Counting and Sampling Perfect Matchings in Regular Expanding Non-Bipartite Graphs

Farzam Ebrahimnejad ✉
University of Washington, Seattle, WA, USA

Ansh Nagda ✉
University of Washington, Seattle, WA, USA

Shayan Oveis Gharan ✉
University of Washington, Seattle, WA, USA

Abstract

We show that the ratio of the number of near perfect matchings to the number of perfect matchings in d-regular strong expander (non-bipartite) graphs, with $2n$ vertices, is a polynomial in n, thus the Jerrum and Sinclair Markov chain [14] mixes in polynomial time and generates an (almost) uniformly random perfect matching. Furthermore, we prove that such graphs have at least $\Omega(d)^n$ many perfect matchings, thus proving the Lovasz-Plummer conjecture [18] for this family of graphs.

2012 ACM Subject Classification Theory of computation → Expander graphs and randomness extractors; Mathematics of computing → Combinatoric problems; Mathematics of computing → Markov-chain Monte Carlo methods

Keywords and phrases perfect matchings, approximate sampling, approximate counting, expanders

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.61

Funding *Farzam Ebrahimnejad*: Research supported in part by NFS grant CCF-1552097.
Shayan Oveis Gharan: Research supported by Air Force Office of Scientific Research grant FA9550-20-1-0212, NSF grants CCF-1552097, CCF-1907845, and a Sloan fellowship.

1 Introduction

Given a (general) graph $G = (V, E)$ with $2n = |V|$ vertices, the problem of counting the number of perfect matchings in G is one of the most fundamental open problems in the field of counting. Jerrum and Sinclair in their landmark result [14] designed a Monte Carlo Markov Chain (MCMC) algorithm for this task and proved that such an algorithm runs in polynomial time if the ratio of the number of near perfect matchings to the number of perfect matchings is bound by a polynomial (in n). As a consequence one would be able to count perfect matchings if G is *very* dense, i.e., it has min-degree at least n. Not much is known beyond this case, despite several exciting results when the given graph G is bipartite [16, 17, 3, 15, 4].

This problem is also extensively studied in combinatorics. Around 40 years ago, Falikman and Egorychev [8, 10] proved the van-der-Waerden conjecture, thus showing that if G is a d-regular bipartite graph, then it has at least $(d/e)^n$ perfect matchings. This bound was further improved by Schrijver [21] and simpler and more general proofs were found [13, 1]. But it remains a mystery whether van-der-Waerden conjecture extends to non-bipartite graphs. Lovasz, Plummer most famously made the following conjecture:

► **Conjecture 1** ([18, Conjecture 8.1.8]). *For $d \geq 3$, there exist constants $c_1(d), c_2(d) > 1$ such that any d-regular $k-1$-edge connected graph G with $2n$ vertices contains at least $c_1(d)c_2(d)^n$ perfect matchings and $c_2(d) \to \infty$ as $d \to \infty$.*

To this date the above conjecture is only proved for $d = 3$ [9], although the same proof shows that the conjecture holds for all $d \geq 3$ as long as $c_2(d)$ is allowed to be a fixed constant.

At a high-level, the study of perfect matchings in general graphs faces the following barriers:

- Unlike bipartite graphs, the perfect matching polytope of a general graph has exponentially many constraints, and it is believed that there does not exist any poly-size convex program to test whether a given graph has perfect matchings. This fact significantly limits exploiting Gurvits' like techniques [13] in lower-bounding the number of perfect matchings.
- In a bipartite graph, any odd alternating *walk* (that starts and ends at un-saturated vertices) can be used to extend a near perfect matching to a perfect matching. However, in a general graph, an odd alternating walk may contain odd cycles. Therefore, typical augmenting path arguments which bound the ratio of near perfect to perfect matchings fail in a non-bipartite graph (see e.g., [16]).

In this paper we study perfect matchings in regular *strong* expander graphs: We show that for these graphs the classical algorithm of [14] runs in polynomial time and can generate an approximately uniform random perfect matching. On the combinatorial side, we prove a significantly stronger version of Conjecture 1 for this family of graphs.

1.1 Main Contributions

Given a graph $G = (V, E)$, let $A_G \in \mathbb{R}^{2n\times 2n}$ be its adjacency matrix, and let $D \in \mathbb{R}^{2n\times 2n}$ be the diagonal matrix of vertex degree. The normalized adjacency matrix of G is defined as $\tilde{A}_G = D^{-1/2}AD^{-1/2}$; when G is clear in the context we may drop the subscript. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n}$ be the eigenvalues of $\tilde{A}$. We write

$$\sigma_2(\tilde{A}) = \max\{\lambda_2, |\lambda_{2n}|\},$$

to denote the largest eigenvalue of $\tilde{A}$ in absolute value (excluding λ_1).

► **Definition 2.** *For $0 < \epsilon < 1$, we write G is an ϵ-spectral expander if $\sigma_2(\tilde{A}) \leq \epsilon$.*

For two probability distributions μ, ν defined in $\{1, \dots, n\}$, the total variation distance of μ, ν is $\frac{1}{2}\sum_{i=1}^n |\mu_i - \nu_i|$.

► **Theorem 3** (Algorithm). *There is a randomized algorithm that for $\epsilon \leq 1/11$, $\delta > 0$, given a d-regular ϵ-spectral expander G on $2n$ vertices outputs a perfect matching of G from a distribution μ of total variation distance δ of the uniform distribution (of perfect matchings) in time $\mathrm{poly}(n^{\log_{1/\epsilon} d}, \log(1/\delta))$. Furthermore, there is a randomized algorithm that for any $\delta > 0$ approximates the number of perfect matchings of G up to $1 \pm \delta$ multiplicative factor in time $\mathrm{poly}(n^{\log_{1/\epsilon} d}, 1/\delta)$.*

In particular, observe that the running time of the above algorithms is polynomial in n if d is a constant or $1/\epsilon$ is a polynomial in d and it is quasi-polynomial in n otherwise.

