*

$$\kappa_H \leq 2 + \frac{\sqrt{c}}{\sqrt{d}-\sqrt{c}}.$$

*Moreover, for every $d \geq 11$ it holds that $\kappa_H \leq 3$. Lastly, if $H$ is triangle-free then*

$$\kappa_H \leq 2 + \frac{c}{d} \cdot \frac{1}{1-\sqrt{\frac{c}{d}}}.$$

*Proof.* Let $\mathbf{A}$ be the adjacency matrix of $H$. Recall Equation (4.2) which states that $\mathcal{G}_H(x) = \sum_{r=0}^{\infty} \frac{m_r(H)}{x^{r+1}}$, where $m_r(H) = \frac{1}{d}\mathsf{Tr}(\mathbf{A}^r)$. Clearly, $m_0(H) = 1$, and since $H$ has no self-loops, $m_1(H) = 0$. Note further that for every $r \geq 2$ it holds that $m_r(H) \leq c^{r-1}$. Indeed, since $H$ is simple, each step on a length-$r$ cycle that originate at some fixed vertex of $H$ has at most $c$ choices, and the last step is determined, returning to that vertex. Therefore, for every $x > 0$,

$$\mathcal{G}_H(x) \leq \frac{1}{x} + \frac{c}{x^3}\sum_{r=0}^{\infty}\left(\frac{c}{x}\right)^r = \frac{1}{x} + \frac{c}{x^2(x-c)}.$$

Thus,

$$\psi_H(x) = dx - \frac{d-1}{\mathcal{G}_H(x)} \leq \frac{x(x^2-cx+cd)}{x^2-cx+c}.$$

Recall Theorem 5.9 which states that $\Lambda_H = \min_{x>c}\psi_H(x)$, and so to upper bound $\Lambda_H$, and hence $\kappa_H$ after a suitable normalization, we may take any $x_0 > c$ and evaluate, or upper bound, $\psi_H(x_0)$. A good choice for the case $c \ll d$ would be $x_0 = \sqrt{cd}$, which yields the bound

$$\kappa_H \leq \sqrt{\frac{cd}{cd-1}} \cdot \frac{2d-\sqrt{cd}}{d+1-\sqrt{cd}} \leq 2 + \frac{\sqrt{c}}{\sqrt{d}-\sqrt{c}}.$$

As for the moreover part, by substituting $x_0 = c + d$, we get

$$\kappa_H \leq \frac{\psi_H(c+d)}{\sqrt{cd}-1} \leq \frac{1}{\sqrt{cd}-1} \cdot \frac{d(c+d)(2c+d)}{cd+c+d^2}.$$

It can be verified that for $d \geq 11$ and $c \geq \frac{d}{4}$, the RHS of the above equation is bounded by

$$\frac{1}{\sqrt{cd}} \cdot \frac{d(c+d)(2c+d)}{cd+d^2} = \frac{2c+d}{\sqrt{cd}}.$$

From here, it straightforward to verify that for every $d \geq 11$ and $1 \leq c \leq d-1$,

$$\kappa_H \leq \min\left(2 + \frac{\sqrt{c}}{\sqrt{d}-\sqrt{c}}, \frac{2c+d}{\sqrt{cd}}\right) \leq 3.$$

To conclude the proof, consider a triangle-free graph $H$. Under this additional assumption, $m_3(H) = 0$, and so

$$\mathcal{G}_H(x) \leq \frac{1}{x} + \frac{c}{x^3} + \frac{c^3}{x^5}\sum_{r=0}^{\infty}\left(\frac{c}{x}\right)^r = \frac{x^4 - cx^3 + cx^2 - c^2x + c^3}{x^4(x-c)}.$$

Using an argument as the one above, taking again $x_0 = \sqrt{cd}$, we conclude that

$$\kappa_H \leq \frac{\psi_H(\sqrt{cd})}{\sqrt{cd}-1} \leq \frac{d}{\sqrt{cd}-1} \cdot \frac{2d\sqrt{cd} - c(2d-\sqrt{cd})}{c+(d+1)(d-\sqrt{cd})} \leq 2 + \frac{c}{d} \cdot \frac{1}{1-\sqrt{\frac{c}{d}}}.$$

$\square$

### 8.3 Spectral expanders

In this section we prove a stronger bound on $\kappa_H$ than the one obtained in Theorem 8.1, which recall holds for general bounded-degree graphs, assuming that $H$ is a good spectral expander. The proof follows the same argument as in the proof of Theorem 8.1 though takes into account the bound on the spectral expansion.

**Proposition 8.2.** *Let $H$ be a simple vertex-transitive $c$-regular graph on $d$ vertices. Assume that $10 \leq c < \sqrt{d}$. Then,*

$$\kappa_H \leq 2 + \frac{3}{\sqrt{d}}\left(\frac{\lambda(H)}{\sqrt{c}}\right)^3.$$

*Furthermore, if $H$ is triangle-free then*

$$\kappa_H \leq 2 + \frac{4}{d}\left(\frac{\lambda(H)}{\sqrt{c}}\right)^4.$$

*Proof.* Denote $\lambda = \lambda(H)$ and let $\mathbf{A}$ be the adjacency matrix of $H$. Recall Equation (4.2) which states that $\mathcal{G}_H(x) = \sum_{r=0}^{\infty} \frac{m_r(H)}{x^{r+1}}$ where $m_r(H) = \frac{1}{d}\mathsf{Tr}(\mathbf{A}^r)$. Clearly, $m_0(H) = 1$ and as $H$ has no self-loops, $m_1(H) = 0$. Since $H$ is a simple $c$-regular graph, we have that $m_2(H) = c$, and per our assumption on the spectral expansion of $H$, for every $r \geq 3$ it holds that

$$m_r(H) = \frac{1}{d}\mathsf{Tr}(\mathbf{A}^r) \leq \frac{c^r + (d-1)\lambda^r}{d} \leq \frac{c^r}{d} + \lambda^r.$$

