Local Statistics, Semidefinite Programming, and Community Detection

Jess Banks [*] Sidhanth Mohanty [†] Prasad Raghavendra[‡]

October 31, 2019

Abstract

We propose a new hierarchy of semidefinite programming relaxations for inference problems, inspired by recent ideas of 'pseudocalibration' in the Sum-of-Squares literature. As a test case, we consider the problem of community detection in a distribution of random regular graphs we'll call the Degree Regular Block Model , wherein the vertices are partitioned into k communities, and a graph is sampled conditional on a prescribed number of inter- and intra-community edges. The problem of *detection*, where we are to decide with high probability whether a graph was drawn from this model or the uniform distribution on regular graphs, is conjectured to undergo a computational phase transition at a point called the Kesten-Stigum (KS) threshold, and we show (i) that sufficiently high constant levels of our hierarchy can perform detection arbitrarily close to this point, (ii) that our algorithm is robust to $o(n)$ adversarial edge perturbations, and (iii) that below Kesten-Stigum no level constant level can do so.

In the more-studied case of the (irregular) Stochastic Block Model, it is known that efficient algorithms exist all the way down to this threshold, although none are robust to adversarial perturbations of the graph when the average degree is small. More importantly, there is little complexity-theoretic evidence that detection is hard below Kesten-Stigum. In the RSBM with more than two groups, it has not to our knowledge been proven that any algorithm succeeds down to the KS threshold, let alone that one can do so robustly, and there is a similar dearth of evidence for hardness below this point.

Our SDP hierarchy is highly general and could potentially be useful for a wide range of hypothesis testing problems.

[*]University of California, Berkeley
[†]University of California, Berkeley
[‡]University of California, Berkeley

1 Introduction

Community detection in graphs is a canonical and widely applicable problem in computer science and machine learning. The setup is both simple and flexible: we are shown a graph and asked for a coarse-grained description in the form of a partition of the vertices into 'communities' with atypically many internal edges. The literature contains innumerable algorithms and approaches for this task, but perhaps the most fruitful has been a Bayesian perspective wherein we treat the graph as the output of some generative model, whose unknown parameters we attempt to estimate. In other words, we assume that there are some true and hidden community labels, and that the graph has been drawn probibalistically in a way that respects this 'planted' structure.

Much of the existing literature on community detection concerns the *stochastic block model (SBM)*. For now let us discuss the symmetric setting where we first partition n vertices in to k groups, and include each edge independently and with probability p_{in} or p_{out} depending on whether or not the labels of its endpoints coincide. Research in this area spans several decades, and it will not be fruitful to attempt a thorough review of the literature here; we refer the reader to [cite] for a survey. Most salient to us, however, is a rich theory of computational threshold phenomena which has emerged out of the past several years of collaboration between computer scientists, statisticians, and statistical physicists.

The key computational tasks associated with the SBM are *recovery* and *detection*: we attempt either to reconstruct the planted communities from the graph, or to decide whether a graph was drawn from the planted model or the Erdős-Rényi model with the same average degree. A set of fascinating conjectures were posed in Decelle et al.[DKMZ11], regarding these tasks in the case of 'sparse' models where $p_{\text{in}}, p_{\text{out}} = O(1/n)$ and the average degree is $O(1)$ as the number of vertices diverges.

It is typical to parametrize the symmetric SBM in terms of k, the average degree

$$d = \frac{np_{\text{in}} + (k-1)np_{\text{out}}}{k},$$

and a 'signal-to-noise ratio'

$$\lambda \triangleq \frac{np_{\text{in}} - np_{\text{out}}}{kd}.$$

In this setup, it is believed that as we hold k and λ constant, then there is an *information-theoretic threshold* $d_{\text{IT}} \approx \frac{\log k}{k\lambda^2}$, in the sense that when $d < d_{\text{IT}}$ both detection and recovery are impossible for any algorithm. Moreover, Decelle et al. conjecture that efficient algorithms for both tasks exist only when the degree is larger than a point known as the *Kesten-Stigum threshold* $d_{\text{KS}} = \lambda^{-2}$. Much of this picture is now rigorous [MNS18, Mas14, BLM15, ABH16]. Still, fundamental questions remain unanswered. What evidence can we furnish that detection and recovery are indeed intractible in the so-called 'hard regime' $d_{\text{IT}} < d < d_{\text{KS}}$? How robust are these thresholds to adversarial noise or small deviations from the model?

Zooming out, this discrepancy between information-theoretic and computational thresholds is conjectured to be quite universal among planted problems, where we are to reconstruct or detect a structured, high-dimensional signal observed through a noisy channel [citaions]. The purpose behind our work is to begin developing a framework capable of providing evidence for average case computational intractability in such settings. To illustrate this broader motivation, consider a different average-case problem also conjectured to be computationally intractable: refutation of random 3-SAT. A random instance of 3-SAT with n literals and, say $m = 1000n$ clauses is unsatisfiable with high probability. However, it is widely conjectured that the problem of *certifying* that a given random 3-SAT instance is unsatisfiable is computationally intractable (all the way up to $n^{3/2}$ clauses) [Fei02]. While proving intractability remains out of

reach, the complexity theoretic literature now contains ample evidence in support of this conjecture. Most prominently, exponential lower bounds are known for the problem in restricted computational models such as linear and semidefinite programs [Gri01] and resolution based proofs [BSW01]. Within the context of combinatorial optimization, the Sum-of-Squares (SoS) SDPs yield a hierarchy of sucessively more powerful and complex algorithms which capture and unify many other known approaches. A lower bound against the SoS SDP hierarchy such as [Gri01] provides strong evidence that this refutation problem is computationally intractable. This paper is a step towards developing a similar framework to reason about the computational complexity of detection and recovery in stochastic block models specifically, and planted problems generally.

Mention Sam/David/et work here?

A second motivation is the issue of robustness of computational thresholds under adversarial perturbations of the graph. Spectral algorithms based on non-backtracking walk matrix [BLM15] achieve weak-detection as soon as $d > d_{KS}$, but are not robust in this sense. Conversely, robust algorithms for recovery are known, but only when the edge-densities are significantly higher than Kesten-Stigum [GV16, MMV16, CSV17, SVC16]. The positive result that gets closest to robustly achieving the conjectured computational phase transition at d_{KS} is the work of Montanari and Sen [MS15] who observe that their SDP-based algorithm for testing whether the input graph comes from the Erdős-Rényi distribution or a Stochastic Block Model with $k = 2$ communities also works in presence of $o(|E|)$ edge outlier errors. On the negative side, Moitra et al. [Moi12] consider the problem of weak recovery in a SBM with two communities and $p_{in} > p_{out}$ in the presence of *monotone errors* that add edges within communities and delete edges between them. Their main result is a statistical lower bound indicating the phase transition for weak recovery changes in the presence of monotone errors. This still leaves open the question of whether there exist algorithms that weakly recover right at the threshold and are robust to $o(|E|)$ perturbations in the graph.

Cite recent result on robustness?

2 Main Results

We define a new hierarchy of semidefinite programming relaxations for inference problems that we refer to as the *Local Statistics* hierarchy, denoted $\mathrm{LoSt}(D_1, D_2)$ and indexed by parameters $D_1, D_2 \in \mathbb{N}$. This family of SDPs is inspired by the technique of pseudocalibration in proving lower bounds for sum-of-squares (SoS) relaxations, as well as subsequent work of Hopkins and Steurer [HS17] extending it to an SoS SDP based approach to inference problems. The LoSt hierarchy can be defined for a broad range of inference problems involving a joint distribution μ on an observation and hidden parameter.

As a test case, we apply our SDP relaxations to community detection in the *Degree Regular Block Model (DRBM)*, a family of distributions over degree regular graphs with planted community structure. The degree-regularity will simplify some aspects of our analysis, allowing us to illustrate key features of the LoSt hierarchy without a proliferation of technicalities. We will comment later on about the possibilities for extension to the irregular case. As an aside, we cannot help but editorialize briefly that, although the DRBM is less useful in practice than the standard block model discussed above, its combinatorics are intricate and beautiful in their own right, and the related case of d-regular graphs with planted colorings have been quite well-studied [citations].

We will specify the DRBM on n vertices in full generality by several parameters: the number of communities k, degree d, and a $k \times k$ transition matrix M for a reversible Markov chain, with stationary distribution π. In other words, M has row sums equal to one, and $\mathrm{Diag}(\pi)M$ is a symmetric matrix. To sample a

graph $\mathbf{G} = (\mathbf{V}, \mathbf{E})$—we will use bold-face type for random objects throughout the paper—first partition the n vertices randomly into k groups $\mathbf{V}_1, ..., \mathbf{V}_k$ with $|\mathbf{V}_i| = \pi(i)n$, and then choose a d-regular random graph conditional on there being $\pi(i)M_{i,j}dn$ edges between groups $i \neq j$ and $\pi(i)M_{i,i}dn/2$ internal to each group i. As $\mathrm{Diag}(\pi)M$ is symmetric, this process is well-defined. We will assume always that the parameters are set to make these quantities integer-valued; settings for which this holds infinitely often as $n \to \infty$ are dense in the parameter space.

Remark 2.1. The DRBM as we have defined it differs from the Regular Stochastic Block Model of [cite], in which each vertex has a prescribed number of neighbors in every community. Although superficially similar, the behavior of this 'equitable' model (as it is known in the physics literature [cite]) is quite different from ours. For instance, [cite] show that whenever detection is possible, one can recover the community labels *exactly*. This is not true in our case.

Sketch why. Also should we change the name?

The DRBM contains several more familiar distributions as special cases, and the reader is welcome to focus on her favorite for concreteness. When $\pi(i) = 1/k$ for every i, we have the DRBM with equal groups. Setting $M_{i,i} = 0$ and $M_{i,j} = \frac{1}{k-1}$, we are in a somewhat restrictive case of the planted k-coloring model, where each pair of color classes has the same number of edges between them. We will refer to the case when $M_{i,i} = m_{\text{in}}$ and m_{out} otherwise as the symmetric DRBM . As M describes a reversible Markov chain, its spectrum is real, and we will write its eigenvalues as $1 = \lambda_1 \geq |\lambda_2| \geq \cdots \geq |\lambda_k|$. The second eigenvalue λ_2 can be thought of as a kind of signal-to-noise ratio, and will be repeatedly important to our analysis. One can verify, for instance, that in the case of the symmetric RSBM, $\lambda_2 = \cdots = \lambda_n = m_{\text{in}} - m_{\text{out}}$.

It is widely believed that the threshold behavior of the DRBM is similar to that of the SBM, though the inhomogeneities in group size and edge density we allow for make the situation somewhat more complicated than in the symmetric case discussed earlier. This phenomenology includes an information-theoretic threshold $d_{\text{IT}} \approx \frac{\log k}{k\lambda_2^2}$ for the symmetric DRBM (and a more complicated characterization in general that will not be relevant to us here). In the general model, the Kesten-Stigum threshold for *detection* is $d_{\text{KS}} \triangleq \lambda_2^{-2} + 1$, and we expect recovery of *all* communities once $d > 1/\lambda_k^2 + 1$. However, most formal treatment in the literature has been limited to the distribution of d-regular graphs conditional on having a planted k-coloring, a case not fully captured by our model [citations]. Characterization of the information-theoretic threshold, even for the symmetric DRBM remains largely folklore, and in Appendix [ref] we will for good measure provide a few rigorous pieces of the picture.

Our main theorem is that the the Local Statistics hierarchy can robustly solve the detection problem on the DRBM whenever $d > d_{\text{KS}}$, but that otherwise any constant level fails to do so.

Theorem 2.2. *For every $\epsilon > 0$, and set of parameters (d, k, M, π) satisfying $d > d_{\text{KS}} + \epsilon = 1/\lambda_2^2 + 1 + \epsilon$, there exists $m \in \mathbb{N}$ sufficiently large so that with probability $1 - o(1)$ the $\mathrm{LoSt}(2, m)$ SDP, given an input graph $\mathbf{G}$, can distinguish in time [need] whether*

- *$\mathbf{G}$ is a uniformly random d-regular graph*
- *$\mathbf{G}$ is sampled from the DRBM with parameters (d, k, M, π)*

and is robust to adversarial addition or deletion of $o(n)$ edges. On the other hand, for any constant m and $d < d_{\text{KS}}$, the $\mathrm{LoSt}(2, m)$ SDP fails with probability $1 - o(1)$ to distinguish.

We also prove a stronger robustness guarantee, in particular that that $\mathrm{LoSt}(2, m)$ can tolerate $\epsilon_m n$ adversarial edge perturbations, although $\epsilon_m \to 0$ as we move up the hierarchy. This creates a trade-off

between robustness, which we lose as added information is incorporated to the SDP at each successive level, and fidelity to the threshold, which we approach as $m \to \infty$.

Theorem 2.3. *For every $\epsilon > 0$, there exists $\delta > 0$ and m sufficiently large, so that even given a graph $\tilde{\mathbf{G}}$ which is a $\delta|E|$-perturbation of the edges of some $\mathbf{G}$, $\mathrm{LoSt}(2, m)$ can be used to distinguish whether $\mathbf{G}$ is a uniformly random d-regular graph or was drawn from an RSBM ϵ-away from the threshold.*

Along the way we will inadvertently prove that standard spectral detection using the adjacency matrix succeeds above d_{KS}, but cannot have the same robustness guarantee. It is a now-classic result of Friedman that, with probability $1 - o_n(1)$, the spectrum of a uniformly random d-regular graph is within $o_n(1)$ of $(-2\sqrt{d-1}, 2\sqrt{d-1}) \cup \{d\}$. Conversely, we show:

Corollary 2.4. *Let $\mathbf{G}$ be drawn from the RSBM with parameters (d, k, M, π), and set $\epsilon > 0$. There exists some $\delta = \delta(\epsilon)$ such that, for each eigenvalue λ of M satisfying $|\lambda| > 1/\sqrt{d-1} + \epsilon$, the adjacency matrix $A_{\mathbf{G}}$ is guaranteed one eigenvalue μ satisfying $|\mu| > 2\sqrt{d-1} + \delta$.*

Regrettably, we do not resolve to similar satisfaction the issue of efficient or robust recovery above Kesten-Stigum. The eigenvectors guaranteed to us by Theorem [ref] are certainly correlated to the community structure, and we can prove that the Local Statistics hierarchy can robustly approximate them:

Theorem 2.5. *In any planted model $\mathcal{P}$ for which the $\mathrm{LoSt}(2, m)$ hierarchy can solve the distinguishing problem, it can robustly approximate the eigenvectors outside the bulk of $A_{\mathbf{G}}$, for $\mathbf{G} \sim \mathcal{P}$, in the sense that [finish].*

However, the remaining and technically challenging ingredient is a proof that graphs drawn from the planted model do not accumulate *additional*, spurious eigenvalues outside the bulk. From weak convergence of the empirical spectral distribution of $A_{\mathbf{G}}$ to the Kesten-McKay law, we know that there must be $o(n)$ eigenvalues with modulus larger than $2\sqrt{d-1}$, but the guarantee of Theorem [ref] only kicks in once there are, i.e. $O(1)$ of them. We believe the following conjecture feasible to prove with a careful mirroring of the techniques in [ref Bordenave], but the execution of this is beyond the scope of the current work.