► **Theorem 4** (Lower Bound). *For any $\epsilon \leq 1/11$, every d-regular ϵ-spectral expander on $2n$ vertices has at least $(d/e)^n \left(\frac{\epsilon}{2e^3d^6}\right)^{\epsilon n}$ many perfect matchings.*

Putting the above theorem together with [9] proves Conjecture 1 for (strong) spectral graphs.

Recall that by a work of Friedman, a random d-regular graph is a $\epsilon = \frac{2\sqrt{d-1}+o(1)}{d}$-spectral expander with probability $1 - 1/\mathrm{poly}(n)$[11, 6]. So, for a sufficiently large value of d, we can count the number perfect matchings in random d-regular graphs up to $1\pm\delta$-multiplicatively in time polynomial in $n, 1/\delta$. Furthermore, the above theorem implies that the Lovasz-Plummer Conjecture 1 holds for almost all graphs.

We remark our proof technique can naturally be extended to non-regular expanders where the ratio of maximum to minimum degree is bounded. However, in the following statement we show that if this ratio is unbounded the graph may not even have a single perfect matching.

▶ **Theorem 5.** *For $d \geq 3$, there exists $n_0 > 0$ such that for any $n \geq n_0$, there is a $O(1/\sqrt{d})$-spectral expander G on $2n$ vertices that does not have any perfect matchings.*

1.2 Related Works

Bollabás and McKay [5] showed that when $d = \Omega(\log^{1/3} n)$, as $d \to \infty$, a random d-regular graph contains $\Omega(d)^n$ many perfect matchings with probability at least $1 - 1/d^2$. Similar bounds are also implicitly given in the work of Robinson and Wormald [19], but to the best of our knowledge no explicit bound on the number of perfect matchings was known which holds almost surely as $n \to \infty$. Note that Theorem 4 implies that this statement is true with probability $1 - 1/\text{poly}(n)$ even if d is as small as a constant.

Chudnovsky and Seymour [7] proved that any planar cubic graph with no cut edge has at least $2^{n/655978752}$ many perfect matchings. Building on [7], Esperet, Kardos, King, Král, and Norine [9] showed that any d-regular $d-1$ edge connected graph has at least $2^{(1-3/d)\frac{n}{3656}}$ perfect matchings. Barvinok [2] showed that any 3-regular graph in which any set S with $2 \leq |S| \leq |V| - 2$ satisfies $|E(S, \overline{S})| \geq 4$ has at least c^n many perfect matchings for some universal constant $c > 1$.

Jerrum and Sinclair [14] showed the ratio of perfect to near perfect matchings in *bipartite* Erdös-Réyni graphs is polynomial in n. Thus, one can efficiently sample a perfect matching in such graphs. However, to the best of our knowledge, no such result is known for (non-bipartite) random graphs.

Barvinok [3] designed a randomized c^n approximation algorithm to the number of perfect matchings of any (general) graph, for some universal constant $c > 1$. Rudelson, Samarodnitsky, Zeitouni [20] showed that for a family of strong expander graphs Barvinok's estimator [3] has a sub-exponential variance, thus obtaining a randomized polynomial time sub-exponential approximation algorithm for the number of perfect matchings of any such graphs.

Gamarnik and Katz [12] designed a *deterministic* $(1+\epsilon)^n$ approximation algorithm to the number of perfect matching in expanding *bipartite* graphs.

1.3 Overview of Approach

At high-level our proof builds on works of [16, 12]. We show that given a non-perfect matching M in a (strong) expander graph G, one can find many augmenting paths of length $O(\log \frac{n}{n-|M|})$.

▶ **Lemma 6.** *Let G be a d-regular ϵ-spectral expander graph on $2n$ vertices for $\epsilon \leq 1/11$, and let M be any (not perfect) matching in G. Then there exist at least $\lceil (n - |M|)/2 \rceil$ augmenting paths in G of length at most $\rho = O\left(\max\left(\log_{1/\epsilon}(\frac{2\epsilon n}{n-|M|}), 1\right)\right)$ for ρ defined in Lemma 16.*

As alluded to in the introduction, the main difficulty in proving the above theorem is that since G is not necessarily bipartite, an augmenting walk cannot necessarily be turned into an augmenting path since it may have odd cycles. To avoid this issue, first we construct a random bi-partitioning of the vertices of G by placing the endpoints of each edge of M on opposite sides. We exploit the expansion property of G to argue that, under this random bi-partition, every set expands with high probability. So, one can start from two unsaturated vertices and follow "alternating BFS trees" from each until getting to a common middle point. The expansion property allows us to show that, with high probability, after $\log_{1/\epsilon} n$ steps we can construct an augmenting path. This method essentially tries to mimic the approach of [16] while exploiting the random partitioning. As an immediate corollary of the above lemma, we can upper bound the ratio of k to $k+1$ matchings in expanders.

▶ **Lemma 7.** *Let G be a d-regular ϵ-spectral expander graph on $2n$ vertices, and let $k \in [n]$. Let $m(j)$ denote the number of matchings of size j in G. Then we have*

$$\frac{m(k)}{m(k+1)} \leq \frac{2(k+1)}{n-k} d^{(\rho-1)/2}$$

for ρ defined in Lemma 16.

Building on [14], this lemma is already enough to prove Theorem 3.

To prove Theorem 4, we first show that for some constant $\epsilon > 0$, G has at least $\Omega(d)^n$ many $n(1-\epsilon)$-matchings. This part uses a greedy algorithm to find so many distinct matchings in an expander graph. Then, we exploit the above lemma to argue that the ratio of the number of $n(1-\epsilon)$ matchings of G to the number of its perfect matchings is at most $d^{O(\epsilon)n}$.