Therefore, for every $x > 0$,

$$
\begin{aligned}
\mathcal{G}_H(x) &\leq \frac{1}{x} + \frac{c}{x^3} + \sum_{r=3}^{\infty} \frac{1}{x^{r+1}} \left( \frac{c^r}{d} + \lambda^r \right) \\
&= \frac{1}{x} + \frac{c}{x^3} + \frac{c^3}{dx^4} \cdot \frac{1}{1 - \frac{c}{x}} + \frac{\lambda^3}{x^4} \cdot \frac{1}{1 - \frac{\lambda}{x}} \\
&\leq \frac{1}{x} + \frac{c}{x^3} + \frac{1}{x^3} \left( \frac{c^3}{d} + \lambda^3 \right) \frac{1}{x - c},
\end{aligned}
$$

where we used the fact that $\lambda \leq c$ for the last inequality. Per our assumption $10 \leq c < \sqrt{d}$ and since the inequality $\lambda \geq \sqrt{c}$ holds in general, we have that

$$
\left( \frac{c^3}{d} + \lambda^3 \right) \frac{1}{\sqrt{cd} - c} \leq \frac{2\lambda^3}{\sqrt{cd}},
$$

and so

$$
\mathcal{G}_H(\sqrt{cd}) \leq \frac{1}{\sqrt{cd}} + \frac{1}{\sqrt{cd^3}} + \frac{2\lambda^3}{(cd)^2}.
$$

Therefore,

$$
\begin{aligned}
\frac{\psi_H(\sqrt{cd})}{\sqrt{cd} - 1} &= \frac{1}{\sqrt{cd} - 1} \left( d\sqrt{cd} - \frac{d-1}{\mathcal{G}_H(\sqrt{cd})} \right) \\
&\leq \sqrt{\frac{cd}{cd-1}} \cdot \frac{2(cd)^{3/2} + 2\lambda^3 d}{(cd)^{3/2} + 2\lambda^3} \\
&\leq 2 + \frac{3}{\sqrt{d}} \left( \frac{\lambda}{\sqrt{c}} \right)^3.
\end{aligned}
$$

As for the moreover part, since there are no triangles, $m_3(H) = 0$ and so similarly to the above derivation, we get that

$$
\begin{aligned}
\mathcal{G}_H(x) &\leq \frac{1}{x} + \frac{c}{x^3} + \sum_{r=4}^{\infty} \frac{1}{x^{r+1}} \left( \frac{c^r}{d} + \lambda^r \right) \\
&\leq \frac{1}{x} + \frac{c}{x^3} + \left( \frac{c^4}{d} + \lambda^4 \right) \frac{1}{x^4(x-c)} \\
&\leq \frac{1}{x} + \frac{c}{x^3} + \frac{2\lambda^4}{x^4(x-c)},
\end{aligned}
$$

where the last inequality is per our assumption $d > c^2$ and using again the fact that $\lambda \geq \sqrt{c}$. Substituting $x = \sqrt{cd}$ as before, we get that

$$
\mathcal{G}_H(\sqrt{cd}) \leq \frac{1}{\sqrt{cd}} + \frac{1}{\sqrt{cd^3}} + \frac{2\lambda^4}{(cd)^2(\sqrt{cd} - c)}.
$$

Therefore,

$$
\begin{aligned}
\frac{\psi_H(\sqrt{cd})}{\sqrt{cd} - 1} &\leq \sqrt{\frac{cd}{cd-1}} \cdot \frac{2(cd)^3 - 2c^{3.5}d^{2.5} + 2\lambda^4 cd^2}{(cd)^3 + c^3d^2 - c^{3.5}d^{1.5} + 2\lambda^4 cd - c^{3.5}d^{2.5}} \\
&\leq \sqrt{\frac{cd}{cd-1}} \cdot \frac{2e + 2\lambda^4 cd^2}{e + c^3d^2 - c^{3.5}d^{1.5} + 2\lambda^4 cd},
\end{aligned}
$$

where $e = (cd)^3 - c^{3.5}d^{2.5}$. It can be verified that the RHS of the above equation is bounded by

$$2 + \frac{3\lambda^4 cd^2}{e} \leq 2 + \frac{4\lambda^4 cd^2}{(cd)^3} = 2 + \frac{4}{d}\left(\frac{\lambda}{\sqrt{c}}\right)^4.$$

□

### 8.4 Cycles

We now focus on the spectral expansion in the context of derandomized squaring with the length-$d$ cycle graph, denoted by $C_d$. Ideally, we could leverage the known eigenvalues of $C_d$. However, this method proves to be excessively intricate, involving complex trigonometric expressions that are impractical to handle. Instead, the objective of this section is to introduce a combinatorial strategy to establish a lower bound for the spectral expansion resulting from derandomized squaring. For this purpose, we explore an alternative formulation of Theorem 2.1 that adopts a more combinatorial perspective, enabling the use of the symbolic method to determine the generating function for the cycle graph. The reader should keep in mind that Theorem 8.1 has already established that $\kappa_{C_d} \leq 2 + \frac{4}{d}$ for all $d \geq 11$.

For an integer $\ell \geq 0$, denote the number of length-$\ell$ cycles that originate at some fixed arbitrary vertex $v$ by $c_\ell(H)$. If we denote by $\mathbf{H}$ the adjacency matrix of $H$ then the corresponding generating function is given by

$$\mathcal{C}_H(x) = \sum_{\ell=0}^{\infty} c_\ell(H)x^\ell = \sum_{\ell=0}^{\infty} (e_v^\mathsf{T}\mathbf{H}^\ell e_v)x^\ell = e_v^\mathsf{T}(\mathbf{I} - x\mathbf{H})^{-1}e_v.$$

As follows from Equation (4.1), the connection between the generating function $\mathcal{C}_H(x)$ and the Cauchy transform is given by $\mathcal{C}_H(x) = \frac{1}{x}\mathcal{G}_H(\frac{1}{x})$. Using this relation, we can recast Theorem 2.1 in terms of $\mathcal{C}_H(x)$ as follows: Let $x_0$ be the real positive solution to the equation

$$\frac{d}{d-1}\mathcal{C}_H(x)^2 = \mathcal{C}_H(x) + x\mathcal{C}_H'(x). \tag{8.1}$$

Then,

$$\Lambda_H = \frac{1}{x_0}\left(d - \frac{d-1}{\mathcal{C}_H(x_0)}\right). \tag{8.2}$$

Instead of going through the spectrum of $C_d$, we will once again employ the symbolic method, this time to describe $\mathcal{S}_{C_d}(x)$ which, recall, is the combinatorial class that consists of nonempty cycles that start at a fixed vertex $v$ of $C_d$ and revisit $v$ only upon completing the cycle. Using the symbolic method, in the following lemma, we give a closed form for the generating function of $\mathcal{S}_{C_d}(x)$.