Conjecture 2.6. *Let $\mathcal{P}_{(d,k,M,\pi)}$ be any DRBM with $|\lambda_1|, ..., |\lambda_\ell| > (d-1)^{-1/2}$. Then, for any ϵ, with high probability, $A_{\mathbf{G}}$ has only ℓ eigenvalues with modulus larger than $2\sqrt{d-1} + \epsilon$.*

Related Work. Semidefinite programming approaches have been most studied in the dense, irregular case, where exact recovery is possible (for instance [ABH16, AS15]), and it has been shown that an SDP relaxation can achieve the information-theoretically optimal threshold [HWX16]. However, in the sparse regime we consider, the power of SDP relaxations for weak recovery remains unclear. Guedon and Vershynin [GV16] show upper bounds on the estimation error of a standard SDP relaxation in the sparse, two-community case of the SBM, but only when the degree is roughly 10^4 times the information theoretic threshold. More recently, in a tour-de-force, Montanari and Sen [MS15] showed that for two communities, the SDP of Guedon and Vershynin achieves the information theoretically optimal threshold for large but constant degree, in the sense that the performance approaches the threshold if we send the number of vertices, and then the degree, to infinity. Semi-random graph models have been intensively studied in [BS95, FK00, FK01, CO04, KV06, CO07, MMV12, CJSX14, GV16] and we refer the reader to [MMV16] for a more detailed survey. In the logarithmic-degree regime, robust algorithms for community detection are developed in [CL+15, KK10, AS12]. Less is known in the case of regular graphs. However, [BKM17] show that the Lovàsz ϑ function—a strengthening of the SDP we will consider—can distinguish between graphs drawn from the symmetric RSBM and the uniformly random model when $d > 4d_{KS}$.

Is this the correct characterization of their results?

3 Technical Overview

Denote by $\mathcal{N}$ the uniform distribution on n-vertex d-regular graphs, and write $\mathcal{P} = \mathcal{P}_{d,k,M,\pi}$ the DRBM. We will use bold face font for random objects sampled from these distributions. Because we care only about the case when the number of vertices is very large, we will use *with high probability (w.h.p)* to describe any sequence of events with probability $1 - o_n(1)$ in $\mathcal{N}$ or $\mathcal{P}$ as $n \to \infty$. We will write $[n] = \{1, ..., n\}$, and in general use the letters u, v, w to refer to elements of $[n]$ and i, j for elements of $[k]$. The identity matrix will be denoted by $\mathbb{1}$, and we will write X^T for the transpose of a matrix X, $\langle X, Y\rangle = \operatorname{tr} X^T Y$ for the standard matrix inner product, and $\|X\|_F$ for the associated Frobenius norm. Positive semidefiniteness will be indicated with the symbol $\succeq$. The standard basis vectors will be denoted $e_1, e_2, ...$, the all-ones vector written as e, and the all-ones matrix as $\mathbb{J} = ee^T$. Finally, let $\operatorname{diag} : \mathbb{R}^{n\times n} \to \mathbb{R}$ be the function extracting the diagonal of a matrix, and $\operatorname{Diag} : \mathbb{R}^n \to \mathbb{R}^{n\times n}$ be the one which populates the nonzero elements of a diagonal matrix with the vector it is given as input.

3.1 Detection, Refutation, and Sum-of-Squares

We will begin the discussion of the Local Statistics algorithm by briefly recalling Sum-of-Squares programming. Say we have a constraint satisfaction problem presented as a system of polynomial equations in variables $x = (x_1, ..., x_n)$ that we are to simultaneously satisfy. In other words, we are given a set

$$\mathcal{S} = \{x \in \mathbb{R}^n : f_1(x), ..., f_m(x) = 0\}$$

and we need to decide if it is non-empty. Whenever the problem is satisfiable, any probability distribution supported on $\mathcal{S}$ gives rise to an operator $\mathbb{E} : \mathbb{R}[x] \to \mathbb{R}$ mapping a polynomial x to its expectation. Trivially, $\mathbb{E}$ obeys

$$\begin{aligned} &\textit{Normalization} && \mathbb{E}\, 1 = 1 && && (1)\\ &\textit{Satisfaction of } \mathcal{S} && \mathbb{E}\, f_i(x) \cdot p(x) = 0 && \forall i \in [m], \forall p \in \mathbb{R}[x] && (2)\\ &\textit{Positivity} && \mathbb{E}\, p(x)^2 \geq 0 && \forall p \in \mathbb{R}[x] && (3) \end{aligned}$$

In general, we will say that an operator mapping some subset of $\mathbb{R}[x]$ to the reals is *normalized*, *satisfies* $\mathcal{S}$, or is *positive* if it obeys (1), (2), or (3), respectively, on all polynomials in its domain.

Proving that $\mathcal{S} = \emptyset$, and thus that our problem is unsatisfiable, is equivalent to showing that no operator obeying (1)-(3) can exist. The key insight of SoS is that, at least sometimes, one can do this by focusing only on polynomials of some bounded degree. Writing $\mathbb{R}[x]_{\leq D}$ for the polynomials of degree at most D, we call an operator $\widetilde{\mathbb{E}} : \mathbb{R}[x]_{\leq D} \to \mathbb{R}$ a *degree-*D *pseudoexpectation* if it is normalized, and for every polynomial in its domain satisfies $\mathcal{S}$ and is positive. It is well-known that one can search for a degree D pseudoexpectation with a semidefinite program of size $O(n^d)$, and if this smaller, relaxed problem is infeasible, we've shown that $\mathcal{S}$ is empty. This is the *degree-*D *Sum-of-Squares relaxation* of our CSP.

A naive way to employ SoS for hypothesis testing or reconstruction problems such as community detection is to choose some statistic known to distinguish the planted and null distributions, and write down a relaxed sum-of-squares search algorithm for this statistic. In the case of the DRBM, a graph drawn from the planted model is guaranteed a partition of the vertices into groups of sizes $\pi(i)n$, with $\pi(i)M_{i,j}dn$ edges between groups i and j. Let us refer to such a partition $\sigma : [n] \to [k]$ as M-*good*. A routine first moment calculation shows that when d is sufficiently large, uniformly random d-regular graphs from the null distribution, $\mathcal{N}$, are exponentially unlikely to have an M-good partition.

Proposition 3.1. *With probability* $1 - o_n(1)$ *(in fact, exponentially close to one) a graph* $\mathbf{G}$ *from the null model has no* M*-good partitions whenever*

$$d - 1 > \frac{H(\pi) + H(\pi, M)}{H(\pi) - H(\pi, M)}, \tag{4}$$

where $H(\pi) = -\sum_i \pi(i) \log \pi(i)$ *is the standard Shannon entropy, and* $H(\pi, M)$ *is the average with respect to* π *of the entropy of the rows of* M*.*

Thus we can solve detection in exponential time above this first moment threshold by exhaustively searching for even one M-good division of the vertices. In other words, detection in this regime is no harder than *refutation* of an M-good partition. This refutation problem can be encoded with kn variables $x_{u,i}$, describing whether each vertex $u \in [n]$ is in group $i \in [k]$, subject to the polynomial constraints

Boolean	$x_{u,i}^2 = x_{u,i}$	$\forall u \in [n]$ and $i \in [k]$
Single Color	$\sum_i x_{u,i} = 1$	$\forall u \in [n]$
Group size	$\sum_u x_{u,i} = \pi(i)n$	$\forall i \in [k]$
M*-good*	$\sum_{(u,v)\in E} x_{u,i}x_{v,j} = \pi(i)M_{i,j}dn$	$\forall i, j \in [k]$

It will be useful later to denote by $\mathcal{B}_k \subset \mathbb{R}^{nk}$ the set described by the Boolean and Single Color equations above. Each level of the SoS Hierarchy, applied to the polynomial system described above, immediately gives us a one-sided detection algorithm: if given a graph $\mathbf{G}$ the degree-D SoS relaxation is infeasible, we can be sure that there are no M-good partitions, and thus that graph came from the null model and not the planted one. However, as it is a relaxation, if this SDP is feasible we have not a priori learned anything at all. For a two-sided test we need to prove that with high probability there is no feasible solution for graphs drawn from the null model.

There are two fundamental limitations to this approach. First, statistics like existence of an M-good partition are in some cases not optimal for differentiating the null and planted distributions. Consider for simplicity a less constrained version of the symmetric DRBM, where for a parameter $\lambda < 0$ we partition the vertices into 2 equal sized groups, and sample a d-regular graph conditional on there being $(1-\lambda)dn/4$ edges among vertices in the same community, with the remaining $(1+\lambda)dn/4$ connecting vertices in different groups. Both the information theoretic and Kesten-Stigum thresholds in this case occur when $\lambda > 1/\sqrt{d-1}$ [need a citation?]. Such graphs are guaranteed to have a maximum cut of at least $(1+\lambda)dn/4$, so we can distinguish the null and planted models for any λ making this larger than the maximum cut in a d-regular random graph. However, we know from work of Dembo et al. [cite] that the maximum cut in d-regular random graphs is, with high probability,

$$\left(1 + \frac{2P_*}{\sqrt{d}} + o_d(\sqrt{d})\right)\frac{dn}{4} + o_n(n),$$

where $2P_* \approx 1.5264$ is twice the vaunted Parisi constant from statistical physics. Thus, when d is large, the maximum cut cannot distinguish the null and planted distributions until roughly $\lambda > 2P_*/\sqrt{d-1}$, i.e $d > 4P_*^2 d_{KS}$. This same phenomenon holds in the irregular SBM with two groups.

The second issue is that even in regimes where we know detection can be performed by exhaustive search for an M-good partition, low-degree SoS relaxations of this search problem are known to fail. In

the case of the symmetric DRBM , with $m_{in} < m_{out}$, a similar first moment bound to the one above shows that at roughly the same threshold, random d-regular graphs are exponentially unlikely to have any k-way cut with the same total number of between-group vertices as the hidden partition in the planted model. Banks et al. [cite] show that, for the degree-two SoS relaxation of k-way cut, detection is only possible once $d > 4d_{KS}$: for smaller degree, when $\mathbf{G}$ is sampled from the null model, there exists a feasible degree-two pseudoexpectation. A similar result for a slightly weaker SDP holds in the case of Erdős-Rényi graphs with planted k-colorings [cite].

between-group edges?

This is not the only case where degree-two SoS for refutation—which usually coincides with a well-known SDP relaxation—does not succeed all the way down to the conjectured computational threshold for detection. Consider for instance the *Rademacher-spiked Wigner model*, where our goal is to distinguish whether an observed matrix X is either (Null) an $n \times n$ Wigner matrix W, with $W_{i,j} \sim \mathcal{N}(0, 1/n)$ and $W_{i,i} \sim \mathcal{N}(0, 2/n)$, or (Planted) of the form $X = \lambda n^{-1}\sigma\sigma^T + W$ for some uniformly random hypercube vector $\sigma \in \{\pm 1\}^n$. Results of Feral and Peche, and Banayach-Georges and Nadakuditi tell us that detection is possible simply be examining the spectrum of X, whenever $\lambda > 1$, and Perry et al. [cite] show that this is in fact the information-theoretic threshold. On the other hand, the planted model satisfies $\sigma^T X \sigma \approx \lambda n$, so we can could try and solve detection by refuting the existence of a hypercube vector with a large quadratic form. Unfortunately, in the null model $X = W$, degree-two SoS can only refute the existence of some $\tau \in \{\pm 1\}^n$ satisfying $\tau^T X \tau > 2$ [cite]. [cite] provide evidence, using ideas of Hopkins and Steurer regarding low-degree test statistics, that there is a fundamental computational barrier to outperforming degree-two SoS at this refutation task; quite recently, [cite] show that this gap persists for degree-four SoS, and conjecture that refutation of any smaller maximum is impossible for SoS of constant degree.

drop the sentence fragment "which usually coincides with..." – makes it more effective?

Correct ref?

These results fit into a broader current in the literature probing the nature and origin of computational barriers in random refutation problems [citations]. In the preceding discussion, we were attempting to solve detection in the DRBM , for d in the conjectured computationally feasible regime, by refuting the existence of some combinatorial structure in the observed graph. However, refutation is essentially a prior-free task! There are, at least potentially, many planted distributions for producing graphs with M-good partitions—just as there are many ways to produce a Gaussian random matrix whose maximum quadratic form over the hypercube is atypically large—and *they need not all have the same computational phase transition.* The idea is that refutation in the null model is hard exactly when it would allow us to solve *detection* in the computationally hard or information-theoretically impossible regime of some 'quietly' planted distribution, whose low degree moments mimic those of the null model (see [cite], for example).

did not follow this sentence

All of this is bad news for refutation, but not necessarily for detection. The problem of detection and the related one on reconstruction are in a Bayesian setting, where the prior distribution is completely specified. Yet, the semi-definite programs described above use little information from the prior distribution in their formulation. Why not include information about the prior distribution in our SDP?

3.2 The Local Statistics Hierarchy

Let us regard the planted model as a joint distribution on random variables $\mathbf{x} = \{\mathbf{x}_{u,i}\}$ encoding the group labels, and $\mathbf{G} = \{\mathbf{G}_{u,v}\}$ indexed by $\{u, v\} \subset [n]$ and describing which edges of the graph are present. Instead of our somewhat ad-hoc SDP relaxing the problem of searching for an M-good partition, we will try and find a pseudoexpectation on the variables $x_{u,i}$ which (i) satisfies $\mathcal{B}_k$—the Boolean and Single-Color constraints—and (ii) matches certain low-degree moments of the planted distribution. To a first approximation, we will

add constraints of the form

$$\widetilde{\mathbb{E}}\, p(G, x) \simeq \mathop{\mathbb{E}}_{(\mathbf{G},\mathbf{x})\sim\mathcal{P}} p(\mathbf{G}, \mathbf{x}),$$

for a restricted class of polynomials p in variables $x = \{x_{u,i}\}_{u\in[n],i\in[k]}$ and $G = \{G_{u,v}\}_{u,v\in[n]}$. The exact meaning of $\simeq$ will depend on the concentration of $p(\mathbf{G}, \mathbf{x})$ with respect to the randomness in $\mathbf{x}$ and $\mathbf{G}$; we will make it precise below.

The DRBM has a natural symmetry: we can freely permute the vertices, and the distribution is unchanged. This gives us an action of $\mathfrak{S}_n$, the symmetric group on n elements, on the random variables $\mathbf{x} = \{\mathbf{x}_{u,i}\}$ and $\mathbf{G} = \{\mathbf{G}_{u,v}\}$ describing our random graphs, and their non-random counterparts $x = \{x_{u,i}\}$ and $G = \{G_{u,v}\}$ appearing in the polynomials in the domain of $\widetilde{\mathbb{E}}$. In particular, $\theta \in \mathfrak{S}_n$ acts as $\theta : x_{u,i} \mapsto x_{\theta(u),i}$ and $\theta : G_{u,v} \mapsto G_{\theta(u),\theta(v)}$. It is only meaningful to consider polynomials in x and G that are fixed under this action; these roughly correspond to counting the instances of subgraphs of G with vertices constrained to have particular labels. See [planted clique?] for a discussion of a similar nature. Note that unless we are in the case of the symmetric DRBM, the community labels do not have a similar symmetry.