2 Preliminaries

Given a graph $G = (V, E)$ with $|V| = 2n$ and $k \in [n]$, a k-matching $M \subseteq E$ is any subset with $|M| = k$ and $e \cap e' = \emptyset$ for all $e \neq e' \in M$. For a set $S \subseteq V$, we write $G[S]$ to denote the *induced* subgraph on the set S. For a vertex $v \in V$, we write $\deg_G(v)$ to denote the degree of v in G.

Given a set of vertices $S \subseteq V$, define

$$M(S) := \{v : \exists u \in S, (u, v) \in M\}.$$

We also define $m_G(k)$ to denote the number of k-matchings in G.

Given a matching M, a walk $v_0, v_1, \ldots, v_k$ is an *alternating walk* for M if for any $1 \leq i \leq k-1$ exactly one of (v_{i-1}, v_i) and (v_i, v_{i+1}) is in M. An *augmenting path* for M is any alternating path that starts and ends with an unmatched vertex.

For a graph $G = (V, E)$ and $S, T \subseteq V$,

$$E_G(S, T) := \{(u, v) \in S \times T : (u, v) \in E\}.$$

For a set $S \subseteq V$, we write

$$N_G(S) := \{u \notin S : \exists u \in S, (u, v) \in E\}$$

to denote the set of all vertices outside S that has an edge to S. When the graph G is unambiguous from the context, we may drop the subscripts.

2.1 Spectral Graph Theory

The following facts are the main properties of spectral expanders that we will need.

▶ **Fact 8** (Expander Mixing Lemma). *Let G be a d-regular graph on $2n$ vertices. Then for any two sets $S, T \subseteq V$, we have*

$$\left| |E(S,T)| - \frac{d|S| \cdot |T|}{2n} \right| \leq d\sigma_2(\tilde{A})\sqrt{|S| \cdot |T|}$$

▶ **Lemma 9.** *Let $G = (V, E)$ be a $2n$-vertex d-regular ϵ-expander, and let $S \subseteq V$. The following holds: Then, there exists $v \in S$ such that* $\deg_{G[S]}(v) \geq \lceil d(|S|/2n - \epsilon) \rceil$.

Proof. By the Expander Mixing Lemma (Fact 8), we have $|E(S,S)| \geq \frac{d|S|^2}{2n} - d\epsilon|S|$. Hence the average degree of the vertices in $G[S]$ is at least $d(|S|/2n - \epsilon)$, and in particular there exists $v \in S$ whose degree in $G[S]$ is at least that much. ◀

▶ **Lemma 10** ([22])**.** *Let G be a d-regular ϵ-expander on $2n$ vertices. Then for any $S \subseteq V$ we have*

$$|N(S)| \geq \frac{|S|}{\epsilon^2 + (1-\epsilon^2)|S|/2n}$$

When $|S| \leq 2\epsilon n$, we immediately get the following corollary.

▶ **Corollary 11.** *Let G be a d-regular ϵ-expander on $2n$ vertices. Then for any $S \subseteq V$ with $|S| \leq 2\epsilon n$ we have*

$$|N(S)| \geq \frac{|S|}{\epsilon^2 + \epsilon - \epsilon^3} \geq \frac{|S|}{\epsilon^2 + \epsilon}.$$

2.2 Inequalities

▶ **Theorem 12** (Hoeffding's Inequality)**.** *Let $X_1, \ldots, X_k$ be independent random variables in the range $[0,1]$. Then,*

$$\mathbb{P}\left[\sum X_i < \mathbb{E}\sum X_i - \epsilon\right] \leq \exp(-2\epsilon^2/k).$$

▶ **Theorem 13** (Stirling's Formula)**.** *For $n \geq 1$ we have*

$$n! \geq \left(\frac{n}{e}\right)^n.$$

▶ **Theorem 14** (Weierstrass's Inequality)**.** *Let $0 < x_i < 1$ for $1 \leq i \leq n$. Then,*

$$\prod_{i=1}^{n}(1-x_i) \geq 1 - \sum_{i=1}^{n} x_i.$$

▶ **Theorem 15** (Hoffman-Wielandt's Inequality)**.** *Let $A, B \in \mathbb{R}^{n\times n}$ be symmetric matrices with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$ and $\lambda'_1 \geq \cdots \geq \lambda'_n$, respectively. We have*

$$\sum_{i=1}^{n}(\lambda_i - \lambda'_i)^2 \leq \|A - B\|_F^2,$$

where $\|\cdot\|_F$ denotes the Frobenius norm.

3 Proof of the Main Lemma

The following lemma is the main result of this section.

▶ **Lemma 16.** *Let $G = (V, E)$ be a d-regular ϵ-spectral expander graph on $2n$ vertices with $\epsilon \leq 1/11$, M be any (not perfect) matching in G, and U the set of unsaturated vertices (in M). For any partitioning of $U = U_L \cup U_R$ with $|U_L| = |U_R|$ there is an augmenting path from U_L to U_R of length at most $\rho = 4\max\left(\lceil \log_{C_1(\epsilon)}(\frac{2\epsilon n+1}{n-|M|}) \rceil, 0\right) + 1$, where $C_1(\epsilon) = \frac{1}{\epsilon+\epsilon^2}$.*

Before proving this lemma we use it to prove Lemma 6.

Proof of Lemma 6. Let U be the set of unmatched vertices of M and let U' be vertices of U that are not an endpoint to any augmenting path of length at most ρ. Observe that if $|U'| \leq n - |M|$, then there are at least $\lceil (n - |M|)/2 \rceil$ augmenting paths for M and we are done.