**Lemma 8.3.** *For every $d \geq 3$,*

$$S_{C_d}(z) = 2z^2 \cdot \frac{z^{d-2} + b_{d-2}(z)}{b_{d-1}(z)},$$

*where, for every $\ell \geq 1$,*

$$b_\ell(z) = \frac{1}{2^{\ell+1}\Delta}\left((1+\Delta)^{\ell+1} - (1-\Delta)^{\ell+1}\right), \tag{8.3}$$

*and $\Delta = \sqrt{1-4z^2}$.*

Recall that since an element of $\mathcal{C}_H$ is a sequence of elements in $\mathcal{S}_H$, we have that $C_H(z) = \frac{1}{1-S_H(z)}$. The first couple of values are given by

$$C_{C_3}(z) = \frac{z-1}{(z+1)(2z-1)},$$
$$C_{C_4}(z) = \frac{1-2z^2}{1-4z^2},$$
$$C_{C_5}(z) = \frac{z^2+z-1}{(1-2z)(z^2-z-1)},$$

and so the corresponding values of $\kappa$ are $\kappa_{C_3} = \sqrt{5} \approx 2.236$ as expected, being a special case of a clique, see Section 8.1.2; and $\kappa_{C_4} = \frac{\sqrt{59+11\sqrt{33}}}{2\sqrt{7}} \approx 2.089$ which, of course, is consistent with our result on $K_{2,2}$ from Section 8.5. The next value, $\kappa_{C_5} \approx 2.026$ is consistent with the result from Section 8.7 on strongly regular graphs.

*Proof of Lemma 8.3.* Two types of cycles are included in $\mathcal{S}_{C_d}$, those in which the first node in the cycle, following the fixed vertex $v$, is also the last node visited before returning to $v$, and those cycles that revisit $v$ from its other neighbor. We partition the class $\mathcal{S}_{C_d}$ into two types of classes: $\mathcal{L}_{d-1}$ and $\mathcal{P}_{d-1}$ ($\mathcal{L}$ stands for loops and $\mathcal{P}$ for paths). Note that each type appears twice in $\mathcal{S}_{C_d}$ as in both cases we can start the cycle from any of the two neighbors of $v$. Using the symbolic method we summarize this succinctly as

$$\mathcal{S}_{C_d} = 2\mathcal{Z}^2\left(\mathcal{L}_{d-1} + \mathcal{P}_{d-1}\right). \tag{8.4}$$

We start by expressing, using the symbolic method, the class $\mathcal{L}_\ell$, for $\ell > 1$, in terms of $\mathcal{L}_{\ell-1}$. We can think of $\mathcal{L}_\ell$ as the class of cycles on the length-$\ell$ path that start and end at the leftmost node on the path. The cycle can visit the latter node any number of times, and so

$$\mathcal{L}_\ell = \mathsf{SEQ}\left(\rightarrow \times \mathcal{L}_{\ell-1} \times \leftarrow\right).$$

To see this, note that within the sequence construct, we consider nonempty cycles from the leftmost node to itself that revisit the latter only upon completing the cycle. Indeed, any such cycle begins by taking a right step, symbolized by the atom $\rightarrow$, followed by a cycle on the length $\ell-1$ path obtained by excluding the leftmost node, and then return by taking a left step.

As a direct implication we get the following recursive relation, with respect to $\ell$, on the generating functions of $\mathcal{L}_\ell$,

$$L_\ell(z) = \frac{1}{1-z^2 L_{\ell-1}(z)}.$$

It will be useful to express $L_\ell(z)$ as the quotient of two polynomials $L_\ell(z) = \frac{a_\ell(z)}{b_\ell(z)}$ in the following way. We have that

$$L_\ell(z) = \frac{1}{1-z^2\cdot\frac{a_{\ell-1}(z)}{b_{\ell-1}(z)}} = \frac{b_{\ell-1}(z)}{b_{\ell-1}(z)-z^2 a_{\ell-1}(z)}.$$

By the above recurrence relation, we get that $a_\ell(z) = b_{\ell-1}(z)$ and

$$b_\ell(z) = b_{\ell-1}(z) - z^2 b_{\ell-2}(z), \tag{8.5}$$

where $b_1(z) = 1$ and $b_2(z) = 1 - z^2$. That is,

$$L_\ell(z) = \frac{b_{\ell-1}(z)}{b_{\ell-1}(z) - z^2 b_{\ell-2}(z)}. \tag{8.6}$$

We turn to consider the combinatorial class $\mathcal{P}_\ell$. We can think of this class as the class of paths in the length-$\ell$ path that start at the leftmost vertex and end at the rightmost vertex, where any vertex can be revisited any number of times. Observe that every such path can be described using a path of the same type though from the leftmost vertex to the node that is adjacent to the rightmost vertex, followed by a right step, which gives the first time we visit the rightmost vertex. Then, to accommodate for the fact that we can revisit the later node any number of times, we follow the later path by an element of $\mathcal{L}_\ell$, exchanging the left and right directions. This gives the relation

$$\mathcal{P}_\ell = \mathcal{P}_{\ell-1} \times \to \times \mathcal{L}_\ell,$$

and so $P_\ell(z) = zP_{\ell-1}(z)L_\ell(z)$. Using Equation (8.6) we get that $P_\ell(z) = \frac{z^{\ell-1}}{b_\ell(z)}$, and so, using Equation (8.4), we conclude that

$$S_{C_d}(z) = 2z^2 \cdot \frac{z^{d-2} + b_{d-2}(z)}{b_{d-1}(z)}.$$

To complete the proof, we find a closed form for $b_\ell(z)$. By Equation (8.5), we have that

$$b_\ell(z) - b_{\ell-1}(z) + z^2 b_{\ell-2}(z) = 0,$$

and so

$$b_\ell(z) = A\left(\frac{1-\Delta}{2}\right)^\ell + B\left(\frac{1+\Delta}{2}\right)^\ell,$$

where, recall, $\Delta = \sqrt{1-4z^2}$. Using the initial conditions, $b_1(z) = 1$, $b_2(z) = 1 - z^2$ we can compute $A, B$. The result, $A = \frac{1}{2}(1 - \frac{1}{\Delta})$, $B = \frac{1}{2}(1 + \frac{1}{\Delta})$ then yeilds the desired closed form. $\square$