Since the random variables $\mathbf{G}$ are all zero-one indicators, we only need consider polynomials $p(x, G)$ that are multilinear in G. We claim that every such polynomial in $\mathbb{R}[x, G]$ fixed under this action, and with degrees D_1 ad D_2 in the x and G variables respectively, is of the following form. Let $H = (V(H), E(H))$ be a graph with at most D_2 edges, $S \subset V(H)$ a designated subset of at most D_1 vertices, and $\tau : S \to [k]$ a set of labels on these distinguished vertices. Write Φ_H for the set of all injective homomorphisms $\varphi : H \to \mathbf{G}$, i.e. maps for which (1) $\varphi(a) \neq \varphi(b)$ for every distinct $a, b \in V(H)$ and (2) $(a, b) \in E(H)$ implies $(\varphi(a), \varphi(b)) \in E(\mathbf{G})$. The image of each $\varphi \in \Phi_H$ is a copy of H inside $\mathbf{G}$. For each, there is a corresponding polynomial

$$p_{H,S,\tau}(x, G) = \sum_{\varphi\in\Phi_H} \prod_{u\in S} x_{\varphi(u),\tau(u)}, \tag{5}$$

that counts occurrences H in G which conform, on the vertices in S, to the labels specified by τ. One can check that these polynomials are a basis for the vector space of polynomials in $\mathbb{R}[x, G]$ fixed under the action above.

Definition 3.2. The degree (D_1, D_2) level of the Local Statistics hierarchy is the following SDP: find a degree-D_1 pseudoexpectation $\widetilde{\mathbb{E}}$ satisfying $\mathcal{B}_k$, such that

$$\widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, G) \approx \mathop{\mathbb{E}}_{(\mathbf{x},\mathbf{G})\sim\mathcal{P}} p_{H,S,\tau}(\mathbf{x}, \mathbf{G}) \tag{6}$$

for every $|S| \leq D_1$ and $|E(H)| \leq D_2$.

Note that, among many new constraints that this this SDP imposes on $\widetilde{\mathbb{E}}$, it recovers the conditions on group size and M-good-ness from our earlier SoS relaxation, as

$$\sum_i x_{u,i} \qquad \text{and} \qquad \sum_{(u,v)\in E} x_{u,i} x_{v,j}$$

are both of the form (5). We obtain the first when H is the graph on one vertex with label i, and the second when H is a single edge, with endpoints labeled i and j. Note also that, although we have stated it in the specific context of the DRBM, this framework extends readily to any planted problem involving a joint distribution μ on pairs $(\mathbf{x}, \mathbf{G})$ of a hidden structure and observed signal, if we take appropriate account of the natural symmetries in μ.

The remainder of the paper will be laid out as follows. In section [ref] we will collect some preliminary results, including several standard and useful observations on non-backtracking walks and reversible Markov chains. Section [ref] contains the proof that our SDP can distinguish the null and planted models above the KS threshold, and Section [ref] adapts this proof to show that spectral distinguishing is possible in this regime as well. In Section [ref] we prove the other half of Theorem [ref], namely that no constant level of our hierarchy succeeds below this threshold, as well as Theorem [ref], that there planted models *below* the KS threshold for which arbitrarily many rounds are required to distinguish. Section [ref] concerns the robustness guarantees of our algorithm. Finally, in Appendix [ref], we will perform several calculations on the DRBM , including the first moment bound of Lemma [ref], and the explicit computation of the local statistics appearing in the LoSt hierarchy.

4 Preliminaries

4.1 Nonbacktracking Walks and Orthogonal Polynomials

The central tool in our proofs will be *non-backtracking walks* on G—these are walks which on every step are forbidden from visiting the vertex they were at two steps previously. We will collect here some known results on these walks specific to the case of d-regular graphs. Write $A_G^{(s)}$ for the $n \times n$ matrix whose (v, w) entry counts the number of length-s non-backtracking walks between verties v and w in G. One can check that the $A_G^{(s)}$ satisfy a two-term linear recurrence,

$$\begin{aligned} A_G^{(0)} &= \mathbb{1} \\ A_G^{(1)} &= A_G \\ A_G^{(2)} &= A_G^2 - d\mathbb{1} \\ A_G^{(s)} &= AA_G^{(s-1)} - (d-1)A_G^{(s-2)} \qquad s > 2, \end{aligned}$$

since to enumerate non-backtracking walks of length s, we can first extend each such walk of length $s-1$ in every possible way, and then remove those extensions that backtrack.

On d-regular graphs, the above recurrence immediately shows that $A_G^{(s)} = q_s(A_G)$ for a family of monic, scalar 'non-backtracking polynomials' $\{q_s\}_{s \geq 0}$, where $\deg q_s = s$. It is well known that these polynomials are an orthogonal polynomial sequence with respect to the Kesten-McKay measure

$$\frac{d\mu_{KM}}{dx} = \frac{1}{2\pi} \frac{d}{\sqrt{d-1}} \frac{\sqrt{4(d-1) - x^2}}{d^2 - x^2} \mathbf{1}\left[|x| < 2\sqrt{d-1}\right],$$

with its associated inner product

$$\langle f, g \rangle_{KM} \triangleq \int f(x) g(x) d\mu_{KM}$$

on the vector space of square integrable functions on $(-2\sqrt{d-1}, 2\sqrt{d-1})$. One can again check that

$$\|q_s\|_{KM}^2 \triangleq \int q_s(x)^2 \, d\mu_{KM} = q_s(d) = \begin{cases} 1 & s = 0 \\ d(d-1)^{s-1} & s \geq 1 \end{cases} = \frac{1}{n} (\text{\# length-s n.b. walks on } G)$$

in the normalization we have chosen [ABLS07]. Thus any function f in this vector space can be expanded as

$$f = \sum_{s \geq 0} \frac{\langle f, q_s \rangle_{KM}}{\|q_s\|_{KM}^2} q_s.$$

We will also need the following lemma of Alon et al. [ABLS07, Lemma 2.3] bounding the size of the polynomials q_s:

Lemma 4.1. *For any $\epsilon > 0$,*

$$|q_s(x)| \leq 2(s+1)\sqrt{d(d-1)^{s-1}} = 2(s+1)\|q_s\|_{KM}$$

ϵ? is x in some range here?

The behavior of the non-backtracking polynomials with respect to the inner product $\langle \cdot, \cdot \rangle_{KM}$ idealizes that of the $A_G^{(s)} = q_s(A_G)$ under the trace inner product. In particular, if $s + t < \text{girth}(G)$

$$\langle A_G^{(s)}, A_G^{(t)} \rangle = n \langle q_s, q_t \rangle_{KM} = \begin{cases} n(\#\text{ length-}s\text{ n.b. walks on } G) & s = t \\ 0 & s \neq t \end{cases}.$$

This is because the diagonal entries of $A_G^{(s)} A_G^{(t)}$ count pairs of non-backtracking walks with length s and t respectively: if $s \neq t$ any such pair induces a cycle of length at most $s + t$, or perhaps is a pair of identical walks in the case $s = t$. Above the girth, if we can control the number of cycles, we can quantify how far the $A_G^{(s)}$ are from orthogonal in the trace inner product.

Luckily for us, sparse random graphs have very few cycles. To make this precise, call a vertex *bad* if it is at most L steps from a cycle of length at most C. These are exactly the vertices for which the diagonal entries of $A_G^{(s)} A_G^{(t)}$ are nonzero, when $s + t < C + L$.

Lemma 4.2. *For any constant C and L, with high probability any graph $\mathbf{G} \sim \mathcal{P}$ has at most $O(\log n)$ bad vertices.*

We will defer the proof of this lemma to the appendix, but two nice facts follow from it immediately. First, from the above discussion,

$$\langle A_{\mathbf{G}}^{(s)}, A_{\mathbf{G}}^{(t)} \rangle = O(\log n)$$

for any $s, t = O(1)$. The second useful corollary is more or less that in random graphs we can use non-backtracking walks as a proxy for self-avoiding ones.

Lemma 4.3. *Write $A_{\mathbf{G}}^{\langle s \rangle}$ for the $n \times n$ matrix whose i, j entry is a one exactly when i and j are connected by a self-avoiding walk of length s. Then with high probability, for any graph $\mathbf{G} \sim \mathcal{P}$,*

$$\left\| A_{\mathbf{G}}^{\langle s \rangle} - A_{\mathbf{G}}^{(s)} \right\| = O(\log n) \tag{7}$$

4.2 Reversible Markov Chains

We will need standard fact about reversible Markov chains. Let us maintain the notation for M, its eigenvalues $1 = \lambda_1 \geq |\lambda_2| \geq \cdots \geq |\lambda_k|$, and its stationary distribution π. Recall from above that $Me = e$, $\pi^T M = \pi^T$, and the reversibility condition on M means $\mathrm{Diag}(\pi)M$ is symmetric.

Lemma 4.4. *Let F be the matrix of right eigenvectors, normalized so that the columns have unit norm (note that the first column of F is, up to scaling, the all-ones vector). Then $F^{-1}\,\mathrm{Diag}(\pi)F = \mathbb{1}$.*

Proof. First, reversibility tells us $\mathrm{Diag}(\pi)^{1/2} M\,\mathrm{Diag}(\pi)^{-1/2}$ is symmetric, and thus by the spectral theorem that it satisfies

$$\mathrm{Diag}(\pi)^{1/2} M\,\mathrm{Diag}(\pi)^{1/2} O = O\Lambda$$

for some orthogonal O. It is readily seen that $M\,\mathrm{Diag}(\pi)^{-1/2}O = \mathrm{Diag}(\pi)^{-1/2}O\Lambda$, so $\mathrm{Diag}(\pi)^{-1/2}O$ contains, up to scaling, the right eigenvectors of M. □

4.3 Local Statistics in the Planted Model

The Local Statistics SDP that we are studying includes constraints that our pseudoexpectation match certain low-degree moments in the planted distribution. As we discussed in the technical overview, these correspond to the counts of partially labelled subgraphs in G. To set some notation, a *partially labelled graph* (H, S, τ) is a graph $H = (V(H), E(H))$, together with a distinguished subset of vertices $S \subset V(H)$, and a labelling $\tau : S \to [k]$ of these distinguished vertices. We'll say a graph is *unlabeled* or *fully labelled* if $S = \emptyset$ or $S = V(H)$, and in these cases abuse notation and simply refer to H or (H, τ) respectively. At times it will also be useful to refer to graphs with distinguished vertices, but no labelling; we will write these as (H, S). An *occurrence* of a partially labelled graph (H, S, τ) in a fully labelled one (G, σ) is an injective homomorphism $H \to G$, that agrees on labels, i.e. vertices in S are mapped to ones in $V(G)$ with the same label.

The low-degree moment constraints in $\mathrm{LoSt}(2, m)$ are exactly the counts of occurrences of partially labelled subgraphs (H, S, τ) in a graph $\mathbf{G} \sim \mathcal{P}$, for which H has at most m edges and 2 distinguished vertices. The following theorem characterizes these counts in any planted model; we will discuss it briefly below and remit the proof to the appendix.

Definition 4.5. Let (H, S) be a connected graph on $O(1)$ edges, with distinguished vertices S. Define $C_{H,S,d}$ to be the number of occurrences of (H, S) in an infinite d-regular tree in which some vertex in S is mapped to the root. If $S = \emptyset$, choose some distinguished vertex arbitrarily—the count will be the same no matter which one is chosen. Finally, if $(H, S) = (H_1, S_1) \sqcup \cdots \sqcup (H_\ell, S_\ell)$ has ℓ connected components, take $C_{H,S,d} = C_{H_1,S_1} \cdots C_{H_\ell,S_\ell}$. We note for later use that if H contains a cycle, $C_{H,S} = 0$, and if it is a path of length s with endpoints distinguished, $C_{H,S} = \|q_s\|_{KM}^s$, the number of vertices at depth s in the tree.

Theorem 4.6 (Local Statistics)**.** *If (H, S, τ) is a partially labelled graph with $O(1)$ edges, then in any planted model $\mathcal{P}_{d,k,M,\pi}$,*

1. *If H is unlabelled, i.e. $S = \emptyset$, then $n^{-\ell}\,\mathbb{E}\,p_{H,S,\tau}(\mathbf{x}, \mathbf{G}) \to C_{H,S,d}$*
2. *If H is labelled, with $S = \{\alpha, \beta\}$, $\tau(\alpha) = i$, and $\tau(\beta) = j$, then*

$$n^{-\ell}\,\mathbb{E}\,p_{H,S,\tau}(\mathbf{x}, \mathbf{G}) \to \pi(i) M_{i,j}^{\mathrm{dist}(\alpha,\beta)} C_{H,S,d},$$

and $p_{H,S,\tau}(\mathbf{x}, \mathbf{G})$ *enjoys concentration up to an additive* $\pm o(n^\ell)$. *We say that* $\mathrm{dist}(\alpha, \beta) = \infty$ *if these two vertices lie in disjoint components of* H, *and we interpret* $M^\infty_{i,j} = \pi(j)$.

Remark 4.7. In our Local Statistics SDP [ref], we promised to formalize the symbol $\simeq$ appearing in the affine moment-matching constraints on the pseudoexpectation; let's do so now. Throughout the paper, fix a very small error tolerance $0 < \delta$, and write $\simeq_\ell$ to mean "equal up to $\pm\delta n^\ell$". Then the constraint for each partially labelled subgraph with ℓ connected components should read $\widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, G) \simeq_\ell \mathbb{E}\, p_{H,S,\tau}(\mathbf{x}, \mathbf{G})$. We will write $\simeq$ instead of $\simeq_1$ whenever there is no chance for confusion. Finally, because we have defined our model quite rigidly, whenever (H, S, τ) consists of a single vertex with label $i \in [k]$, $p_{H,S,\tau}(\mathbf{x}, \mathbf{G}) = \pi(i)n$. Similarly when (H, S) consists of two distinguished vertices with labels $i, j \in [k]$ respectively,

$$p_{H,S,\tau}(\mathbf{x}, \mathbf{G}) = \begin{cases} \pi(i)\pi(j)n^2 & i \neq j \\ \pi(i)^2 n^2 - \pi(i)n & i = j \end{cases}$$

and the moment-matching constraints in our SDP will accordingly include $=$ instead of $\simeq$.

Should we restate the entire SDP here?

Let's take a moment and get a feel for Theorem [ref]. As a warm-up, consider the case when (H, S, τ) is a path of length $s \leq m$ with the endpoints labelled as $i, j \in [k]$, and we simply need to count the number of pairs of vertices in G with labels i and j respectively that are connected by a path of length s. As d-regular random graphs from models like $\mathcal{P}$ have very few short cycles, assume for simplicity that the girth is in fact much larger than m, so that the depth-s neighborhood about every vertex is a tree. If we start from a vertex i and follow a uniformly random edge, the parameter matrix M from our model says that, on average at least, the probability of arriving at a vertex in group j is roughly $M_{i,j}$, and similarly if we take s (non-backtracking) steps, this probability is roughly $M^s_{i,j}$. There are $\pi(i)n$ starting vertices in group i, and $d(d-1)^{s-1}$ vertices at distance s from any such vertex.