For the sake of contradiction suppose $|U'| > n - |M|$. Now arbitrarily partition U into two equal-sized sets $U_L \cup U_R$ (each of size exactly $n - |M|$) with the constraint that $U_L \subseteq U'$. So, by construction, no vertex in U_L is an endpoint of augmenting path of length at most ρ. But, by Lemma 16 there is an augmenting path from U_L to U_R of length at most ρ which is a contradiction. ◀

Proof of Lemma 7. Given a k-matching M, by Lemma 6 there are at least $(n - k)/2$ augmenting paths for M (in G) of length at most ρ for ρ defined in Lemma 16. Note that for any vertex v of G the number of paths of length at most ρ starting at v is at most d^{ρ}. Therefore, for any $k+1$-matching M', there are at most $2(k+1)d^{(\rho-1)/2}$ k-matchings that can be mapped to M'. This is because any such matching can be obtained by "undoing" an alternating path that starts and ends at the saturated vertices of M'. Together, these imply $\frac{m(k)}{m(k+1)} \leq \frac{2(k+1)d^{(\rho-1)/2}}{n-k}$. ◀

► **Definition 17** (Bipartition of G)**.** *Given a matching M and $\omega : M \to \{0,1\}$, we define the bipartite graph $G_M(\omega) = (L_M(\omega), R_M(\omega), E_M(\omega))$ as follows. We drop the subscript M and ω if they are clear in the context.*

All vertices of U_L are in L, all vertices of U_R are in R. For any edge $e = (u, v) \in M$, we add u to L and v to R if $\omega(e) = 0$ and we add u to R and v to L otherwise. We simply let $E_M(\omega)$ be all edges of E connecting L to R. We use μ_M to denote the uniform distribution over functions $M \to \{0,1\}$.

► **Lemma 18.** *Let $G = (V, E)$ be a graph with $2n$ vertices such that for every set $S \subseteq V$ with $|S| \leq 2\epsilon n$, $|N(S)| \geq \alpha|S|$ for $\alpha \geq 10$ and $0 < \epsilon < 1$. Given a non-perfect matching M and a partition of non-saturated vertices into equal sized sets U_L, U_R, if for $t = \max(\lceil \log_{\alpha/4} \frac{2\epsilon n+1}{|U_L|} \rceil, 0)$ there is no augmenting path of length at most $4t+1$ from U_L to U_R, then with probability $> 1/2$ (for $\omega \sim \mu_M$) there exists a set $S \subseteq L$ such that $|S| > 2\epsilon n$, and for every $v \in S$ there is an alternating path of length at most $2t$ from U_L to v in $G_M(\omega)$.*

Proof of Lemma 16. First, by Corollary 11, since G is an ϵ-spectral expander and $\epsilon < 1/11$, we can let $\alpha = 1/(\epsilon + \epsilon^2) \geq 10$. We prove the claim by contradiction. Suppose G has no augmenting path of length $\rho := 4t + 1$ from U_L to U_R, for t defined in Lemma 18. By Lemma 18, for $\omega \sim \mu$, with probability $> 1/2$ there is a set $S \subseteq L$ with $|S| > 2\epsilon n$, such that for any $v \in S$ there is an alternating path in $G_M(\omega)$ of length (at most) $2t$ from U_L to v. By renaming U_L, U_R, with probability $> 1/2$ there also exists another set $S' \subseteq R$ such that $|S'| > 2\epsilon n$ such that for every $v \in S'$, there is an alternating path of length at most $2t$ from U_R to v in $G_M(\omega)$. By union bound, with positive probability both of these sets exist. Now, by Fact 8 we have

$$|E(S, S')| \geq \frac{d|S| \cdot |S'|}{2n} - \epsilon d\sqrt{|S| \cdot |S'|} > d\sqrt{|S| \cdot |S'|}(\epsilon - \epsilon) = 0.$$

So there is an edge $(v, v') \in E(S, S')$. Now, the path formed by concatenating an alternating path from U_L to v of length $2t$, the edge (v, v'), and an alternating path from v' to U_R of length $2t$ we find alternating walk of length (at most) $\rho = 2t + 2t + 1$ from U_L to U_R in

$G_M(\omega)$. But since $G_M(\omega)$ is a bipartite graph this walk can only have even length cycles; by removing these cycles we obtain an alternating path of length at most ρ from U_L to U_R (in $G_M(\omega)$). ◀

In the rest of this section, we prove Lemma 18. First note that as $\alpha/4 > 1$, we have $\log_{\alpha/4} \frac{2\epsilon n+1}{|U_L|} \leq 0$ if and only if $|U_L| > 2\epsilon n$, and the claim is trivial in this case as we can set $S = U_L$. Now suppose $|U_L| \leq 2\epsilon n$. Let us fix an arbitrary ordering on the vertices of G. Given a bipartition $G_M(\omega)$, we define a sequence of sets $U_L = L_0 \subseteq L_1 \subseteq \ldots L_T \subseteq L$, and $\emptyset = X_0 \subseteq X_1 \subseteq \ldots X_T \subseteq V$, where T is a stopping time which is the minimum of t and the first time that $|L_T| > \epsilon n$. Given L_{i-1}, X_{i-1} for $i \geq 1$, we construct L_i, X_i as follows: If $|L_{i-1}| > 2\epsilon n$ then we stop and we let $T = i - 1$. Otherwise, $|L_{i-1}| \leq 2\epsilon n$ so by assumption of the lemma, $N(L_{i-1}) \geq \alpha|L_{i-1}|$. Let A_i be the lexicographically first $\alpha|L_{i-1}| - |X_{i-1}|$ neighbors of L_{i-1} which are not in X_{i-1}. In other words, we sort all neighbors of L_{i-1} which are not in X_{i-1} lexicographically and we let the first $\alpha|L_{i-1}| - |X_{i-1}|$ of them to be A_i. Note that as L_{i-1} has at least $\alpha|L_{i-1}|$ neighbors, there are at least $\alpha|L_{i-1}| - |X_{i-1}|$ "new" neighbors and so the set A_i is well-defined. We let $X_i = X_{i-1} \cup A_i$. Observe that by definition, we always have

$$|X_i| = \alpha|L_{i-1}|. \tag{1}$$

Finally, we let

$$L_i = L_{i-1} \cup M(A_i \cap R) = L_{i-1} \cup M(X_i \cap R).$$

The following fact follows inductively from the above construction

▶ **Fact 19.** *For every $1 \leq i \leq T$ and every $v \in L_i$, there is an alternating path of length at most $2i$ from $U_L = L_0$ to v in $G_M(\omega)$.*