## 8.5 Complete bipartite graphs

In this section we consider the operation of derandomized squaring with the complete bipartite graph on $d$ vertices, for an even integer $d \geq 4$. This is, of course, a $c = \frac{d}{2}$ regular graph which we denote as $\mathrm{K}_{c,c}$. It is easy to see that $\mathrm{K}_{c,c}$ has eigenvalues $\pm c$, each with multiplicity 1, and the remaining eigenvalues are all 0. Therefore, the corresponding Cauchy transform, which for ease of notation we denote by $\mathcal{G}_{c,c}$, is given by

$$\mathcal{G}_{c,c}(x) = \frac{4x^2 - d(d-2)}{(4x^2 - d^2)x}.$$

From here one can compute the derandomized squaring polynomial

$$\Delta_{c,c}(x) = x^4 - \frac{d(2d-3)}{2}x^2 - \frac{(d-2)d^3}{16}$$

whose unique positive root $x_0 = \frac{\sqrt{md}}{2}$, where $m = 2d - 3 + \sqrt{(d-1)(5d-9)}$. One can verify that $\mathcal{G}(x_0) = \frac{m-d+2}{x_0(m-d)}$. Substituting this to Equation (2.5), we get

$$\Lambda_{\mathrm{K}_{c,c}} = x_0 \left( \frac{m+d}{m-d+2} \right) = \frac{\sqrt{md}}{2} \left( \frac{m+d}{m-d+2} \right).$$

The resulted graph is $D = \frac{d^2}{2}$-regular, and so we normalize by dividing by $\sqrt{D-1}$ to get

$$\kappa_{\mathrm{K}_{c,c}} = \sqrt{\frac{md}{2d^2-4}} \left( \frac{m+d}{m-d+2} \right).$$

From here one can compute the first couple of values, $\kappa_{\mathrm{K}_{2,2}} \approx 2.089$ which, of course, matches the bound we computed for the length-4 cycle, and $\kappa_{\mathrm{K}_{3,3}} \approx 2.157$. Considering the limit behavior as $d \to \infty$ we have that $m \approx \gamma d$ where $\gamma = 2 + \sqrt{5}$, and so

$$\kappa_{\mathrm{K}_{\infty,\infty}} \triangleq \lim_{c \to \infty} \kappa_{\mathrm{K}_{c,c}} = \sqrt{\frac{\gamma}{2}} \cdot \frac{\gamma+1}{\gamma-1} = \frac{1}{2}\sqrt{11 + 5\sqrt{5}} \approx 2.355.$$

## 8.6 Paley graphs

Let $q = 4r + 1$ be a prime power. The *Paley graph*, denoted as $\mathrm{Pal}_q$, has vertex set corresponding to the finite field $\mathbb{F}_q$ with the vertices adjacent if and only if their difference is a nonzero square in $\mathbb{F}_q$. As $q \equiv 1$ modulo 4, we have that $-1$ is a square in $\mathbb{F}_q$, and so $\mathrm{Pal}_q$ is undirected. Note that $\mathrm{Pal}_q$ is a $2r$-regular graph on $q$ vertices. It is well-known that the corresponding characteristic polynomial is $\chi_x(\mathrm{Pal}_q) = (x - 2r)(x-\alpha)^{2r}(x-\beta)^{2r}$, where $\alpha = \frac{-1-\sqrt{q}}{2}$ and $\beta = \frac{-1+\sqrt{q}}{2}$. Note that $\alpha + \beta = -1$ and $\alpha\beta = -r$. Hence, the Cauchy transform associated with $\mathrm{Pal}_q$ is given by

$$\mathcal{G}_{\mathrm{Pal}_q}(x) = \frac{1}{q}\left( \frac{1}{x-2r} + \frac{2r}{x-\alpha} + \frac{2r}{x-\beta} \right) = \frac{x^2 + x - r + 2r(x-2r)(2x+1)}{qM},$$

where $M = (x-2r)(x^2+x-r)$. Now,

$$\begin{aligned}
\mathcal{G}'_{\mathrm{Pal}_q}(x) &= -\frac{1}{q}\left( \frac{1}{(x-2r)^2} + \frac{2r}{(x-\alpha)^2} + \frac{2r}{(x-\beta)^2} \right) \\
&= -\frac{1}{q} \cdot \frac{(x^2+x-r)^2 + 2r(x-2r)^2\left(2x^2+2x+2r+1\right)}{M^2}.
\end{aligned}$$

For invoking Theorem 2.2, we wish to find the positive solution to Equation (2.4) which, after some manipulations leads us to the derandomized squaring polynomial

$$\Delta_{\mathrm{Pal}_q}(x) = x^4 - (4r-2)x^3 - (4r^2+6r-1)x^2 + 2r(2r+1)(4r-1)x - r^2(4r-1)(4r+1). \tag{8.7}$$