If (H, S, τ) is a tree in which the two distinguished vertices are at distance s, then we can enumerate occurrences of (H, S, τ) in G by first choosing the image of the path connecting these two, and then counting the ways to place the remaining vertices. If we again assume that the girth is sufficiently large, it isn't too hard to see that the number of ways to do this second step is a constant independent of the number of ways to place the path, so we've reduced to the case above. The idea for the cases $|S| = 0, 1$ is similar. We'll prove Theorem [ref] in Appendix [ref].

5 Distinguishing with Local Statistics

Throughout this section, fix the parameters (d, k, M, π) of a planted model $\mathcal{P}$. We'll prove half of our main theorem, namely that for any $\epsilon > 0$, if

$$\lambda_2^2(d-1) = 1 + \epsilon$$

then there exists some m so that the $\mathrm{LoSt}(2, m)$ SDP can distinguish the planted and null models. When $(\mathbf{x}, \mathbf{G}) \sim \mathcal{P}$, the SDP is surely feasible as we can simply set

$$\widetilde{\mathbb{E}}\, p(x, G) = p(\mathbf{x}, \mathbf{G})$$

for any polynomial we choose. We will thus be done if we can show *infeasibility* when $\mathcal{P}$ is above the KS threshold, m is sufficiently large, and $\mathbf{G} \sim \mathcal{N}$. Our strategy will be to first reduce to the problem of designing a univariate polynomial with particular properties, and then to solve this design problem using some elementary results from Section [ref].

Let $\mathbf{G} \sim \mathcal{P}$, and assume we had a viable pseudoexptation $\widetilde{\mathbb{E}}$ for the LoSt$(2, m)$ SDP. Write $X \succeq 0$ for the $nk \times nk$ matrix whose $(u, i), (v, j)$ entry is $\widetilde{\mathbb{E}}\, x_{u,i} x_{v,j}$ (it is routine that $\widetilde{\mathbb{E}} \succeq 0$ implies positive semidefiniteness of X; we refer the reader to [ref]). It will at times be useful to think of X as a $k \times k$ matrix of $n \times n$ blocks $X_{i,j}$, and at others as an $n \times n$ matrix of $k \times k$ blocks $X_{u,v}$. Recall also the matrices $A_{\mathbf{G}}^{\langle s \rangle}$ from Section [] that count self-avoiding walks of length s. Our strategy will be to first write the moment-matching constraints on $\widetilde{\mathbb{E}}$ as affine constraints of the form $\langle X_{i,j}, Y \rangle \simeq C$, and then combine these affine constraints to contradict feasibility of X.

Lemma 5.1. *For any i, j, and any $s = 0, \ldots, m$, recalling that $A_G^{(s)}$ is the matrix counting non-backtracking walks of length s, and $\mathbb{J}$ is the all-ones matrix,*

$$\langle X_{i,j}, A_{\mathbf{G}}^{(s)} \rangle \simeq \pi(i) M_{i,j}^s \|q_s\|_{KM}^2 n$$
$$\langle X_{i,j}, \mathbb{J} \rangle = \pi(i)\pi(j) n^2.$$

Proof. For the first assertion, let (H, S, τ) be the path of length s whose endpoints are labelled $i, j \in [k]$. Each *self-avoiding* walk of length s in G is an occurrence of H, so from Lemma [ref]

$$\langle X_{i,j}, A_{\mathbf{G}}^{\langle s \rangle} \rangle = \widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, \mathbf{G}) \simeq \pi(i) M_{i,j}^s \|q_s\|_{KM}^2.$$

We can now use Lemma [ref] to replace the self-avoiding walk matrices $A_{\mathbf{G}}^{\langle s \rangle}$ with their non-backtracking counterparts. The matrix X has diagonal elements $X_{(u,i),(u,i)} = \widetilde{\mathbb{E}}\, x_{u,i}^2 = \widetilde{\mathbb{E}}\, x_{i,u}$ by the Boolean constraint, and $\widetilde{\mathbb{E}}\,(x_{u,1} + \cdots + x_{u,k}) = 1$ by the Single Color constraint. By PSD-ness of X, every $\widetilde{\mathbb{E}}\, x_{u,i}^2 = \widetilde{\mathbb{E}}\, x_{u,i}$ is nonnegative, so each is between zero and one. It is a standard fact that the off-diagonal entries of such a PSD matrix have magnitude at most one, so from Lemma [ref]

$$\langle X_{i,j}, A_{\mathbf{G}}^{(s)} \rangle = \langle X_{i,j}, A_{\mathbf{G}}^{\langle s \rangle} \rangle + \langle X_{i,j} A_{\mathbf{G}}^{\langle s \rangle} - A_{\mathbf{G}}^{(s)} \rangle = \langle X_{i,j}, A_{\mathbf{G}}^{\langle s \rangle} \rangle \pm O(\log n) \simeq \pi(i) M_{i,j}^s \|q_s\|_{KM}^2$$

for $s = 0, \ldots, m$. For the second assertion, when $i \neq j$ take (H, S, τ) to be the partially labelled graph on two disconnected vertices, with labels i and j respectiveely. From Remark [ref] we have

something off in the previous equation

$$\langle X_{i,j}, \mathbb{J} \rangle = \widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, \mathbf{G}) = \pi(i)\pi(j) n^2.$$

When $i = j$, take (H, S, τ) as above and (H', S', τ') to be a single vertex labelled i. □

We will now apply a fortuitous change of basis furnished to us by the parameter matrix M. Recall that F is the matrix whose columns are the right eigenvectors of M, satisfying $MF = F\Lambda$ and $F^T \operatorname{Diag}(\pi) F = \mathbb{1}$. Now define a matrix $\check{X} \triangleq (F^T \otimes \mathbb{1}) X (F \otimes \mathbb{1})$, by which we mean that

$$\check{X} = \begin{pmatrix} F_{1,1}\mathbb{1} & \cdots & F_{1,k}\mathbb{1} \\ \vdots & \ddots & \vdots \\ F_{k,1}\mathbb{1} & \cdots & F_{k,k}\mathbb{1} \end{pmatrix} \begin{pmatrix} X_{1,1} & \cdots & X_{1,k} \\ \vdots & \ddots & \vdots \\ X_{k,1} & \cdots & X_{k,k} \end{pmatrix} \begin{pmatrix} F_{1,1}\mathbb{1} & \cdots & F_{1,k}\mathbb{1} \\ \vdots & \ddots & \vdots \\ F_{k,1}\mathbb{1} & \cdots & F_{k,k}\mathbb{1} \end{pmatrix}.$$

We will think of $\check{X}$, analogous to X, as a $k \times k$ matrix of $n \times n$ blocks $\check{X}_{i,j}$. Note that we can also think of this as as a change of basis $x \mapsto F^T x$ directly on the variables appearing in polynomials accepted by our pseudoexpectation.

Lemma 5.2. *For any* $s = 0, \ldots, m$, *if* $i \neq j$ $\langle \check{X}_{i,j} A_{\mathbf{G}}^{(s)} \rangle \simeq 0$, *and*

$$\langle \check{X}_{i,i}, A_{\mathbf{G}}^{(s)} \rangle \simeq \lambda_i^s \|q_s\|_k^2 n.$$

Furthermore,

$$\langle \check{X}_{i,j}, \mathbb{J} \rangle = \begin{cases} n^2 & i = j = 1 \\ 0 & \textit{else} \end{cases}.$$

Proof. Our block-wise change of basis commutes with taking inner products between the blocks $X_{i,j}$ and the non-backtracking walk matrices. In other words,

$$\begin{aligned}
\begin{pmatrix} \langle \check{X}_{1,1}, A_{\mathbf{G}}^{(s)} \rangle & \cdots & \langle \check{X}_{1,k}, A_{\mathbf{G}}^{(s)} \rangle \\ \vdots & \ddots & \vdots \\ \langle \check{X}_{k,1}, A_{\mathbf{G}}^{(s)} \rangle & \cdots & \langle \check{X}_{k,k}, A_{\mathbf{G}}^{(s)} \rangle \end{pmatrix} &= F^T \begin{pmatrix} \langle X_{1,1}, A_{\mathbf{G}}^{(s)} \rangle & \cdots & \langle X_{1,k}, A_{\mathbf{G}}^{(s)} \rangle \\ \vdots & \ddots & \vdots \\ \langle X_{k,1}, A_{\mathbf{G}}^{(s)} \rangle & \cdots & \langle X_{k,k}, A_{\mathbf{G}}^{(s)} \rangle \end{pmatrix} F \\
&\simeq F^T \operatorname{Diag}(\pi) M^s F \cdot \|q_s\|_{KM}^s n \\
&= F^T \operatorname{Diag}(\pi) F \Lambda^s \cdot \|q_s\|_{KM}^s n \\
&= \Lambda^s \cdot \|q_s\|_{KM}^s n
\end{aligned}$$

A parallel calculation gives us

$$\begin{aligned}
\begin{pmatrix} \langle \check{X}_{1,1}, \mathbb{J} \rangle & \cdots & \langle \check{X}_{1,k}, \mathbb{J} \rangle \\ \vdots & \ddots & \vdots \\ \langle \check{X}_{k,1}, \mathbb{J} \rangle & \cdots & \langle \check{X}_{k,k}, \mathbb{J} \rangle \end{pmatrix} &= F^T \begin{pmatrix} \langle X_{1,1}, \mathbb{J} \rangle & \cdots & \langle X_{1,k}, \mathbb{J} \rangle \\ \vdots & \ddots & \vdots \\ \langle X_{k,1}, \mathbb{J} \rangle & \cdots & \langle X_{k,k}, \mathbb{J} \rangle \end{pmatrix} F \\
&= F^T \pi \pi^T F \cdot n^2 \\
&= e_1 e_1^T n^2,
\end{aligned}$$

where e_1 is the first standard basis vector. The final line comes since π, being the left eigenvector associated to $\lambda_1 = 1$, is (up to scaling) the first row of F^{-1}. □

The remainder of the proof will amount to combining the constraints on the diagonal blocks of $\check{X}$. As X is PSD, $\check{X}$ is as well, so any PSD linear combination $0 \preceq c_0 \mathbb{1} + \cdots + c_m A_{\mathbf{G}}^{(s)}$ must satisfy

$$0 \leq \frac{1}{n} \langle \sum_{s=0}^{m} c_s A_{\mathbf{G}}^{(s)}, \check{X}_{i,i} \rangle \simeq \sum_{s=0}^{m} c_s \lambda_i^s \|q_s\|_{KM}^2.$$

We can show that no $\check{X}$ satisfying the given constraints, and thus that the SDP is infeasible, by producing such constants c_s as to make the right hand side of the above equation negative for at least one of $\lambda_1, \ldots, \lambda_k$. Notice also

$$\sum_{s=0}^{m} c_s A_{\mathbf{G}}^{(s)} = \sum_{s=0}^{m} c_s q_s(A_{\mathbf{G}}) \triangleq f(A_{\mathbf{G}})$$

for some polynomial $f \in \mathbb{R}[x]$ of degree m. Because $f(A_{\mathbf{G}})$ is a scalar polynomial in $A_{\mathbf{G}}$, its eigenvalues are f applied to those of $A_{\mathbf{G}}$, and we get $f(A_{\mathbf{G}}) \succeq 0$ with high probability when f is nonnegative on Spec $A_{\mathbf{G}}$. By Friedman's Theorem [ref], this spectrum consists of the 'trivial' eigenvalue d, together with $n - 1$

no need for high probability here?

remaining eigenvalues whose magnitudes with high probability are at most $2\sqrt{d-1}+\eta$ for any $\eta > 0$. In fact, it is not necessary even that $f(d) > 0$. To see this, note that from our discussion above,

$$\langle f\left(A_{\mathbf{G}} - \tfrac{d}{n}\mathbb{J}\right), \check{X}_{i,i}\rangle = \langle f(A_{\mathbf{G}}) - \tfrac{f(d)}{n}\mathbb{J}, \check{X}_{i,i}\rangle = \langle f(A_{\mathbf{G}}), \check{X}_{i,i}\rangle$$

for $i = 2, ..., k$. Since $A_{\mathbf{G}} - \frac{d}{n}\mathbb{J}$ is the projection of A away from the eigenspace corresponding to $d \in \operatorname{Spec} A_{\mathbf{G}}$, $f(A_{\mathbf{G}} - \frac{d}{n}\mathbb{J}) \succeq 0$ whenever f is positive on the remainder of the spectrum.

From our discussion in Section [ref] of the preliminaries, for any λ

$$\begin{aligned}\sum_{s=0}^{m} c_s \|q_s\|_{KM}^2 \lambda^s &= \sum_{s=0}^{m} \frac{\langle f, q_s\rangle_{km}}{\|q_s\|_{km}^2} \|q_s\|_{KM}^2 \lambda^s \\ &= \langle f, \sum_{s=0}^{m} \lambda^s q_s\rangle_{KM} \\ &\triangleq \langle f, \phi_{m,\lambda}\rangle_{KM}.\end{aligned}$$

Thus we've reduced the proof to the construction of a degree m polynomial f, strictly positive on $(-2\sqrt{d-1}, 2\sqrt{d-1})$—so that by continuity it is nonnegative on a slightly larger interval to which Friedman's theorem applies—and satisfying $\langle f, \phi_{m,\lambda}\rangle_{KM} < 0$. The following extremely simple choice of f will finish things up.

Call μ the largest even number less than or equal to m, and take

$$f(x) = -q_\mu(x) + 2\mu\|q_\mu\|_{KM} + \epsilon$$

which by Lemma [ref] is nonnegative on the desired interval. This choice of f satisfies

$$\langle f(x), \Phi_{\mu,\lambda}\rangle = -\|q_\mu\|_{KM}^2 |\lambda|^\mu + 2\mu\|q_\mu\|_{KM} + \epsilon,$$

which is negative when

$$|\lambda| > \left(\frac{2\mu + \epsilon/\|q_\mu\|_{KM}}{\|q_\mu\|_{KM}}\right)^{1/\mu} \to_\mu \frac{1}{\sqrt{d-1}}.$$

Remark 5.3. We can choose constants a and b such that the $\mathtt{LocalStatistic}$ SDP (**??**) is infeasible on $\mathbf{G}$ drawn from $\mathcal{N}$ if we set the distance from the Kesten-Stigum bound ϵ and global error tolerance δ as $(\varepsilon, \delta) = (a, b)$, and also if we choose these as $(\varepsilon, \delta) = (a, 2b)$. In particular, this means that when $\delta = b$, for any PSD matrix X with an all-ones diagonal, there is a polynomial f such that the constraint

$$\langle f(A_{\mathbf{G}}), X\rangle = \|q_s\|_{KM}^2 \lambda^s n \pm \delta n$$

is violated by a margin of $\Omega(n)$.

6 Interlude: Spectral Distinguishing

Our argument in the previous section can be recast to prove Corollary [ref], namely that above the Kesten-Stigum threshold the spectrum of the adjacency matrix can also be used to distinguish the null and planted distributions.