▶ **Fact 20.** *For any $1 \leq i \leq T$, $L_{i-1} \cap M(A_i \cap R) = \emptyset$. Therefore,*

$$|L_i| = |L_{i-1}| + |A_i \cap R|.$$

Proof. For the sake of contradiction let $v \in M(A_i \cap R)$ such that $v \in L_{i-1}$ as well. Then, since v has a match, $v \notin U_L$; so we must have $i \geq 2$. Let $1 \leq j \leq i-1$ be the smallest index such that $v \in L_j$. That means that, by construction, $M(v) \in A_j \cap R$. Therefore, $M(v) \in X_j \subseteq X_{i-1}$. So, $v \notin M(A_i)$. ◀

Since in the above construction we only "look at" the first $\alpha|L_{i-1}| - |X_{i-1}|$ new neighbors of L_{i-1} to construct L_i, it follows that all edges which have no endpoints in these sets are conditionally independent. More precisely, we obtain the following Fact.

▶ **Fact 21.** *Let ω be chosen uniformly at random. For any $1 \leq i < t$, conditioned on $L_0, \ldots, L_{i-1}$, the law of ω on all edges that have no endpoints in L_{i-1}, X_{i-1} remain invariant, i.e., it is i.i.d., with expectation $1/2$ on each edge.*

▷ Claim 22. For $1 \leq i \leq T$,

$$\mathbb{P}_{\omega\sim\mu}\left[|A_i \cap R| \leq |A_i|/4 \mid L_0, \ldots, L_{i-1}\right] < \exp(-|A_i|/8).$$

Proof. Note that given $L_0, \ldots, L_{i-1}$, $X_1, \ldots, X_i$ and $A_1, \ldots, A_i$ are uniquely determined. Let $v \in A_i$. Consider the following cases:

- $v \in U_R$. This case cannot happen because we get an augmenting path of length $2i + 1$ to U_L which is a contradiction.

- $v \in L_{i-1}$. This cannot happen because $v \in N(L_{i-1})$. This in particular shows $v \notin U_L$. So, v has a match in M.
- $M(v) \in A_i$. Then, by Definition 17 exactly one of $v, M(v)$ is in R.
- $M(v) \in X_{i-1}$. If $M(v) \in R$ then we must have $v \in L_{i-1}$ which cannot happen as we said in case (2). Otherwise, $M(v) \in L$, so $v \in R$.
- $M(v) \in L_{i-1}$. Then, $v \in R$.
- $v \notin L_{i-1}, M(v) \notin X_i, L_{i-1}$. In this case since $v \in A_i$, by Fact 21, $v \in R$ with probability $1/2$ independent of all other vertices of A_i.

Let A'_i be the set of vertices v that fall into the last case. Say we have a Bernoulli B_v with success probability $1/2$ for every $v \in A'_i$. Then, by above discussion, conditioned on $L_0, \dots, L_{i-1}$, with probability 1,

$$|A_i \cap R| \geq |A_i \setminus A'_i|/2 + \sum_{v \in A'_i} B_v.$$

Therefore, by the Hoeffding bound (Theorem 12)

$$\begin{aligned}\mathbb{P}\left[|A_i \cap R| \leq |A_i/4| \mid L_0, \dots, L_{i-1}\right] &\leq \mathbb{P}\left[\sum_{v \in A'_i} B_v \leq |A'_i|/2 - |A_i|/4 \,\middle|\, L_0, \dots, L_{i-1}\right] \\ &\leq \exp(-|A_i|^2/8|A'_i|) \leq \exp(-|A_i|/8)\end{aligned}$$

as desired. ◁

Since $|L_1| \geq |A_1 \cap R|$ and $|A_1| = \alpha|L_0|$,

$$\begin{aligned}\mathbb{P}_\mu\left[|L_1| \geq (\alpha/4)|L_0|\right] &\geq \mathbb{P}_\mu\left[|A_1 \cap R| \geq (\alpha/4)|L_0|\right] \\ &= \mathbb{P}_\mu\left[|A_1 \cap R| \geq |A_1|/4\right] \geq 1 - \exp(-|A_1|/8) = 1 - \exp(-\alpha|L_0|/8)\end{aligned} \tag{2}$$

where the last inequality follows form Claim 22.