Evaluating the LHS at $x = c = 2r$ and at $x = 5r$ yields a negative and a positive value, respectively. Hence, the desired root lies in $(2r, 5r]$. Therefore, for the purpose of approximating the root in the limit, as $r \to \infty$, the above polynomial equation can be approximated by the equation

$$x^4 - 4rx^3 - 4r^2x^2 + 16r^3x - 16r^4 = 0.$$

More precisely, the solution to the original equation, Equation (8.7), which lies in $(2r, 5r]$, when divided by $r$ is approximated by the solution to the latter equation when divided by $r$. The solution to the latter equation is given by $x_0 = \gamma r$, where $\gamma = 1 + \sqrt{5 + \sqrt{32}}$. Now,

$$\mathcal{G}_{\mathrm{Pal}_q}(x_0) = \frac{\gamma^2 r^2 + x - r + 2r(x - 2r)(2x + 1)}{qM} = \frac{\gamma^2 r - 2\gamma r + \gamma - 1}{r(\gamma - 2)(\gamma^2 r + \gamma - 1)}.$$

Thus, by Theorem 2.2, the lower bound one obtains is

$$qx_0 - \frac{q-1}{\mathcal{G}_{\mathrm{Pal}_q}(x_0)} = \gamma r + \frac{8(\gamma - 1)r^2}{(\gamma^2 - 2\gamma)r + \gamma - 1}.$$

In the limit as $r \to \infty$, the above expression converges to

$$\left(\gamma + \frac{8(\gamma - 1)}{\gamma^2 - 2\gamma}\right) r = \left(1 + \sqrt{13 + 16\sqrt{2}}\right) r.$$

Recall that $q = 4r + 1 \approx 4r$ and that $D \approx \frac{q^2}{2} \approx 8r^2$. Thus, $r \approx \frac{1}{\sqrt{8}}\sqrt{D}$ and so the bound above implies that

$$\kappa_{\mathrm{Pal}_\infty} \triangleq \lim_{q \to \infty} \kappa_{\mathrm{Pal}_q} = \frac{1 + \sqrt{13 + 16\sqrt{2}}}{\sqrt{8}} \approx 2.464.$$

## 8.7 Strongly regular graphs

A $c$-regular graph on $d$ vertices with no self-loops is called *strongly regular* with parameters $\lambda, \mu$ [6] if $0 < c < d$ (namely, the graph is neither complete nor edgeless) and the following hold:

1. For each pair of adjacent vertices there are $\lambda$ vertices adjacent to both.
2. For each pair of nonadjacent vertices there are $\mu$ vertices adjacent to both.

Strongly regular graphs include dozens of interesting graphs such as the Peterson graph, the Hoffman-Singelton graph (see Section 8.8), and the symplectic graphs (see Section 8.7.2), as well as all Paley graphs which we analyzed in Section 8.6. It is a well-known fact that strongly regular graphs have two eigenvalues other than the trivial eigenvalue $c$, denoted $r, s$, with the convention $r > s$. This is, in fact, a spectral characterization of strongly regular graph among regular graphs. The multiplicity of these eigenvalues are denoted by $f, g$, respectively. In the following we compute the derandomized squaring polynomial of a strongly regular graph.

**Proposition 8.4.** *Let $H$ be a $c$-regular strongly regular graph on $d \geq 3$ vertices with parameters $\lambda, \mu$. Let $\alpha = \lambda - \mu$ and $e = c - d + 1$. Then, the derandomized squaring polynomial associated with $H$ is given by*

$$\Delta_H(x) = x^4 - 2(\alpha + c)x^3 + Ax^2 + Bx + C,$$

[6] It is customary to denote these parameters by $\lambda$ and $\mu$ and so, despite our use of $\lambda$ for denoting the spectral expansion, we proceed with this standard notation.

*where*

$$\begin{aligned}
A &= 2\mu + 4\alpha c + \alpha^2 + ce, \\
B &= -2\alpha\mu + 2c\left(c - ce - \alpha^2 - \mu\right), \\
C &= (\mu - c)(\mu + 2\alpha c + c) + c^3 e.
\end{aligned}$$

For proving Proposition 8.4, we make use of the fact that the different parameters of a strongly regular graph are, of course, not independent of each other. In the following theorem we gather the well-known relations we make use of. For a proof, and for an in-depth exposition to strongly regular graphs, the reader is referred to Chapter 10 in [GR01].

**Theorem 8.5.** *Let $G$ be a $c$-regular graph on $d$ vertices which is strongly regular with parameters $\lambda, \mu$. Then, with the notation above,*

1. $c(c-1-\lambda) = \mu(d-c-1)$
2. $rs = \mu - c$
3. $r + s = \lambda - \mu$
4. $f + g = d - 1$
5. $fr + gs + c = 0$
6. $fg(r-s)^2 = dc(d-c-1)$

*Proof of Proposition 8.4.* For ease of notation, we begin the proof by writing $C$ as a shorthand for $x - c$, and similarly $R$ for $x - r$ and $S$ for $x - s$. Then, the Cauchy transform corresponding to $H$ is given by

$$\mathcal{G}_H(x) = \frac{1}{d}\left(\frac{1}{C} + \frac{f}{R} + \frac{g}{S}\right) = \frac{RS + fCS + gCR}{dCRS}.$$

After some straightforward manipulations, Equation (2.4) takes the form

$$(RS + fCS + gCR)^2 = (d-1)\left((RS)^2 + f(CS)^2 + g(CR)^2\right). \tag{8.8}$$

We write the LHS as $(RS)^2 + f^2(CS)^2 + g^2(CR)^2 + 2T$, where

$$T = RSC(fS + gR) + fgC^2RS. \tag{8.9}$$

Returning to Equation (8.8), we get

$$2T = (d-2)(RS)^2 + ((d-1)f - f^2)(CS)^2 + ((d-1)g - g^2)(CR)^2.$$

But $(d-1)f - f^2 = (d-1-f)f = gf$, and similarly $(d-1)g - g^2 = (d-1-g)g = gf$. Thus,

$$2T = (d-2)(RS)^2 + fgC^2(R^2 + S^2).$$

Substituting for $T$ according to Equation (8.9), we get

$$\begin{aligned}2RSC(fS+gR) &= (d-2)(RS)^2 + fgC^2(R^2+S^2-2RS)\\ &= (d-2)(RS)^2 + fgC^2(r-s)^2.\end{aligned}$$