Let $(\mathbf{x}, \mathbf{G}) \sim \mathcal{P}_{d,k,M,\pi}$, and write $\mathbf{X} \triangleq \mathbf{x}\mathbf{x}^T$, and

$$\check{\mathbf{X}} = (F^T \otimes \mathbb{1})\mathbf{X}(F \otimes \mathbb{1}) = (F^T\mathbf{x})(F^T\mathbf{x})^T \triangleq \check{\mathbf{x}}\check{\mathbf{x}}^T.$$

Think of $\check{\mathbf{X}}$ as a block matrix $(\mathbf{X}_{i,j})_{i,j\in[k]}$, as we did X in the previous section, and $\check{\mathbf{x}}$ as a block vector $(\check{\mathbf{x}}_i)_{i\in[k]}$. Applying Theorem [ref:local statistics] and repeating the calculations in Lemmas [ref] *mutatis mutandis* with $\mathbf{X}$ instead of X, we can show that w.h.p.

$$\langle \check{\mathbf{X}}_{i,j}, A_{\mathbf{G}}^{(s)} \rangle \simeq \lambda_i \|q_s\|_{KM}^2 n \text{ if } i = j$$

and zero otherwise, for every $s = O(1)$ and

$$\langle \check{\mathbf{X}}_{1,1}, \mathbb{J} \rangle = \begin{cases} n^2 & i = j = 1 \\ 0 & \text{else} \end{cases}.$$

Because $A_{\mathbf{G}}^{(s)} = \mathbb{1}$, we know

$$\check{\mathbf{x}}_i^T \check{\mathbf{x}}_j = \langle \check{\mathbf{X}}_{i,j}, \mathbb{1} \rangle = 0$$

when $i \neq j$. In other words, the k vectors $\check{\mathbf{x}}_1, \ldots, \check{\mathbf{x}}_k$ are orthogonal.

Now let $|\lambda_i|^2(d-1) > 1$. We can show that $A_{\mathbf{G}}$ has an eigenvalue outside the bulk by proving

$$\check{\mathbf{x}}_i^T f(A_{\mathbf{G}})\check{\mathbf{x}}_i = \langle \check{\mathbf{X}}_{i,i}, f(A_{\mathbf{G}}) \rangle < 0$$

for some polynomial $f(x)$ positive within $\pm o_n(1)$ of $(-2\sqrt{d-1}, 2\sqrt{d-1})$. The same polynomial from Section [ref] works here. As the $\check{\mathbf{x}}_i$ are orthogonal, we get one distinct eigenvalue outside the bulk for each eigenvalue of M for which $|\lambda_i|^2(d-1) > 1$.

Remark 6.1. To distinguish the null model from the planted one using the spectrum of $A_{\mathbf{G}}$, simply return PLANTED if $A_{\mathbf{G}}$ has a single eigenvalue other than d whose magnitude is bigger than $2\sqrt{d-1} + \delta$ for any error tolerance δ you choose, and NULL otherwise. Unfortunately, this distinguishing algorithm is not robust to adversarial edge insertions and deletions. For instance, given a graph $\mathbf{G} \sim \mathcal{N}$, the adversary can create a disjoint copy of K_{d+1}, the complete graph on $d+1$ vertices, whose eigenvalues are all $\pm d$. The spectrum of the perturbed graph is the disjoint union of $\pm d$ and the eigenvalues of the other component(s), so the algorithm will be fooled. We will show in Section [ref] that the Local Statistics SDP is robust to this kind of perturbation.

Can you do this without disconnecting the graph? Can you move eigenvalues *inside* the bulk?

7 Lower Bounds Against Local Statistics SDPs

In this section, we prove the complementary bound to Theorem [ref], namely that if every one of $\lambda_2, \ldots, \lambda_k$ has modulus at most $1/\sqrt{d-1}$ there exists some feasible solution to the Local Path Statistics SDP for every $m \geq 1$. We can specify a pseudoexpectation completely by way of an $(nk+1) \times (nk+1)$ positive semidefinite matrix

$$\begin{pmatrix} 1 & \widetilde{\mathbb{E}}\, x^T \\ \widetilde{\mathbb{E}}\, x & \widetilde{\mathbb{E}}\, x^T x \end{pmatrix} \triangleq \begin{pmatrix} 1 & l^T \\ l & X \end{pmatrix}.$$

After first writing down the general properties required of *any* quadratic pseudoexpectation satisfying $\mathcal{B}_k$, we'll show that in order for $\widetilde{\mathbb{E}}$ to match every moment asked of it by the LoSt$(2, m)$ SDP, it suffices for it to satisfy

$$\widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, G) \simeq \mathbb{E}\, p_{H,S,\tau}(\mathbf{x}, \mathbf{G})$$

when (H, S, τ) is a path of length $0, ..., m$ with labelled endpoints. Finally, we'll construct a pseudoexpectation matching these path moments by way of some elementary properties of the non-backtracking polynomials from Section [ref].

Lemma 7.1. *The set of $\mathcal{B}_k$-satisfying pseudoexpectations is parameterized by pairs $(X, l) \in \mathbb{R}^{nk \times nk} \times \mathbb{R}^{nk}$ for which*

$$\begin{pmatrix} 1 & l^T \\ l & X \end{pmatrix} \succeq 0 \tag{8}$$

$$\operatorname{diag}(X) = l \tag{9}$$

$$\operatorname{tr} X_{u,u} = e^T l = 1 \qquad \forall u \in [n] \tag{10}$$

$$X_{u,v} e = l_u \qquad \forall u, v \in [n] \tag{11}$$

Proof. Recall that the set $\mathcal{B}_k$ is defined by the polynomial equations

$$\begin{array}{lll} \textit{Boolean} & x_{u,i}^2 = x_{u,i} & \forall u \in [n] \text{ and } i \in [k] \\ \textit{Single Color} & \sum_i x_{u,i} = 1 & \forall u \in [n] \end{array}$$

That a degree-two pseudoexpectation *satisfies* these constraints means

$$\begin{aligned} \widetilde{\mathbb{E}}\, p(x) x_{u,i}^2 &= \widetilde{\mathbb{E}}\, p(x) x_{u,i} && \forall p \text{ s.t. } \deg p = 0 \\ \widetilde{\mathbb{E}}\, p(x) \sum_i x_{u,i} &= \widetilde{\mathbb{E}}\, p(x) && \forall p \text{ s.t. } \deg p \leq 1. \end{aligned}$$

Writing $X = \widetilde{\mathbb{E}}\, x^T x$ and $l = \widetilde{\mathbb{E}}\, x$ as above, the first constraint is equivalent to $l = \operatorname{diag}(X)$, since the degree-zero polynomials are just constants, and we can guarantee that the second holds for every polynomial of degree at most one by requiring it on $p = 1$ and $p =, x_{v,j}$ for all v and j. The Lemma is simply a concise packaging of these facts, using the block notation $X = (X_{u,v})_{u,v \in [n]}$ and $l = (l_u)_{u \in [n]}$. □

Proposition 7.2. *It suffices to check*

$$\widetilde{\mathbb{E}}\, p_{H,S,\tau}(x, \mathbf{G}) \simeq \mathbb{E}\, p_{H,S,\tau}(\mathbf{x}, \mathbf{G})$$

in the cases (i) (H, S, τ) is a path of length $s = 0, ..., m$ with labelled endpoints, and (ii) when (H, S, τ) is a graph with no edges on one or two labelled vertices.

Proof. Assume that $\widetilde{\mathbb{E}}$ matches all the promised moments, and let (H, S, τ) be an arbitrary partially labelled graph with ℓ connected components, and two distinguished vertices connected by a path of length $0 \leq\leq \infty$, where $s = 0$ means that the distinguished vertices, and their labels, are identical, and $s = \infty$ means that they have no path connecting them. Let's use the shorthand (P_s, i, j) for the path of length s with distinguished endpoints labelled i and j respectively. This extends naturally to the corner cases $s = 0$, when there is only one distinguished vertex and $i = j$, and $s = \infty$ when we will interpret it as two disconnected and labelled vertices.

Our central claim will be that, as polynomials, with high probability

$$\left\| n^{\ell-1} \frac{C_{d,H,S}}{C_{d,P_s,T}} p_{P_s,i,j} - p_{H,S,\tau} \right\|_1 = o(n^\ell) \simeq_\ell 0 \tag{12}$$

where here $\|\cdot\|$ means the coefficient-wise L^1 norm. To get a feel for this, in the case when H is connected and its two distinguished vertices are connected by a path of length s, $\frac{C_{H,S,d}}{C_{P_s,d}}$ counts the number of ways to place the remainder of H in a d-regular tree (or locally-treelike graph), once we commit to the locations of the two distinguished vertices and the path between them.

Once we've shown (12), it is a standard SoS calculation that the Boolean constraint implies $|\widetilde{\mathbb{E}}\, x_{u,i}x_{v,j}| \leq 1$ for every u, v, i, j. Thus, using the local statistic constraints from Proposition [ref], we will have

$$\widetilde{\mathbb{E}}\, p_{H,S,\tau} \simeq_\ell n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}\widetilde{\mathbb{E}}\, p_{P_s,i,j} \simeq_\ell n^\ell \pi(i) M^s_{i,j} C_{d,H,S}$$

as desired. To prove (12), we need to open up the subgraph counting polynomials $p_{H,S,\tau}$ a bit more, and we'll require some notation to do this cleanly. For each (H, S, τ), write $\Phi_{H,S,u,v}$ for the set of all injective homomorphisms $H \to \mathbf{G}$ such that the distinguished vertices are mapped to the vertices u and v of $\mathbf{G}$. Then

$$\begin{aligned}\left\| n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}p_{P_s,i,j}(x) - p_{H,S,\tau}(x)\right\| &= \left\|\sum_{u,v}\left(n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}|\Phi_{P_s,u,v}| - |\Phi_{H,S,\tau}|\right)x_{u,i}x_{v,j}\right\| \\ &= \sum_{u,v}\left|n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}|\Phi_{P_s,u,v}| - |\Phi_{H,S,u,v}|\right|.\end{aligned}$$

Let's first consider the case when $s < \infty$, so that the two distinguished vertices in H are connected by some path of length at most m. Under this assumption $|\Phi_{H,S,u,v}| = O(n^{\ell-1})$. Writing U for the set of m-good vertices—which by Lemma [ref] has size at least $n - O(\log n)$—and recalling that every vertex has at most $O(1)$ vertices in its depth-m neighborhood, we can restrict the above sum to run over only $u, v \in U$ and pay a cost of no more than $O(n^{\ell-1}\log n) = o(n^\ell)$. Thus

$$\left\| n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}p_{P_s,i,j}(x) - p_{H,S,\tau}(x)\right\|_1 = \sum_{u,v\in U}\left|n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}|\Phi_{P_s,u,v}| - |\Phi_{H,S,u,v}|\right| + o(n^\ell).$$

There are only $O(n)$ nonzero terms in the above sum, again because $u \in U$ means that there are only $O(1)$ vertices v reachible via a path of length $s \leq m$, and both $\Phi_{H,S,u,v}$ and $\Phi_{P_s,u,v}$ are empty if u and v are not connected in this way. This means we've reduced the problem to showing that

$$\left|n^{\ell-1}\frac{C_{d,H,S}}{C_{d,P_s,T}}|\Phi_{P_s,u,v}| - |\Phi_{H,S,u,v}|\right| = o(n^{\ell-1}).$$

Let's write $H = H_1 \sqcup H_2 \cdots \sqcup H_\ell$, and assume that both distinguished vertices are in H_1. Recall for later use that $C_{H,S,d} = C_{H_1,S,d}C_{H_2,\emptyset}\cdots C_{H_\ell,\emptyset}$. Since each of the components is of constant size, we claim that

$$|\Phi_{H,S,u,v}| = |\Phi_{H_1,S,u,v}||\Phi_{H_2}|\cdots|\Phi_{H_\ell}| + o(n^{\ell-1})$$

where by the latter terms we mean the number of occurrernces of $H_2, ..., H_\ell$ respectively in G, without any constraints of distinguished vertices or labels. The idea is that we can choose one of the occurrences in $\Phi_{H,S,u,v}$ by first choosing where to place (H_1, S) so that the vertices in S map to u and v, then choosing where to place H_2, etc. Since each component is of constant size, we overcount only by an additive $O(n^{\ell-1})$ by ignoring the requirement that the connected components not collide. But $|\Phi_{H_i}| = p_{H_i,\emptyset,\emptyset}(\mathbf{x}, \mathbf{G})$ for each $i = 2, ..., \ell$, and by Proposition each of these are $nC_{d,H_i,\emptyset} + o(n)$. Similarly, from our discussion above,

$$|\Phi_{H_1,S_1,u,v}| = \frac{C_{H,S,d}}{C_{P_s,d}},$$

since once we declare that the two vertices in S are mapped to m-good vertices u and v, our freedom in place the rest of H_1 is exactly the number of ways to to do so in a d-regular tree. But now we are done:

$$|\Phi_{H,S,u,v}| = |\Phi_{H_1,S_1,u,v}||\Phi_{H_2}|\cdots|\Phi_{H_\ell}|+o(n^{\ell-1}) = n^{\ell-1}\frac{C_{H_1,S,d}}{C_{P_s,d}}C_{H_2}\cdots C_{H_\ell}+o(n^{\ell-1}) = n^{\ell-1}\frac{C_{H,S,d}}{C_{P_s,d}}+o(n^{\ell-1}).$$

We finally need to treat the case when $s = \infty$ and the distinguished vertices of H are in different connected components; under this assumption $|\Phi_{H,S,u,v}| = O(n^{\ell-2})$, since there are only $\ell-2$ components to place once we commit to mapping the distinguished vertices to a given u and v. Again we need to consider

$$\sum_{u,v}\left|n^{\ell-1}\frac{C_{H,S,d}}{C_{P_s,d}}|\Phi_{P_s,u,v}| - |\Phi_{H,S,u,v}|\right|,$$

and again we can restrict the sum to the m-good vertices for the price of an additive $o(n^\ell)$, since we are omitting $O(n\log n)$ terms with magnitude $O(n^{\ell-2})$. From this point the calculation continues more or less as it does above. □

Proposition [ref] in hand, we can now set about constructing a pseudoexpectation. We'll construct $l \in \mathbb{R}^{nk}$ and $X \in \mathbb{R}^{nk\times nk}$ so that (i) the $\mathcal{B}_k$ constraints in Lemma [ref] hold, and (ii)

$$\begin{aligned}\langle e, l_i\rangle &= \pi(i)n\\ \langle X_{i,j}, A_{\mathbf{G}}^{(s)}\rangle &\simeq \pi(i)M^s_{i,j}n\\ \langle X_{i,j}, \mathbb{J}\rangle &= \pi(i)\pi(j)n^2.\end{aligned}$$

It will simplify things immensely to use the same change of basis as we did in Section [ref]. Namely, letting F be the matrix of right eigenvectors, we will produce a pair $\check{l} \in \mathbb{R}^{nk}$ and $\check{X} \in \mathbb{R}^{nk\times nk}$ so that $l = (F^{-T}\otimes \mathbb{1})\check{l}$ and $X = (F^{-T}\otimes\mathbb{1})\check{X}(F^{-1}\otimes\mathbb{1})$ satisfy the above conditions. Recycling the relevant calculations from Section [ref], the above moment conditions translate to

$$\begin{aligned}\langle e, \check{l}_i\rangle &= \begin{cases} n & i = 1\\ 0 & \text{else}\end{cases}\\ \langle \check{X}_{i,j}, A_{\mathbf{G}}^{(s)}\rangle &\simeq \lambda_i^s\|q_s\|^2_{KM}n\\ \langle \check{X}_{i,j}, \mathbb{J}\rangle &= \begin{cases} n^2 & i = j = 1\\ 0 & \text{else}\end{cases}\end{aligned}$$

The key steps in designing $\check{X}$ are as follows.