▷ Claim 23. Let ω be chosen uniformly at random. For every $2 \leq i \leq T$, we have

$$\mathbb{P}_\mu\left[|L_i| \geq (\alpha/4)|L_{i-1}| \,\middle|\, |L_{i-1}| \geq (\alpha/4)|L_{i-2}|, L_0, \dots, L_{i-1}\right] \geq 1 - \exp(-(\alpha-4)|L_{i-1}|/8).$$

Proof. Suppose $|L_{i-1}| \geq (\alpha/4)|L_{i-1}|$. Recall that by Equation (1) we have $|X_i| = \alpha|L_{i-1}|$. So we can write

$$\begin{aligned}|A_i| = |X_i \setminus X_{i-1}| &= \alpha(|L_{i-1}| - |L_{i-2}|) \\ &\geq \alpha(1 - 4/\alpha)|L_{i-1}| \\ &= (\alpha - 4)|L_{i-1}|.\end{aligned} \tag{3}$$

Let μ' be μ conditioned on $|L_{i-1}| \geq (\alpha/4)|L_{i-2}|$ and $L_0, \dots, L_{i-1}$. Then,

$$\begin{aligned}\mathbb{P}_{\mu'}\left[|L_i| \leq (\alpha/4)|L_{i-1}|\right] &= \mathbb{P}_{\mu'}\left[|L_i| - |L_{i-1}| \leq (\alpha/4 - 1)|L_{i-1}|\right] \\ &= \mathbb{P}_{\mu'}\left[|A_i \cap R| \leq (\alpha/4 - 1)|L_{i-1}|\right] && \text{(Fact 20)} \\ &\leq \mathbb{P}_{\mu'}\left[|A_i \cap R| \leq |A_i|/4\right] && \text{(Equation (3))} \\ &\leq \exp(-|A_i|/8) && \text{(Claim 22)} \\ &\leq \exp(-(\alpha-4)|L_{i-1}|/8), && \text{(Equation (3))}\end{aligned}$$

completing the proof. ◁

▷ Claim 24. If $\alpha \geq 10$, for any $i \geq 1$ we have

$$\mathbb{P}_\mu\left[T < i \vee (T \geq i \wedge |L_i| \geq (\alpha/4)^i |L_0|)\right] > 1/2.$$

Proof. For $1 \leq j \leq i$, let E_j denote the event that $T < j \vee (T \geq j \wedge |L_j| \geq (\alpha/4)|L_{j-1}|)$. Then,

$$\begin{aligned}
\mathbb{P}[E_i] &\geq \mathbb{P}[E_1 \wedge \cdots \wedge E_i] \\
&= \mathbb{P}[E_1] \prod_{j=2}^{i} \mathbb{P}\left[E_j | E_1, \ldots, E_{j-1}\right] \\
&\geq (1 - \exp(-\alpha |L_0|/8)) \prod_{j=2}^{i} \Big(\mathbb{P}\left[T < j | E_1, \ldots, E_{j-1}\right] \\
&\quad + \mathbb{P}\left[T \geq j | E_1, \ldots, E_{j-1}\right] \mathbb{E}\left[1 - \exp\left(\frac{-(\alpha-4)|L_{j-1}|}{8}\right) \,\middle|\, E_1, \ldots, E_{j-1}, T \geq j\right]\Big) && \text{(Claim 23)} \\
&\geq (1 - \exp(-\alpha |L_0|/8)) \prod_{j=2}^{i} \left(1 - \exp\left(\frac{-(\alpha-4)}{8} (\alpha/4)^{j-1} |L_0|\right)\right) \\
&\geq 1 - \exp(-\alpha/8) - \sum_{j=2}^{i} \exp(-\frac{\alpha-4}{8} (\alpha/4)^{j-1}) && \text{(Theorem 14)} \\
&\geq 1 - e^{-\alpha/8} - \sum_{j=0}^{\infty} e^{-\beta(\alpha/4)^j} && (\text{for } \beta = \tfrac{\alpha(\alpha-4)}{32}) \\
&\geq 1 - e^{-\alpha/8} - \frac{e^{-\beta}}{1 - e^{-\beta(\alpha/4-1)}} > 1/2. && (\alpha \geq 10)
\end{aligned}$$

Note that in the third inequality we crucially use that if $E_1, \ldots, E_{j-1}$ occur then either $T < j$, or $T \geq j$ and $|L_j| \geq (\alpha/4)^{j-1}$. ◁

Setting $t = \lceil \log_{\alpha/4} \frac{2\epsilon n+1}{|U_L|} \rceil$ by the above statement we get $\mathbb{P}[T < t \vee (T = t \wedge |L_t| > 2\epsilon n)] > 1/2$. This completes the proof of Lemma 18.

4 Completing the Proofs of Theorems 3 and 4

4.1 The Lower-Bound

▶ **Lemma 25.** *Let $G = (V, E)$ be an $2n$-vertex d-regular ϵ-expander. If $\epsilon < 1/2$, then we have,*

$$m((1-\epsilon)n) \geq \left(\frac{d}{e}\right)^{n(1-\epsilon)} \cdot e^{-2\epsilon n}.$$

Proof. Let $k = n(1-\epsilon)$. We call a sequence of integers $\langle a_1, \ldots, a_k \rangle$ *valid* if $1 \leq a_i \leq \lceil d((n-i+1)/n - \epsilon) \rceil$ for all $1 \leq i \leq k$.

Now, for valid sequence $a = \langle a_1, \ldots, a_k \rangle$, we construct a k-matching $\mathcal{M}(a)$ as follows: We are going to construct a sequence of matchings $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k$, with the property that for $1 \leq i \leq k$, M_i is going to be a matching of size i in G. We then set $\mathcal{M}(a) := M_k$. We start with $M_0 = \emptyset$. For $i \geq 1$, given M_{i-1}, let S_i be the set of unmatched vertices of G with respect to M_{i-1}. Note that by construction M_{i-1} is a matching of size $i-1$, so we have $|S_i| = 2n - 2(i-1)$. Further let $\Delta_i = \max_{u \in S} \deg_{G[S_i]}(u)$, and and let u_i denote the lexicographically first vertex with degree Δ_i in S_i. Note that by Lemma 9, it should be that $\Delta_i \geq \lceil d((n-i+1)/n - \epsilon) \rceil$, and furthermore, by validity of a we obtain $a_i \leq \Delta_i$. Now let let v_i be the a_i-th neighbor of u_i in $G[S_i]$ with respect to the lexicographical order. We set $M_i = M_{i-1} \cup \{(u_i, v_i)\}$. In the next claim we show that any distinct pair of valid sequences give distinct k-matchings. Therefore, the number of k-matchings of G is at least,