By Theorem 8.5, $fg(r-s)^2 = dc(d-c-1)$, and so the above equation takes the form

$$2RSC(fS+gR) = (d-2)(RS)^2 + dc(d-c-1)C^2.$$

Therefore,

$$2(x-r)(x-s)(x-c)((d-1)x-(fs+gr)) = (d-2)((x-r)(x-s))^2 + dc(d-c-1)(x-c)^2.$$

Recall that $\alpha = \lambda-\mu = r+s$, where the last equality is due to Theorem 8.5. Let $\beta = rs$. Invoking Theorem 8.5 once again, we get that

$$fs+gr = (d-1-g)s + (d-1-f)r = c + \alpha(d-1),$$

and that $(x-r)(x-s) = x^2-\alpha x+\beta$. Hence,

$$2(x^2-\alpha x+\beta)(x-c)((d-1)(x-\alpha)-c) = (d-2)(x^2-\alpha x+\beta)^2 + dc(d-c-1)(x-c)^2,$$

or, equivalently,

$$x^4 - 2(\alpha+c)x^3 + Ax^2 + Bx + C = 0, \tag{8.10}$$

where

$$\begin{aligned}A &= \frac{2(\beta+c^2-\alpha c)}{d} + c^2 - cd + 4\alpha c + c + \alpha^2,\\ B &= \frac{2\alpha(\alpha c - c^2 - \beta)}{d} + 2c\left(cd - c^2 - c - \alpha^2 - \beta\right),\\ C &= \frac{2\beta\left(c^2-\alpha c+\beta\right)}{d} + c^3(c-d+1) + 2\alpha\beta c - \beta^2.\end{aligned}$$

The LHS in Equation (8.10) is indeed the derandomized squaring polynomial of $H$. We turn to simplify $A, B$ and $C$. The expression $\frac{c^2-\alpha c+\beta}{d}$ appears in all three parameters. As it turns out, it is in fact an integer. To see this, recall that by Theorem 8.5, $c(c-1-\lambda) = \mu(d-c-1)$ and so $\alpha c = c(c-1)-(d-1)\mu$. Therefore,

$$c^2-\alpha c+\beta = \beta + c + (d-1)\mu = d\mu.$$

Hence, we can simplify $A, B, C$ to

$$\begin{aligned}A &= 2\mu + c^2 - cd + 4\alpha c + c + \alpha^2\\ B &= -2\alpha\mu + 2c\left(cd - c^2 - c - \alpha^2 - \beta\right)\\ C &= 2\beta\mu + c^3(c-d+1) + 2\alpha\beta c - \beta^2\end{aligned}$$

Recall that $\mu = c + rs = c + \beta$, and so $B = -2\alpha\mu + 2c\left(cd - c^2 - \alpha^2 - \mu\right)$. Lastly,

$$C = (\mu - c)(\mu + 2\alpha c + c) + c^3(c-d+1).$$

The proof then follows by the definition of $e$. $\square$

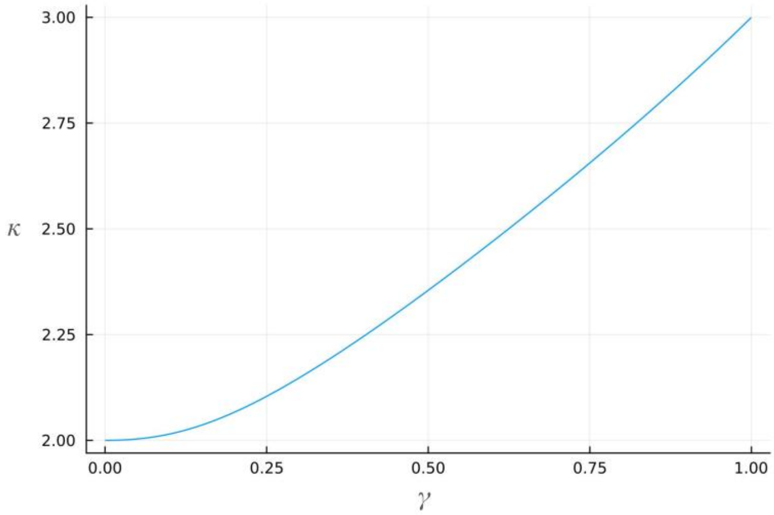


Figure 4: The dependence of $\kappa_H$ of a strongly regular graph $H$ satisfying $\lambda \ll c$ as a function of $\gamma = \frac{c}{d}$.

### 8.7.1 Asymptotic behavior when $\lambda \ll c$

In Proposition 8.4, we have streamlined the derivation of the derandomized squaring polynomial for a strongly regular graph as much as we could, and we will apply this result in the forthcoming examples. Nonetheless, the affect of the various parameters on the polynomial—and consequently, on the bound—remains opaque. In this section, we focus on strongly regular graphs where the parameter $\lambda \ll c$, namely, the number of mutual neighbors of two adjacent vertices is negligible in relation to their degree. Specifically, this class includes triangle-free strongly regular graphs, characterized by $\lambda = 0$. As usual, we consider the limit behavior, as $d \to \infty$, and write $c = \gamma d$.

Recall from Theorem 8.5 that $c(c-1-\lambda) = \mu(d-c-1)$. Thus, when $\lambda \ll c$ and as $d \to \infty$, we have that $\mu \approx \frac{c^2}{d-c} = \frac{\gamma^2}{1-\gamma} d$. Therefore, the coefficients of the derandomized squaring polynomial corresponding to $H$ can be approximated by

$$\begin{aligned} 2(\alpha + c) &\approx \left( \frac{2\gamma - 4\gamma^2}{1-\gamma} \right) d \\ A &\approx \frac{\gamma \left(6\gamma^3 - 7\gamma^2 + 3\gamma - 1\right)}{(\gamma-1)^2} d^2 \\ B &\approx \frac{2\gamma^2(1-2\gamma)(\gamma^2 - \gamma + 1)}{(1-\gamma)^2} d^3 \\ C &\approx \gamma^3(\gamma - 1) d^4. \end{aligned}$$

Although it is technically possible to formulate a closed expression for the positive root of the relevant derandomized squaring polynomial, the complexity of this expression makes it difficult to derive meaningful insights from it. However, in Figure 4, we present a graphical representation of the corresponding $\kappa$ value as it relates to $\gamma$.