Proposition 7.3. *For every m and every λ such that $|\lambda|^2(d-1) < 1$, there exists a polynomial y nonnegative on $(-2\sqrt{d-1}, 2\sqrt{d-1})$ and satisfying*

$$\langle q_s, y\rangle_{KM} = \lambda^s\|q_s\|^2_{KM}.$$

Proposition 7.4. *Let $\mathbf{G} \sim \mathcal{N}$. If there exists a polynomial y meeting the conditions of Proposition [ref] for some $\lambda \in (-1,1)$, then there exists a PSD matrix $Y(\lambda)$ for which*

$$\begin{aligned}Y(\lambda)_{u,u} &= 1 && \forall u \in [n]\\ \langle Y(\lambda), A_{\mathbf{G}}^{(s)}\rangle &\simeq \lambda^s\|q_s\|^2_{KM}n && \forall s \in [m]\\ \langle Y(\lambda), \mathbb{J}\rangle &= 0\end{aligned}$$

With these propositions in hand, define $\check{X}$ to be the $k \times k$ block diagonal matrix

$$\check{X} = \begin{pmatrix} \mathbb{J} & & & \\ & Y(\lambda_2) & & \\ & & \ddots & \\ & & & Y(\lambda_k), \end{pmatrix}$$

i.e. $\check{X}_{i,j} = 0$ when $i \neq j$, and the diagonal blocks are as above, and similarly let $\check{l} = (e, 0, ..., 0)^T$. This way, certainly

$$\begin{pmatrix} 1 & \check{l}^T \\ \check{l} & \check{X} \end{pmatrix} \succeq 0 \tag{13}$$

(by taking a Schur complement), and the three inner product conditions above are satisfied on every block. We now need to check carefully that

$$\begin{pmatrix} 1 & l^T \\ l & X \end{pmatrix} \triangleq \begin{pmatrix} 1 & \\ & F^{-T} \otimes \mathbb{1} \end{pmatrix} \begin{pmatrix} 1 & \check{l}^T \\ \check{l} & \check{X} \end{pmatrix} \begin{pmatrix} 1 & \\ & F^{-1} \otimes \mathbb{1} \end{pmatrix}$$

is a pseudoexpectation satisfying $\mathcal{B}_k$. Equation [ref] guarantees PSD-ness, since we have multiplied a matrix and its transpose on the right and left respectively of a PSD matrix. Since π is the first row of F^{-1}, we know $l_i = \pi(i)e$. On the other hand, X is obtained by changing basis block-wise, the diagonal of X depends only on the diagonals of $\mathbb{J}$ and the $Y(\lambda_i)$, all of which are all ones, so

$$\begin{aligned} \operatorname{diag} X &= \operatorname{diag}\left((F^{-T} \otimes \mathbb{1}) \operatorname{Diag} \operatorname{diag} \check{X} (F^{-1} \otimes \mathbb{1})\right) \\ &= \operatorname{diag}\left((F^{-T} \otimes \mathbb{1})(F^{-1} \otimes \mathbb{1})\right) \\ &= \operatorname{diag}\left(F^{-T}F^{-1} \otimes \mathbb{1}\right) \\ &= \operatorname{diag}\left(\operatorname{Diag} \pi \otimes \mathbb{1}\right) \\ &= (\pi(1)e, ..., \pi(k)e) \end{aligned}$$

as desired. Similarly, because $\check{X}$ is diagonal, $\check{X}_{u,u} = \mathbb{1}$, and

$$\operatorname{tr} X_{u,u} = \operatorname{tr} F^{-T}\check{X}_{u,u}F^{-1} = \operatorname{tr} F^{-T}F^{-1} = \operatorname{tr} \operatorname{Diag} \pi = 1.$$

Finally, the top row of each $\check{X}_{u,v}$ is the vector e_1^T, so

$$X_{u,v}e = F^{-T}\check{X}_{u,v}F^{-1}e = F^{-T}\check{X}_{u,v}e_1 = F^{-T}e_1 = \pi = l_u.$$

This completes the construction of our pseudoexpectation.

Remark 7.5. By correctly setting the ϵ from Proposition [ref] and the global error tolerance δ, we can once again choose $(\epsilon, \delta) = (a, b)$ with the property that whenever the $\mathrm{LoSt}(2, m)$ SDP is feasible $\delta = b$, it is feasible as well with $\delta = 2b$. Thus every one of the $\simeq$ constraints—i.e. those that depend on the observed graph $\mathbf{G}$—are satisfied with slack $\Omega(n)$.

Proof of Proposition 6.1. Such a polynomial y is exactly of the form

$$y = \sum_{s=0}^{m} \lambda^s q_s + \text{terms with larger } q_s\text{'s}.$$

We will use the extremely simple construction of letting the coefficients on the terms $q_{m+1}, q_{m+1}, \cdots$ *also* be powers of λ. The idea here is that, whenever $|\lambda|^2(d-1) < 1$, this series converges to a positive function on $(-2\sqrt{d-1}, 2\sqrt{d-1})$, so by taking a long enough initial segment, we can get a positive approximant.

In particular, let $p \gg m$ be even, and set

$$y = \sum_{s=0}^{p} \lambda^s q_s.$$

It is a standard calculation, employing the recurrence relation on the polynomials q_s, that

$$y(x) = \frac{1 - \lambda^2 + \lambda^{p+2}(d-1)q_p(x) - \lambda^{p+1}q_{p+1}(x)}{(d-1)\lambda^2 - \lambda x + 1}.$$

One an quickly verify that

$$\frac{1-\lambda^2}{(d-1)\lambda^2 - \lambda x + 1} > 0 \qquad \forall |x| \leq 2\sqrt{d-1},$$

so all we need to verify is that $\lambda^2(d-1) < 1$ ensures $\lambda^{p+2}(d-1)q_p - \lambda^{p+1}q_{p+1} \to_p 0$. This follows immediately from Lemma [ref], as $|q_p| \leq 2p\sqrt{d(d-1)^p}$. □

*Proof of Proposition 6.***.* Let y be the polynomial guaranteed in the theorem statement; our strategy will be to modify the matrix $y(A_G)$. First note that by expanding y in the q_s basis, we have

$$y(A_G) = \sum_{s=0}^{m} q_s(A_G)\lambda^s + \cdots = \sum_{s=0}^{m} A_G^{(s)}\lambda^s + \cdots,$$

so it is clear that $y(A_G)$ satisfies the affine constraints against the $A_G^{(s)}$ matrices. Moreover, as y is strictly positive on $[-2\sqrt{d-1}, 2\sqrt{d-1}]$, it is (by continuity) nonnegative on a constant size fattening of this interval, and by Friedman's theorem the spectrum of A_G other than the eignevalue at d is contained w.h.p. in such a set. Thus $y(A_G)$ is positive, except perhaps the eigenvalue $y(d)$, which we will fix in a moment.

However, $y(A_G)$ does not have the right inner product with the all ones matrix, and—unless $2\deg y + 1 < \mathrm{girth}(G)$—its diagonal entries need not be ones. Our corrective to these issues will exploit two fortunate facts. First, those diagonal entries different from one exactly correspond to the $(2\deg y + 1)$-bad vertices in G; from Lemma [ref] we know that there are at most $O(\log n)$ of these. Second, as y is a scalar polynomial and $\mathbb{J}$ commutes with A_G,

$$\langle y(A_G), \mathbb{J}/n\rangle = y(d) = O_n(1).$$

Thus we can correct the inner product with $\mathbb{J}$, and at the same time resolve the possible negativity of the eigenvalue $y(d)$, by passing to

$$\begin{aligned}\tilde{Y}(\lambda) &= \frac{1}{1 - y(d)/n}\,(\mathbb{1} - \mathbb{J}/n)\,y(A_G)\,(\mathbb{1} - \mathbb{J}/n) \\ &= \frac{1}{1 - y(d)/n}\big(y(A_G) - y(d)\mathbb{J}/n\big);\end{aligned}$$

since $\langle A_s^{(G)}, \mathbb{J}/n\rangle = q_s(d) = O(1)$ the result will still satisfy the inner product constraints with the matrices $A_s^{(G)}$ up to an additive $\pm\delta n$. This new matrix is certainly PSD, for instance by writing out $y(A_G)$

in its eigenvalue basis, and observing that left and right multiplication by $(\mathbb{1} - \mathbb{J}/n)$ simply projects away the eigenspace of the $y(d)$ eigenvalue. Thus we can write the $\tilde{Y}(\lambda)_{u,v} = \alpha_u^T \alpha_v$ for some vectors $\alpha_1, ..., \alpha_n \in \mathbb{R}^n$. The scale factor we applied above makes sure that for every u that is not $(2 \deg y + 1)$-bad, $\|\alpha_u\| = 1$, and being orthogonal to the all-ones matrix is equivalent to $\sum_u \alpha_u = 0$.

The remaining diagonal elements are at worst some constant C dependent on d and y, since the diagonal entries of each $A_{\mathbf{G}}^{(s)}$ are all $O(1)$. Thus, writing U for the set of $(2 \deg y + 1)$-bad vertices, we know

$$\left\| \sum_{u \notin U} \alpha_u \right\| = \left\| \sum_{u \in U} \alpha_u \right\| \leq C \log n$$

It is clear that by enlarging U to a set U' of size at most $C \log n$, we can choose a collection of unit vectors β_u for each $u \in U'$ so that

$$\sum_{u \in U'} \beta_u = \sum_{u \notin U'} \alpha_u.$$

Our final matrix $Y(\lambda)$ will be the Gram matrix of these new β and remaining α vectors. We must finally check that the affine constraints against the $A_{\mathbf{G}}^{(s)}$ matrices are still approximately satisfied. However, even starting from a bad vertex, there are at most a constant number of vertices within s steps of it, and at most a constant number of non-backtracking walks to any such vertex. Thus

$$\begin{aligned} \left| \langle Y(\lambda), A_{\mathbf{G}}^{(s)} \rangle - \langle \tilde{Y}(\lambda), A_{\mathbf{G}}^{(s)} \rangle \right| &= \left| 2 \sum_{u \in U', v \notin U'} (A_{\mathbf{G}}^{(s)})_{u,v} \alpha_u^T (\alpha_v - \beta_v) + \sum_{u,v \in U'} (A_{\mathbf{G}}^{(s)})_{u,u} \left(\|\alpha_u\| - \|\beta_u\| \right) \right| \\ &= O(\log n) \end{aligned}$$

where we have used that $\max_u \|\alpha_u\| = O(1)$ and broken up both summations by first enumerating the $O(\log n)$ vertices in U' and then the at most $O(1)$ vertices in its depth s neighborhood. □

8 Robustness Guarantees

In this section, again fix a planted model $\mathcal{P}$ with parameters (d, k, M, π), and let $\kappa(n)$ be some slowly growing function of n. Assume that we observe a graph $\widetilde{\mathbf{H}}$ on n vertices, which we are promised was drawn from one of $\mathcal{N}$ or $\mathcal{P}$ and then corrupted by $\kappa(n)$ adversarial edge insertions or deletions. Our goal is to decide, upon seeing $\widetilde{\mathbf{H}}$, from which model the unperturbed graph $\mathbf{G}$ was was sampled. We present an algorithm below that works for an appropriate regime of κ.

Algorithm 8.1. Given a graph $\widetilde{\mathbf{H}}$ and $m \in \mathbb{N}$ as input, do the following. Delete all edges incident to vertices that have degree greater than d in $\widetilde{\mathbf{H}}$, and then greedily add edges connecting any vertices with degree less than d to obtain a d-regular graph $\mathbf{H}$. Run the distinguishing SDP (**??**) at level m on $\mathbf{H}$ and output NULL if the SDP is infeasible, and PLANTED otherwise.

Theorem 8.2. *Let δ be any positive constant. Supposing $\lambda_2^2(d-1) = 1 + \delta$, there exist $\varepsilon > 0$ satisfying $\kappa(n) \leq \varepsilon n$, and $m \in \mathbb{N}$, such that Algorithm 8.1, on input $\widetilde{\mathbf{H}}$ and m, correctly distinguishes whether $\mathbf{G}$ was drawn from $\mathcal{N}$, or from $\mathcal{P}$ with probability $1 - o(1)$.*

Proof. Note that $\mathbf{H}$ is can be obtained by taking $\mathbf{G}$ and making up to $\beta \varepsilon n$ edge insertions and deletions for an absolute constant β. It suffices to show that (i) the SDP is feasible on $\mathbf{H}$ as input if $\mathbf{G}$ is drawn from the planted distribution, and (ii) the SDP is infeasible on $\mathbf{H}$ as input if $\mathbf{G}$ is drawn from the null distribution.

Call a vertex $v \in [n]$ *corrupted* if its $(m+1)$-neighborhood in $\mathbf{H}$ differs from its $(m+1)$-neighborhood in $\mathbf{G}$. We begin by analyzing the difference $A_{\mathbf{G}}^{(s)} - A_{\mathbf{H}}^{(s)}$ for $s \in [m]$. Suppose v is not a corrupted vertex, then $A_{\mathbf{G}}^{(s)}$ and $A_{\mathbf{H}}^{(s)}$ agree on the v-th row and column, which means $(A_{\mathbf{G}}^{(s)} - A_{\mathbf{H}}^{(s)})_{v,-} = 0$. On the other hand, if v is a corrupted vertex,

$$\begin{aligned}\left\|\left(A_{\mathbf{G}}^{(s)} - A_{\mathbf{H}}^{(s)}\right)_{v,-}\right\|_1 &\leq \left\|A_s^{(\mathbf{G})}\right\|_1 + \left\|A_s^{(\mathbf{H})}\right\|_1 \\ &\leq 2d(d-1)^{s-1}\end{aligned}$$

In particular, this means the entrywise 1-norm of $A_s^{(\mathbf{G})} - A_s^{(\mathbf{H})}$, is bounded by $2\beta\epsilon n \cdot 2d(d-1)^{\ell-1}$ since there are at most $2\beta\varepsilon n$ corrupted vertices (i.e. if all corrupted edges had disjoint endpoints).

From Remark [ref], if $\mathbf{G}$ is drawn from the planted distribution, the matrices $Y(\lambda_i)$ are PSD and satisfy the affine constraints regarding inner products with the $A_{\mathbf{G}}^{(s)}$ matrices with slack $\Omega(n)$. Every diagonal entry of $Y(\lambda_i)$ is one, so by PSDness their off-diagonal entries have modulus at most one. Thus

$$\left|\langle A_s^{(\mathbf{G})} Y(\lambda_i)\rangle - \langle A_s^{(\mathbf{H})}\rangle\right| = \left|\langle A_s^{(\mathbf{G})} - A_s^{(\mathbf{H})}\rangle\right| \leq \left\|A_s^{(\mathbf{G})} - A_s^{(\mathbf{H})}\right\|_1 \leq 2\beta\epsilon d(d-1)^{s-1}.$$

Because of the $\Omega(n)$ slack, if we construct $Y(\lambda_i)$ from $\mathbf{H}$ instead of $\mathbf{G}$, the constraints will *still* be satisfied for small enough ϵ. We can then use these $Y(\lambda_i)$ to build the full feasible solution as before.