$$\prod_{i=1}^{k} (d\frac{n-i+1}{n} - d\epsilon) \geq d^k \prod_{i=1}^{k} \frac{n-i+1-\epsilon n}{n} \geq d^k \frac{k!}{n^k} \geq (d/e)^k \cdot (k/n)^k,$$

where the last inequality uses Theorem 13. By plugging in $k = (1-\epsilon)n$ we obtain

$$m((1-\epsilon)n) \geq (d/e)^{(1-\epsilon)n} \cdot (1-\epsilon)^{(1-\epsilon)n} \geq (d/e)^{(1-\epsilon)n} \cdot e^{-\epsilon n},$$

where in the last inequality we used that $(1-\epsilon)^{1-\epsilon} \geq e^{-\epsilon}$ for $\epsilon \leq 1/2$. ◀

▷ Claim 26. For any distinct valid sequences $a = \langle a_1, \ldots, a_k \rangle$ and $b = \langle b_1, \ldots, b_k \rangle$ we have $\mathcal{M}(a) \neq \mathcal{M}(b)$.

Proof. Since $a \neq b$ there is an index $1 \leq i \leq k$ such that $a_i \neq b_i$; let $1 \leq i \leq k$ be the first such index. Since $a_j = b_j$ for $1 \leq j \leq i-1$, by the above construction we have $S_i(a) = S_i(b)$. So, we would choose a unique vertex u_i in both constructions but we match it to different vertices, since $a_i \neq b_i$. Therefore $\mathcal{M}(a) \neq \mathcal{M}(b)$. ◁

▶ **Lemma 27.** *Let G be a $2n$ vertex d-regular, ϵ-spectral expander for $\epsilon \leq 1/11$. We have,*

$$\frac{m((1-\epsilon)n)}{m(n)} \leq (2e/\epsilon)^{\epsilon n} d^{2\epsilon n + (4\epsilon n+2)/\ln C_1(\epsilon)}.$$

where $C_1(\epsilon)$ is defined in Lemma 16.

Proof. For $k = \epsilon n$, we can write

$$\begin{aligned}\frac{m(n(1-\epsilon))}{m(n)} = \prod_{i=n-k}^{n-1} \frac{m(i)}{m(i+1)} &\leq \prod_{i=n-k}^{n-1} \frac{2(i+1)}{n-i} d^{2\log_{C_1(\epsilon)} \frac{2\epsilon n+1}{n-i} + 2} && \text{(Lemma 7)}\\ &\leq \frac{2^k n^k d^{2k}}{k!} d^{2\sum_{i=1}^{\epsilon n} \log_{C_1(\epsilon)} \frac{2\epsilon n+1}{i}}\\ &\leq (2ed^2 n/k)^k d^{2\log_{C_1(\epsilon)} \frac{(2k+1)^k}{k!}} \leq (2ed^2n/k)^k d^{(4k+2)/\ln C_1(\epsilon)},\end{aligned}$$

where in the second to last inequality we used Theorem 13 and in the last inequality we used $\frac{(2k+1)^k}{k!} = \frac{k^k}{k!}(2+1/k)^k \leq e^{2k+1}$. Plugging $k = \epsilon n$ into the above inequality proves the claim. ◀

Proof of Theorem 4. Using Lemmas 25 and 27 and using for $\epsilon \leq 1/11$, $\ln(C_1(\epsilon)) \geq 2$, we can write

$$m(n) \geq \frac{e^{-\epsilon n}(d/e)^{n(1-\epsilon)}}{(2e/\epsilon)^{\epsilon n} d^{2\epsilon n + (4\epsilon n+2)/\ln C_1(\epsilon)}} \geq \left(\frac{d}{e}\right)^n \left(\frac{\epsilon}{2e^3 d^6}\right)^{\epsilon n}$$

as desired. ◀

4.2 Sampling / Counting Perfect Matchings

As an immediate corollary of Lemma 7 we prove Theorem 3. In particular,

$$\frac{m(n-1)}{m(n)} \leq 2nd^{2\log_{C_1(\epsilon)}(2\epsilon n+1)+2} \tag{4}$$

So, it follows from the following theorem of [14] that for any $\delta > 0$ we can sample a perfect matching of G from a distribution μ of total variation distance δ of the uniform distribution in time $\operatorname{poly}(n^{\frac{\log d}{\log \epsilon^{-1}}}, \log(1/\delta))$.

▶ **Theorem 28** (Jerrum and Sinclair [14, Thm 3.6]). *Let G be a graph with $2n$ vertices. There is a Markov chain with a uniform stationary distribution on the space n and $n-1$ matchings of G such that that mixes in time $\operatorname{poly}(n, \frac{m(n-1)}{m(n)})$.*

Furthermore, Jerrum and Sinclair [14, Thm 5.3] showed how to estimate the number of perfect matchings up to $1 \pm \delta$ multiplicative factor in time $\operatorname{poly}(n, 1/\delta, \frac{m(n-1)}{m(n)})$. So, plugging in Equation (4) into their theorem also allows us to approximate the number of perfect matchings (up to $1 \pm \delta$ multiplicatively) in ϵ-expander regular graphs in time $\operatorname{poly}(n^{\frac{\log d}{\log \epsilon^{-1}}}, 1/\delta)$.

5 A Non-regular Counter-example

In this section we construct an infinite family of *non-regular* strong spectral expanders that do not have any perfect matchings. This shows that the regularity assumption in Theorem 4 is necessary.