### 8.7.2 The symplectic graphs

An interesting sub-family of strongly regular graphs are the so-called *symplectic graphs*. Let $r \geq 1$ be an integer. The symplectic graph $\mathrm{Sp}(2r)$ is the graph whose vertex set consists of all nonzero vectors in $\mathbb{F}_2^{2r}$. Two vertices $x, y$ are adjacent whenever $x^\mathsf{T}\mathbf{N}y = 1$, with all calculations over $\mathbb{F}_2$, where $\mathbf{N}$ is the $(2r) \times (2r)$ block diagonal matrix with $r$ blocks of the form $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. It is well-known that $\mathrm{Sp}(2r)$ is a strongly regular graph with $\lambda = \mu = 2^{2r-2}$. Setting $t = 2^{2r} - 2$, the polynomial whose unique positive solution we wish to compute is given by

$$x^4 - 4tx^3 + t(6 - 4t)x^2 + 4t^2(4t - 3)x - t^2(16t^2 - 16t + 3),$$

which we approximate by $x^4 - 4tx^3 - 4t^2x^2 + 16t^3x - 16t^4$. The positive root of this polynomial is given by $x_0 = \gamma t$, where $\gamma = 1 + \sqrt{5 + 4\sqrt{2}}$. Now,

$$\mathcal{G}_{\mathrm{Sp}(2r)}(x) = \frac{1}{4t-1}\left(\frac{1}{x - 2t} + \frac{2t - \sqrt{t} - 1}{x - \sqrt{t}} + \frac{2t + \sqrt{t} - 1}{x + \sqrt{t}}\right) = \frac{x^2 + t - 2tx}{(x - 2t)(x^2 - t)}.$$

Substituting to Equation (2.5) gives the lower bound

$$(4t - 1)\gamma t - \frac{(4t - 2)(\gamma t - 2t)(\gamma^2 t^2 - t)}{\gamma^2 t^2 + t - 2\gamma t^2} = \frac{(\gamma^3 - 2\gamma^2 + 8\gamma - 8)t^2 + (4 - 3\gamma)t}{(\gamma^2 - 2\gamma)t + 1}.$$

As $t \to \infty$, the above is approximated by

$$\frac{\gamma^3 - 2\gamma^2 + 8\gamma - 8}{\gamma(\gamma - 2)}t = \left(1 + \sqrt{13 + 16\sqrt{2}}\right)t.$$

Now, $\sqrt{cd} \approx \sqrt{8}t$ and so, the limit behavior of $\kappa(\mathrm{Sp}(2r))$ as $r \to \infty$ satisfies

$$\lim_{r \to \infty} \kappa(\mathrm{Sp}(2r)) = \frac{1 + \sqrt{13 + 16\sqrt{2}}}{\sqrt{8}} \approx 2.464.$$

Interestingly, though not unexpectedly, this limit behavior is also shared by Paley graphs (see Section 8.6).

## 8.8 Some specific graphs

In this section we consider some specific interesting graphs.

**The Petersen graph.** The Petersen graph is a 3-regular vertex-transitive graph on 10 vertices. It is strongly regular with parameters $\lambda = 1$ and $\mu = 0$, and so according to Section 8.7, its derandomized squaring polynomial is given by

$$\Delta_{\mathrm{Pet}}(x) = x^4 - 4x^3 - 27x^2 + 116x - 158.$$

Substituting its unique positive root to Equation (2.5), we get that $\Lambda_{\mathrm{Pet}} \approx 10.908$, or, $\kappa_{\mathrm{Pet}} \approx 2.025$.

**The Heawood graph.** The Heawood graph is a 3-regular vertex-transitive graph on 14 vertices having girth 6. It is interesting in our context as no 3-regular graph with fewer vertices have such high girth. The characteristic polynomial for the Heawood graph is $(x-3)(x+3)(x^2-2)^6$, hence the corresponding derandomized squaring polynomial is given by

$$\Delta_{\text{Hea}}(x) = x^6 - 55x^4 + 454x^2 - 1872.$$

Plugging the latter's unique positive root to Equation (2.5), we conclude that $\Lambda_{\text{Hea}} \approx 12.835$, or equivalently, $\kappa_{\text{Hea}} \approx 2.004$.

**The Hoffman-Singelton graph.** This graph was constructed for the classification of Moore graphs, and is the largest known Moore graph. The Hoffman-Singelton graph is a 7-regular vertex-transitive graph on 50 vertices. Its girth is 5, which is the highest possible given the number of vertices and it being 7-regular. The Hoffman-Singelton graph is strongly regular with $\lambda = 0$ and $\mu = 1$. Using our general result for strongly regular graphs, Proposition 8.4, the derandomized squaring polynomial associated with the Hoffman-Singelton graph is given by

$$\Delta_{\text{HS}}(x) = x^4 - 12x^3 - 319x^2 + 4188x - 14370.$$

Substituting its unique positive root to Equation (2.5) yields $\Lambda_{\text{HS}} \approx 37.497$, or $\kappa_{\text{HS}} \approx 2.007$.

**The Biggs-Smith graph.** This is another example of a 3-regular graph, though on 102 vertices, having girth 9. Its characteristic polynomial is given by

$$(x-3)(x-2)^{18}x^{17}(x^2-x-4)^9(x^3+3x^2-3)^{16},$$

from which it follows that $\kappa_{\text{BS}} \approx 2.000000016$. Note that this is significantly closer to 2 than what is guaranteed by Theorem 8.1.

**Conway's 99-graph.** We conclude by discussing our possibly useful yet failed attempt at solving an intriguing unsolved problem. The *Conway's 99-graph problem* asks about the existence of a 99-vertex graph where each edge is part of a unique triangle and each pair of non-adjacent vertices is diagonally opposite in a unique 4-cycle. It has been deduced that such a graph, if it exists, would be 14-regular and is in fact a strongly regular graph with parameters $\lambda = 1$ and $\mu = 2$. Although this brief exposition omits the historical context and significance of the problem, which the reader can easily find in the literature, we note that Conway proposed a \$1000 reward for resolving this problem.