On the other hand, when $\mathbf{G}$ is drawn from the null model, any pseudoexpectation satisfying the Boolean and Single Color constraints violates some linear combination of the above affine constraints by a margin of $\Omega(n)$, and this constraint will still be violated for ϵ sufficiently small. □

Remark 8.3. The parameter ε controlling the number of adversarial edge insertions and deletions made to random input $\mathbf{G}$ that the level-m $\texttt{LocalStatistic}$ SDP can tolerate can be seen to decrease with m, which is indicative of a tradeoff between how close to the threshold an algorithm in this hierarchy works and how robust it is to perturbations.

Corollary 8.4. *Algorithm 8.1 correctly distinguishes between whether* $\mathbf{G}$ *was drawn from the null distribution, or from the planted distribution, from input* $\widetilde{\mathbf{H}}$*, with probability* $1 - o(1)$ *when* $\kappa(n) = o(n)$.

References

[ABH16] Emmanuel Abbe, Afonso S Bandeira, and Georgina Hall, *Exact recovery in the stochastic block model*, IEEE Transactions on Information Theory **62** (2016), no. 1, 471–487.

[ABLS07] Noga Alon, Itai Benjamini, Eyal Lubetzky, and Sasha Sodin, *Non-backtracking random walks mix faster*, Communications in Contemporary Mathematics **9** (2007), no. 04, 585–603.

[AS12] Pranjal Awasthi and Or Sheffet, *Improved spectral-norm bounds for clustering*, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, Springer, 2012, pp. 37–49.

[AS15] Emmanuel Abbe and Colin Sandon, *Community detection in general stochastic block models: Fundamental limits and efficient algorithms for recovery*, 2015 IEEE 56th Annual Symposium on Foundations of Computer Science, IEEE, 2015, pp. 670–688.

[BKM17] Jess Banks, Robert Kleinberg, and Cristopher Moore, *The lov\'asz theta function for random regular graphs and community detection in the hard regime*, arXiv preprint arXiv:1705.01194 (2017).

[BLM15] Charles Bordenave, Marc Lelarge, and Laurent Massoulié, *Non-backtracking spectrum of random graphs: community detection and non-regular ramanujan graphs*, 2015 IEEE 56th Annual Symposium on Foundations of Computer Science, IEEE, 2015, pp. 1347–1357.

[BS95] Avrim Blum and Joel Spencer, *Coloring random and semi-random k-colorable graphs*, Journal of Algorithms **19** (1995), no. 2, 204–234.

[BSW01] Eli Ben-Sasson and Avi Wigderson, *Short proofs are narrowfiresolution made simple*, Journal of the ACM (JACM) **48** (2001), no. 2, 149–169.

[CJSX14] Yudong Chen, Ali Jalali, Sujay Sanghavi, and Huan Xu, *Clustering partially observed graphs via convex optimization*, The Journal of Machine Learning Research **15** (2014), no. 1, 2213–2238.

[CL$^+$15] T Tony Cai, Xiaodong Li, et al., *Robust and computationally feasible community detection in the presence of arbitrary outlier nodes*, The Annals of Statistics **43** (2015), no. 3, 1027–1059.

[CO04] Amin Coja-Oghlan, *Coloring semirandom graphs optimally*, International Colloquium on Automata, Languages, and Programming, Springer, 2004, pp. 383–395.

[CO07] _____, *Solving np-hard semirandom graph problems in polynomial expected time*, Journal of Algorithms **62** (2007), no. 1, 19–46.

[CSV17] Moses Charikar, Jacob Steinhardt, and Gregory Valiant, *Learning from untrusted data*, Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, ACM, 2017, pp. 47–60.

[DKMZ11] Aurelien Decelle, Florent Krzakala, Cristopher Moore, and Lenka Zdeborová, *Inference and phase transitions in the detection of modules in sparse networks*, Physical Review Letters **107** (2011), no. 6, 065701.

[Fei02] Uriel Feige, *Relations between average case complexity and approximation complexity*, Proceedings of the thiry-fourth annual ACM symposium on Theory of computing, ACM, 2002, pp. 534–543.

[FK00] Uriel Feige and Robert Krauthgamer, *Finding and certifying a large hidden clique in a semirandom graph*, Random Structures & Algorithms **16** (2000), no. 2, 195–208.

[FK01] Uriel Feige and Joe Kilian, *Heuristics for semirandom graph problems*, Journal of Computer and System Sciences **63** (2001), no. 4, 639–671.

[Gri01] Dima Grigoriev, *Linear lower bound on degrees of positivstellensatz calculus proofs for the parity*, Theoretical Computer Science **259** (2001), no. 1, 613–622.

[GV16] Olivier Guédon and Roman Vershynin, *Community detection in sparse networks via grothendieckfis inequality*, Probability Theory and Related Fields **165** (2016), no. 3-4, 1025–1049.

[HS17] Samuel B Hopkins and David Steurer, *Efficient bayesian estimation from few samples: community detection and related problems*, Foundations of Computer Science (FOCS), 2017 IEEE 58th Annual Symposium on, IEEE, 2017, pp. 379–390.

[HWX16] Bruce Hajek, Yihong Wu, and Jiaming Xu, *Achieving exact cluster recovery threshold via semidefinite programming*, IEEE Transactions on Information Theory **62** (2016), no. 5, 2788–2797.

[KK10] Amit Kumar and Ravindran Kannan, *Clustering with spectral norm and the k-means algorithm*, 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, IEEE, 2010, pp. 299–308.

[KV06] Michael Krivelevich and Dan Vilenchik, *Semirandom models as benchmarks for coloring algorithms*, 2006 Proceedings of the Third Workshop on Analytic Algorithmics and Combinatorics (ANALCO), SIAM, 2006, pp. 211–221.

[Mas14] Laurent Massoulié, *Community detection thresholds and the weak ramanujan property*, Proceedings of the forty-sixth annual ACM symposium on Theory of computing, ACM, 2014, pp. 694–703.

[MMV12] Konstantin Makarychev, Yury Makarychev, and Aravindan Vijayaraghavan, *Approximation algorithms for semi-random partitioning problems*, Proceedings of the forty-fourth annual ACM symposium on Theory of computing, ACM, 2012, pp. 367–384.

[MMV16] ———, *Learning communities in the presence of errors*, Conference on Learning Theory, 2016, pp. 1258–1291.

[MNS18] Elchanan Mossel, Joe Neeman, and Allan Sly, *A proof of the block model threshold conjecture*, Combinatorica **38** (2018), no. 3, 665–708.

[Moi12] Ankur Moitra, *A singly-exponential time algorithm for computing nonnegative rank*, arXiv preprint arXiv:1205.0044 (2012).

[MS15] Andrea Montanari and Subhabrata Sen, *Semidefinite programs on sparse random graphs and their application to community detection*, arXiv preprint arXiv:1504.05910 (2015).

[SVC16] Jacob Steinhardt, Gregory Valiant, and Moses Charikar, *Avoiding imposters and delinquents: Adversarial crowdsourcing and peer prediction*, Advances in Neural Information Processing Systems, 2016, pp. 4439–4447.

A Recovery

As discussed in the introduction, this paper will not settle fully the question of recovering the planted communities. However, we can at least reduce some key aspects of this problem to Conjecture [ref] regarding the spectrum of $A_{\mathbf{G}}$ when $\mathbf{G} \sim \mathcal{P}_{(d,k,M,\pi)}$.

There are numerous ways to pose the recovery task, and as many metrics of success, but let us set ourselves the modest goal of, given $\mathbf{G}$ drawn from a planted model with $\lambda_1^2, ..., \lambda_\ell^2 > (d-1)^{-1}$ and knowledge of the paramters (d, k, M, π), recovering a vector in $\mathbb{R}^n$ with constant correlation to each of the vectors $\check{x}_1, ..., \check{x}_\ell$ from the prior section. If $\ell = k$, we can use this and our knowledge of M to apply the change-of-basis F^{-1} and recover vectors correlated to the indicators $x_1, ..., x_k$ for each of the k communities.

Our first claim is that, assuming Conjecture [ref], the eigenvectors of $A_{\mathbf{G}}$ can be used to approximate the $\check{x}_i$'s. In the prior section we showed that there exists a polynomial f strictly positive on

$(-2\sqrt{d-1}, 2\sqrt{d-1}) \cup \{d\}$ with the property that

$$\check{x}_i^T f(A)\check{x}_i < -\delta n$$

for some constant δ. Writing $\mu_1, ..., \mu_n$ for the eigenvalues of $A_{\mathbf{G}}$ and $\Pi_1, \cdots \Pi_n$ for the orthogonal projectors onto their associated eigenspaces, we can expand this as

$$\begin{aligned}
-\delta n &> \sum_{u\in[n]} f(\mu_u)\check{x}_i^T \Pi_u \check{x}_i \\
&= \sum_{|\mu_u|<2\sqrt{d-1}} f(\mu_u)\check{x}_i^T \Pi_u \check{x}_i + \sum_{|\mu_u|\geq 2\sqrt{d-1}} f(\mu_u)\check{x}_i^T \Pi_u \check{x}_i \\
&\geq \sum_{|\mu_u|\geq 2\sqrt{d-1}} f(\mu_u)\check{x}_i^T \Pi_u \check{x}_i && f(x) \text{ positive on } (-2\sqrt{d-1}, 2\sqrt{d-1}) \\
&\geq \inf_{|x|\leq d} f(x) \cdot \check{x}_i^T \left(\sum_{|\mu_u|\geq 2\sqrt{d-1}} \Pi_u \right) \check{x}_i.
\end{aligned}$$

Thus, even if there are only constantly many eigenvectors outside the bulk, a (for instance) random vector in their span will have $O(n)$ correlation with each of the $\check{x}_i$'s.

In order to recover *robustly* we will lean on the results of Section [ref]. If we begin with $\mathbf{G}$ from the planted model, perform ϵn adversarial edge insertion or deletions, and then run the SDP again, Theorem [ref] tells us that the old SDP solution will *still* be feasible. Thus, if we take $\check{X}$ from the SDP run on the corrupted graph, we will still have

$$-\delta n > \langle f(A_{\mathbf{G}}), \check{X}_{i,i}\rangle \geq \inf_{|x|\leq d} f(x) \cdot \langle \sum_{|\mu_u|\geq 2\sqrt{d-1}} \Pi_u, \check{X}_{i,i}\rangle,$$

so a, say, Gaussian vector with covariance $\check{X}_{i,i}$ will have constant correlation with the subspace spanned by the outside-the-bulk eigenvectors of $A_{\mathbf{G}}$, the adjacency matrix of the *unperturbed* graph, which we showed above have the same correlation guarantee with the $\check{x}_i$'s.

B The Regular Stochastic Block Model

This appendix is devoted to several results on the RSBM, including the first moment calculation from the first section and the expectation and concentration of non-backtracking walk counts between vertices of different types. We begin with some standard results on the asymptotics of various combinatorial quantities we'll encounter.

From Stirling's approximation

$$\sqrt{2\pi n}\exp(n\log n - n) \leq n! \leq \sqrt{4\pi n}\exp(n\log n - n),$$

and the identity $(2n-1)!! = \frac{(2n)!}{2^n n!}$, we immediately get

$$\exp(n\log 2n - n) \leq (2n-1)!! \leq 2\exp(n\log 2n - n).$$

For some nonnegative vector $\alpha = (\alpha_1, ..., \alpha_k)$ with $\sum \alpha_i = 1$, write $\binom{n}{\alpha n}$ for the multinomial coefficient enumerating the ways to divide n into sets of size $\alpha_1 n, ..., \alpha_k n$. Then

$$\binom{n}{\alpha n} = \frac{n!}{\prod_i (\alpha_i n)!} \leq \frac{\sqrt{4\pi n}}{\prod_i \sqrt{2\pi\alpha_i n}} \exp nH(\alpha)$$

where $H(\alpha) \triangleq -\sum_i \alpha_i \log \alpha_i$ is the entropy of the distribution described by α.

Fix the parameters (d, k, M, π). For ease of analysis, we will work in a version of the configuration model, where a graph $\mathbf{G}$ is sampled as follows.

1. Randomly and uniformly select one of the $\binom{n}{\pi n}$ π-balanced partitions of the vertices, and adorn each vertex with d 'stubs' or 'half-edges.'
2. For each $i \in [k]$, randomly and uniformly select which of the $\pi(i)dn$ stubs will connect with every group j; there are $\binom{\pi(i)dn}{\pi(i)M_{i,-}dn}$ such partitions of each group's stubs.
3. For each $i < j$, randomly and uniformly chose one of the $(\pi(i)M_{i,j}dn)!$ matchings of the stubs between groups i and j.
4. For each $i \in [k]$, randomly and uniformly choose one of the $(\pi(i)M_{i,i}dn - 1)!!$ perfect matchings on the group i stubs.

The result will be a simple graph with probability $1 - o_n(1)$, so any results that hold with high probability in this model will hold with the same guarantee if we choose $\mathbf{G}$ uniformly from all graphs with an M-good partition. To sample in the null model, we simply adorn each vertex with d stubs, and choose one of the $(dn - 1)!!$ perfect matchings uniformly at random.

First Moment Bound. Let Ξ be the random variable counting the number of M-good partitions in a graph $\mathbf{G}$ from the null model. There are $\binom{n}{\pi n}$ possible ways to partition the vertices in accordance with π, and we can read off the probability that a uniformly random matching on the dn half-edges makes each one M-good from the sampling procedure above. In particular, using the fact that M is stocahstic with $\pi^T M = \pi$, we have

$$\begin{aligned}
\mathbb{P}[\Xi > 0] &\leq \mathbb{E}\,\Xi \\
&= \frac{1}{(dn-1)!!}\binom{n}{\pi n}\prod_i \binom{\pi(i)dn}{\pi(i)M_{i,-}dn}\prod_{i<j}(\pi(i)M_{i,j}dn)!\prod_i(\pi(i)M_{i,i}dn-1)!! \\
&\leq \mathrm{poly}(n)\exp\Bigg(-\frac{dn}{2}\log dn + \frac{dn}{2} + nH(\pi) + \sum_i \pi(i)dnH(M_{i,-}) \\
&\qquad + \frac{1}{2}\sum_{i,j}(\pi(i)M_{i,j}dn\log\pi(i)M_{i,j}dn - \pi(i)M_{i,j}dn)\Bigg) \\
&= \mathrm{poly}(n)\exp n\left(\left(1-\frac{d}{2}\right)H(\pi) + \frac{d}{2}H(\pi, M)\right)
\end{aligned}$$

where $H(M, \pi) = \sum_i \pi(i) H(M_{i,-})$ is the average row entropy of M, under the stationary distribution. Thus, the probability that $\Xi > 0$, i.e. that $\mathbf{G}$ has any M-good partitions, is exponentially small whenever

$$d > \frac{2H(\pi)}{H(\pi) - H(\pi, M)}$$

□

Remark B.1. As a sanity check, when M has zero on the diagonal and $\frac{1}{k-1}$ elsewhere, π is the uniform distribution with entropy $\log k$, and the average row entropy of M is $\log(k-1)$, so we have a first moment bound of

$$d > \frac{2 \log k}{\log k - \log(k-1)} \approx 2k \log(k-1) - \log k + 2.$$

An M-good partition is, in this case, a coloring—although not all colorings are M-good, since they might have atypically many edges between each group—and this bound matches roughly the first moment bound for coloring in Erdős-Rényi and d-regular random graphs.