▶ **Lemma 29.** *Given a d-regular graph $G = (V, E)$ with $2n$ vertices, there exists a graph $H = (V', E')$ with $2n + 2$ vertices such that*

- *H does not have any perfect matchings.*
- *$\sigma_2(\tilde{A}_H) \leq \sigma_2(\tilde{A}_G) + \sqrt{5/d}$.*
- *H has $2n - 1$ vertices of degree d, one vertex of degree $d + 2$, and two vertices of degree 1.*

Proof. Say $V = \{v_1, \ldots, v_{2n}\}$. To construct H, we add two new vertices v_{2n+1}, v_{2n+2} and we connect both of them to v_{2n}. Clearly H has no perfect matchings. We abuse notation and extend the normalize adjacency matrix of G, $\tilde{A}_G$ by adding two all-zeros rows and two all-zeros columns. Clearly, only introduces two new zero eigenvalues, and the $\sigma_2(\tilde{A}_G)$ remains invariant. It follows by a simple calculation that

$$\|\tilde{A}_G - \tilde{A}_H\|_F^2 = 2(d-1) \cdot \left(\frac{1}{d(d+1)}\right)^2 + 4\left(\frac{1}{\sqrt{d+1}}\right)^2 \leq \frac{2}{d^3} + \frac{4}{d} \leq \frac{5}{d}.$$

Therefore, by Theorem 15, for any $1 \leq i \leq 2n + 2$ we have

$$|\lambda_i(\tilde{A}_G) - \lambda_i(\tilde{A}_H)|^2 \leq \sum_{j=1}^{2n+2} |\lambda_j(\tilde{A}_G) - \lambda_j(\tilde{A}_H)|^2 \leq \|\tilde{A}_G - \tilde{A}_H\|_F^2 \leq 5/d.$$

Therefore we obtain $\sigma_2(\tilde{A}_H) \leq \sigma_2(\hat{A}_G) + \sqrt{5/d}$. ◀

Recall by the work Friedman [11, 6] for $d \geq 3$ and sufficiently large n, there exists a d-regular $\left(\frac{2\sqrt{d-1}}{d} + o(1)\right)$-expander $G_{2n,d}$ on $2n$ vertices. Theorem 5 is immediate.

References

1 N. Anari, S. Oveis Gharan, and C. Vinzant. Log-concave polynomials i: Entropy and a deterministic approximation algorithm for counting bases of matroids. *Duke Mathematical Journal*, 2021. to appear.

2 Alexander Barvinok. A bound for the number of vertices of a polytope with applications. *Combinatorica*, 33(1):1–10, 2013.

3 Alexander I. Barvinok. Polynomial time algorithms to approximate permanents and mixed discriminants within a simply exponential factor. *Random Struct. Algorithms*, 14(1):29–61, 1999.

4 Ivona Bezáková, Daniel Stefankovic, Vijay V. Vazirani, and Eric Vigoda. Accelerating simulated annealing for the permanent and combinatorial counting problems. In *SODA*, pages 900–907. ACM Press, 2006.

5 Béla Bollobás and Brendan D McKay. The number of matchings in random regular graphs and bipartite graphs. *Journal of Combinatorial Theory, Series B*, 41(1):80–91, 1986.

6 Charles Bordenave. A new proof of Friedman's second eigenvalue Theorem and its extension to random lifts. *Annales scientifiques de l'Ecole normale supérieure*, 2019.

7 M. Chudnovsky and P Seymour. Perfect matchings in planar cubic graphs. *Combinatorica*, 32:403–424, 2012.

8 G.P. Egorychev. The solution of van der waerden's problem for permanents. *Advances in Math.*, 42:299–305, 1981.

9 Louis Esperet, František Kardoš, Andrew D. King, Daniel Král, and Serguei Norine. Exponentially many perfect matchings in cubic graphs. *Advances in Mathematics*, 227(4):1646–1664, July 2011.

10 D. I. Falikman. Proof of the van der waerden's conjecture on the permanent of a doubly stochastic matrix. *Mat. Zametki*, 29(6):931–938, 1981. (in Russian).

11 J. Friedman. A proof of alon's second eigenvalue conjecture and related problems. *Mem. Amer. Math. Soc.*, 195(910), 2008.

12 David Gamarnik and Dmitriy Katz. A deterministic approximation algorithm for computing the permanent of a 0,1 matrix. *Journal of Computer and System Sciences*, 76(8):879–883, 2010.

13 Leonid Gurvits. Hyperbolic polynomials approach to van der waerden/schrijver-valiant like conjectures: sharper bounds, simpler proofs and algorithmic applications. In Jon M. Kleinberg, editor, *STOC*, pages 417–426. ACM, 2006.

14 Mark Jerrum and Alistair Sinclair. Approximating the permanent. *SIAM journal on computing*, 18(6):1149–1178, 1989.

15 Mark Jerrum, Alistair Sinclair, and Eric Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *Journal of the ACM (JACM)*, 51(4):671–697, 2004.

16 Mark Jerrum and Umesh V. Vazirani. A mildly exponential approximation algorithm for the permanent. *Algorithmica*, 16(4/5):392–401, 1996.

17 N. Linial, A. Samorodnitsky, and A. Wigderson. A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents. *Combinatorica*, 20:545–568, 2000.

18 L. Lovász and M.D. Plummer. *Matching Theory*. Elsevier Science, 1986.

19 Robert W. Robinson and Nicholas C. Wormald. Almost all regular graphs are hamiltonian. *Random Structures & Algorithms*, 5(2):363–374, 1994.

20 Mark Rudelson, Alex Samorodnitsky, and Ofer Zeitouni. Hafnians, perfect matchings and gaussian matrices. *Ann. Probab.*, 44(4):2858–2888, July 2016.

21 A. Schrijver. Counting 1-factors in regular bipartite graphs. *Journal of Combinatorial Theory*, B 72:122–135, 1998.

22 R Michael Tanner. Explicit concentrators from generalized n-gons. *SIAM Journal on Algebraic Discrete Methods*, 5(3):287–293, 1984.