One might speculate that disproving the existence of such a graph is achievable by analyzing its action on known constructs, specifically through its application in derandomized squaring. If the derandomized squaring constant, $\kappa_{\text{Conway}}$, were to be strictly less than 2, it would negate the graph's existence. Regrettably, our endeavors do not merit the prize. Indeed, the corresponding derandomized squaring polynomial would be

$$\Delta_{\text{Conway}}(x) = x^4 - 26x^3 - 1227x^2 + 33240x - 230352.$$

Its unique positive root is $x_0 \approx 39.496$. As the corresponding Cauchy transform is given by

$$\mathcal{G}_{\text{Conway}}(x) = \frac{x^2 - 13x - 12}{(x-14)(x-3)(x+4)},$$

Equation (2.5) yields that $\kappa_{\text{Conway}} \approx 2.041$.

## Acknowledgments

We would like to thank Roy Roth for his valuable contributions in producing the case study in Section 1.2.1 and for his insightful feedback throughout various stages of this work.

## References

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

[AKM+20] AmirMahdi Ahmadinejad, Jonathan Kelner, Jack Murtagh, John Peebles, Aaron Sidford, and Salil Vadhan. High-precision estimation of random walks in small space. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science*, pages 1295–1306. IEEE Computer Soc., Los Alamitos, CA, [2020] ©2020.

[Alo86] N. Alon. Eigenvalues and expanders. volume 6, pages 83–96. 1986. Theory of computing (Singer Island, Fla., 1984).

[APP+23] AmirMahdi Ahmadinejad, John Peebles, Edward Pyne, Aaron Sidford, and Salil Vadhan. Singular value approximation and reducing directed to undirected graph sparsification. *arXiv preprint arXiv:2301.13541*, 2023.

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

[BCG19] Mark Braverman, Gil Cohen, and Sumegha Garg. Pseudorandom pseudo-distributions with near-optimal error for read-once branching programs. *SIAM Journal on Computing*, 49(5):STOC18–242, 2019.

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

[Bor20] Charles Bordenave. A new proof of Friedman's second eigenvalue theorem and its extension to random lifts. *Ann. Sci. Éc. Norm. Supér. (4)*, 53(6):1393–1439, 2020.

[CHL+23] Lijie Chen, William Hoza, Xin Lyu, Avishay Tal, and Hongxun Wu. Weighted pseudorandom generators via inverse analysis of random walks and shortcutting. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 114, 2023.

[CL20] Eshan Chattopadhyay and Jyun-Jie Liao. Optimal error pseudodistributions for read-once branching programs. In *35th Computational Complexity Conference*, volume 169 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 25, 27. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2020.

[CM23] Gil Cohen and Gal Maor. Random walks on rotating expanders. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 971–984, 2023.

[Coh16] Michael B. Cohen. Ramanujan graphs in polynomial time. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 276–281. IEEE Computer Soc., Los Alamitos, CA, 2016.

[Fri08] Joel Friedman. A proof of Alon's second eigenvalue conjecture and related problems. *Mem. Amer. Math. Soc.*, 195(910):viii+100, 2008.

[FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics.* Cambridge University Press, 2009.

[GR01] Chris Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2001.

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

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

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

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

[Mar88] Grigorii Aleksandrovich Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problemy peredachi informatsii*, 24(1):51–60, 1988.

[MO20] Sidhanth Mohanty and Ryan O'Donnell. $X$-Ramanujan graphs. In *Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms*, pages 1226–1243. SIAM, Philadelphia, PA, 2020.

[MOP22] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-Ramanujan graphs of every degree. *SIAM J. Comput.*, 51(3):1–23, 2022.

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

[MRSV21] Jack Murtagh, Omer Reingold, Aaron Sidford, and Salil Vadhan. Derandomization beyond connectivity: undirected Laplacian systems in nearly logarithmic space. *SIAM J. Comput.*, 50(6):1892–1922, 2021.

[MSS15a] Adam W. Marcus, Daniel A. Spielman, and Nikhil Srivastava. Interlacing families I: Bipartite Ramanujan graphs of all degrees. *Ann. of Math. (2)*, 182(1):307–325, 2015.

[MSS15b] Adam W. Marcus, Daniel A. Spielman, and Nikhil Srivastava. Interlacing families II: Mixed characteristic polynomials and the Kadison-Singer problem. *Ann. of Math. (2)*, 182(1):327–350, 2015.

[MSS18] Adam W Marcus, Daniel A Spielman, and Nikhil Srivastava. Interlacing families IV: Bipartite Ramanujan graphs of all sizes. *SIAM Journal on Computing*, 47(6):2488–2509, 2018.

[MSS22] Adam W. Marcus, Daniel A. Spielman, and Nikhil Srivastava. Finite free convolutions of polynomials. *Probab. Theory Related Fields*, 182(3-4):807–848, 2022.

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

[NS06] Alexandru Nica and Roland Speicher. *Lectures on the combinatorics of free probability*, volume 335 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[OW20] Ryan O'Donnell and Xinyu Wu. Explicit near-fully X-Ramanujan graphs. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science*, pages 1045–1056. IEEE Computer Soc., Los Alamitos, CA, 2020.

[PŻ11] Karol A Penson and Karol Życzkowski. Product of ginibre matrices: Fuss-Catalan and Raney distributions. *Physical Review E*, 83(6):061118, 2011.

[Rei08] Omer Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4):Art. 17, 24, 2008.

[RV05] Eyal Rozenman and Salil Vadhan. Derandomized squaring of graphs. In *Approximation, randomization and combinatorial optimization*, volume 3624 of *Lecture Notes in Comput. Sci.*, pages 436–447. Springer, Berlin, 2005.

[RVW00] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 3–13. IEEE, 2000.

[TS17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 238–251, 2017.

[Woe00] Wolfgang Woess. *Random walks on infinite graphs and groups*, volume 138 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2000.



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il