C Expectations in the Planted Model

In this section we will compute the quantities

$$\mathbb{E}_{(\mathbf{G},\boldsymbol{\sigma})\sim\mathcal{P}} \langle A_{\mathbf{G}}^{(\ell)}, X_{\boldsymbol{\sigma}} \rangle$$

in the case when $\mathcal{P}$ is the planted coloring model. The calculations for symmetric or generic d-regular block models are analogous, and we will omit them in this paper, as they contribute substantial technicalities and very little in the way of actual insight. Let us assume that $\mathbf{G} \sim \mathcal{P}$ is drawn in the following way. For $1 \leq i \leq k$, let S_i be a cluster of $d\frac{n}{k}$ vertices $v_{i,1}, v_{i,2}, \cdots, v_{i,d\frac{n}{k}}$, and write $V = \bigcup_{i\in[k]} S_i$. Assume $(k-1)|d\frac{n}{k}$ and that both k and d are constant. Now,

1. Sample a uniformly random perfect matching on V, conditional on no edges between vertices in the same cluster.
2. Within each cluster S_i, collapse $v_{i,dt+1}, ..., v_{i,d(t+1)}$ into one vertex $\widetilde{v}_{i,t+1}$ for $0 \leq t \leq \frac{n}{k}$.

The model for drawing a random k-colorable d-regular graph is as follows. For $1 \leq i \leq k$, let S_i be a cluster of $d\frac{n}{k}$ vertices $v_{i,1}, v_{i,2}, \ldots, v_{i,d\frac{n}{k}}$. Let $V = \cup_{i\in[k]} S_i$. Assume $k-1$ divides $d\frac{n}{k}$. We assume k and d are constant.

1. Sample a uniformly random perfect matching on V so there is no edge between two vertices in a cluster.
2. Within each cluster S_i, collapse $v_{i,dt+1}, \ldots, v_{i,d(t+1)}$ into one vertex $\widetilde{v}_{i,t+1}$ for $0 \leq t < \frac{n}{k}$.

Weigh a nonbacktracking walk that starts and ends in the same cluster as 1, and weigh any other nonbacktracking walk with $\left(-\frac{1}{k-1}\right)$. We will need to show that the expected total weight of nonbacktracking

walks is roughly $d(d-1)^{\ell-1}\left(-\frac{1}{k-1}\right)^{\ell} n$. In particular, for a graph G with adjacency matrix A_G, suppose $\left(A_G^{(\ell)}\right)_{uv}$ contains the number of nonbacktracking walks of length ℓ from u to v, we are interested in understanding $\mathbb{E}\langle A_G^{(\ell)}, X_p\rangle$ where X_p is the PSD matrix such that

$$(X_p)_{uv} = \begin{cases} 1 & \text{if } u, v \text{ in same cluster} \\ -\frac{1}{k-1} & \text{if } u, v \text{ in different clusters} \end{cases}$$

Further, we will also need to show that the total weight of such nonbacktracking walks concentrates around the expectation. Towards these goals, we first answer the following question. Let M be a matching on a constant number of edges such that no edge is within a cluster. What is the probability that M is a contained in a random perfect matching $\mathbf{P}$ drawn in step 1?

In order to understand this probability, we zoom into how one samples a matching in step 1. We first sample a matrix C where $C_{a,b}$ denotes the number of edges going between S_a and S_b with probability proportional to the number of such perfect matchings. And then we randomly partition each S_i into $k-1$ buckets $S_{i,1}, \ldots, S_{i,k}$ of sizes $C_{i,1}, \ldots, C_{i,k}$[1] respectively, and then for each $\{i, j\}$ pair, we sample a random perfect matching between $S_{i,j}$ and $S_{j,i}$. For a given C that is symmetric and has rows and columns summing up to $d\frac{n}{k}$, the probability of sampling C in step 1 is proportional to the number of perfect matchings with $C_{a,b}$ edges between S_a and S_b, which is equal to

$$\prod_{a<b} C_{a,b}! \prod_{i\in[k]} \binom{d\frac{n}{k}}{C_{i,1}, \ldots, C_{i,k}} = (ds)!^k \prod_{a<b} \frac{1}{C_{a,b}!}$$

The probability of sampling C is proportional to $\prod_{a<b} \frac{1}{C_{a,b}!}$, which suggests that it can be sampled in the following way. Let $B_{\{a,b\}}$ be a bucket defined for each $a < b$. Then place each of $dn/2$ items in a uniformly random bucket independently, and let $\widetilde{C}_{a,b}$ be the number of items in $B_{\{a,b\}}$. Let $\mathcal{E}$ be the event that all the row and column sums of $\widetilde{C}$ equal $d\frac{n}{k}$. C is distributed as $\widetilde{C}|\mathcal{E}$.

Proposition C.1. *$\mathcal{E}$ occurs with probability $\Omega\left(\frac{1}{(dn/k)^c}\right)$ where c is a constant that only depends on d and k.*

Proof. When each bucket gets exactly $\frac{dn}{k(k-1)}$ items, then $\mathcal{E}$ occurs. The probability of this event occuring is

$$\left(\frac{2}{k(k-1)}\right)^{dn/2} \binom{dn/2}{\frac{dn}{k(k-1)}, \ldots, \frac{dn}{k(k-1)}}$$

which by Stirling's approximation, can be seen to $\Omega\left(\frac{1}{(dn/k)^{k(k-1)/4}}\right)$. □

Proposition C.2. *All $C_{a,b}$ are in the interval $I = \left[\frac{dn}{k(k-1)} - \left(\frac{dn}{k(k-1)}\right)^{1/2+\varepsilon}, \frac{dn}{k(k-1)} + \left(\frac{dn}{k(k-1)}\right)^{1/2+\varepsilon}\right]$ with probability at least $1 - \exp\left(-\Omega\left((dn/k)^{2\varepsilon}\right)\right)$ for any $0 < \varepsilon < 1/2$.*

Proof. Let δ be the probability of event $\mathcal{E}$ and let E be the event that some $\widetilde{C}_{a,b}$ is not in I.

$$\begin{aligned} \Pr[E] &= \delta \Pr[E|\mathcal{E}] + (1-\delta)\Pr[E|\overline{\mathcal{E}}] \geq \delta \Pr[E|\mathcal{E}] \\ \Pr[E|\mathcal{E}] &\leq \frac{\Pr[E]}{\delta} \end{aligned} \tag{14}$$

[1] $C_{ii} = 0$

For each $\widetilde{C}_{a,b}$ is $\frac{dn}{k(k-1)}$ in expectation, and hence it follows from Hoeffding's inequality applied to each $\{a, b\}$ pair along with a union bound over all $\{a, b\}$ pairs that event E occurs with probability at most

$$\Pr[E] \leq \exp\left(-\Omega\left((dn/k)^{2\varepsilon}\right)\right) \tag{15}$$

Combining (14), (15) and (C.1) gives

$$\Pr[E|\mathcal{E}] \leq \exp\left(-\Omega\left((dn/k)^{2\varepsilon}\right)\right)$$

from which the desired statement we want to prove follows. □

Proposition C.3. *Let* $\mathbf{P}$ *be a random perfect matching on* V *sampled in step 1 of the sampling procedure and let* M *be a matching on a constant number of edges* T*. The probability that* $M \subseteq \mathbf{P}$ *is* $(1 \pm o(1))\left(\frac{k}{dn(k-1)}\right)^{T}$*.*

Proof. Let T_a be the number of matched vertices in S_a in M. And let $T_{a,b}$ be the number of edges in M between clusters S_a and S_b. Conditioned on the matrix C with $C_{a,b}$ prescribing the number of edges in M between S_a and S_b, we give an expression for the probability of $M \subseteq \mathbf{P}$. In particular,

$$\Pr\left[M \subseteq \mathbf{P} \middle| C\right] = \frac{\prod_{a<b} \frac{C_{a,b}!}{(C_{a,b}-T_{a,b})!}}{\prod_a \frac{(dn/k)!}{(dn/k-T_a)!}} \tag{16}$$

Let E be the event that for some pair $\{a, b\}$, $C_{a,b}$ is outside interval I as defined in Proposition C.2 for any $0 < \varepsilon < 1/2$. Now, we have

$$\Pr\left[M \subseteq \mathbf{P}\right] = \Pr[E]\Pr\left[M \subseteq \mathbf{P}|E\right] + (1 - \Pr[E])\Pr\left[M \subseteq \mathbf{P}|\overline{E}\right] \tag{17}$$

From (16), we can conclude,

$$\frac{\prod_{a<b}\left(\frac{dn}{k(k-1)} - \left(\frac{dn}{k(k-1)}\right)^{1/2+\varepsilon} - T_{a,b}\right)^{T_{a,b}}}{\prod_a (dn/k)^{T_a}} \leq \Pr\left[M \subseteq \mathbf{P}|\overline{E}\right] \leq \frac{\prod_{a<b}\left(\frac{dn}{k(k-1)} + \left(\frac{dn}{k(k-1)}\right)^{1/2+\varepsilon}\right)^{T_{a,b}}}{\prod_a (dn/k - T_a)^{T_a}}$$

The bounds can be slacked to

$$\left(1 - \left(\frac{dn}{k(k-1)}\right)^{-\frac{1+4\varepsilon}{2}}\right)\frac{\prod_{a<b}\left(\frac{dn}{k(k-1)}\right)^{T_{a,b}}}{\prod_a (dn/k)^{T_a}} \leq \Pr\left[M \subseteq \mathbf{P}|\overline{E}\right] \leq \left(1 + \left(\frac{dn}{k(k-1)}\right)^{-\frac{1+4\varepsilon}{2}}\right)\frac{\prod_{a<b}\left(\frac{dn}{k(k-1)}\right)^{T_{a,b}}}{\prod_a (dn/k)^{T_a}}$$

which leads to the conclusion

$$\Pr\left[M \subseteq \mathbf{P}|\overline{E}\right] = \left(1 \pm \left(\frac{dn}{k(k-1)}\right)^{-\frac{1}{2}+2\varepsilon}\right)\left(\frac{k}{dn(k-1)}\right)^{T}$$

thus completing our proof. □

For the rest of this section, we use $\mathbf{G}$ to denote a d-regular graph sampled according to the procedure described at the start of this section, and $\mathbf{P}$ to denote the random perfect matching sampled in step 1 as an intermediate step to sampling $\mathbf{P}$.

Proposition C.4. *Given a sequence of distinct vertices $u_1, \ldots, u_\ell$ of $\mathbf{G}$ such that u_i and u_{i+1} are in different clusters for $1 \le i < \ell$, the expected number of paths formed by the sequence $u_1 \ldots u_\ell$ is*

$$(1 \pm o(1)) \frac{d}{k-1} \left(\frac{d-1}{k-1}\right)^{\ell-2} \left(\frac{k}{n}\right)^{\ell-1}$$

Proof. Let $U_i = \{u_{i,1}, \ldots, u_{i,d}\}$ be the d vertices that were collapsed to u_i in step 2. Let $\mathcal{M}$ be the collection of matchings on $\ell - 1$ edges such that there is exactly one edge between U_i and U_{i+1} for $1 \le i < \ell$. The expected number of paths in $\mathbf{G}$ in order $u_1 \ldots u_\ell$ is equal to the expected number of matchings in $\mathcal{M}$ that are contained in the random matching $\mathbf{P}$ sampled in step 1. This is in the range

$$\begin{aligned}(1 \pm o(1))|\mathcal{M}| \left(\frac{k}{dn(k-1)}\right)^{\ell-1} &= (1 \pm o(1)) d^\ell (d-1)^{\ell-2} \left(\frac{k}{dn(k-1)}\right)^{\ell-1} \\ &= (1 \pm o(1)) \frac{d}{k-1} \left(\frac{d-1}{k-1}\right)^{\ell-2} \left(\frac{k}{n}\right)^{\ell-1}\end{aligned}$$

□

The next task is to count sequences of vertices that start and end in the same cluster, and also sequences that start and end in different clusters.

Proposition C.5. *Let $P_{i,0}$ be the number of length-$(i+1)$ sequences of vertices starting and ending in the same cluster, and $P_{i,1}$ be the number of length-$(i+1)$ sequences of vertices whose last vertex is in a different cluster from the first vertex. Then*

$$Q_i := P_{i,0} - \frac{1}{k-1} P_{i,1} = (1 \pm o(1))(-1)^i \left(\frac{n}{k}\right)^{i+1} k$$

for $i \le T$ for constant T.

Proof. It is easy to see that $P_{i,0}$ and $P_{i,1}$ satisfy

$$\begin{gathered}\left(\frac{n}{k} - i\right) P_{i-1,1} \le P_{i,0} \le \frac{n}{k} P_{i-1,1} \\ \left(\frac{n}{k}(k-1) - i\right) P_{i-1,0} + \left(\frac{n}{k}(k-2) - i\right) P_{i-1,1} \le P_{i,1} \le \frac{n}{k}(k-1) P_{i-1,0} + \frac{n}{k}(k-2) P_{i-1,1}\end{gathered}$$

from which we have

$$\begin{aligned}P_{i,0} &= (1 \pm o(1)) \frac{n}{k} P_{i-1,1} \\ P_{i,1} &= (1 \pm o(1)) \left(\frac{n}{k}(k-1) P_{i-1,0} + \frac{n}{k}(k-2) P_{i-1,1}\right)\end{aligned}$$

Thus, we have

$$\begin{aligned}Q_i = P_{i,0} - \frac{1}{k-1} P_{i,1} &= (1 \pm o(1)) \left(\frac{n}{k(k-1)} P_{i-1,1} - \frac{n}{k} P_{i-1,0}\right) \\ &= -(1 \pm o(1)) \frac{n}{k} \left(P_{i-1,0} - \frac{1}{k-1} P_{i-1,1}\right) = -(1 \pm o(1)) \frac{n}{k} Q_{i-1}\end{aligned}$$

Since $Q_0 = n$, we have that Q_i must be $(1 \pm o(1))(-1)^i \left(\frac{n}{k}\right)^{i+1} k$ as long as i is constant. □

Definition C.6. Let G and H be graphs. Given an injective map π from $V(G)$ to $V(H)$, we call π an *occurrence* of G in H if $\pi(E(G)) := \{\{\pi(a), \pi(b)\} : \{a, b\} \in E(G)\}$ is contained in $E(H)$. The number of occurrences of G in H under π is the number of subsets of $E(H)$ that are equal to $\pi(E(G))$ (this could be a greater than 1 if $E(H)$ is a multiset, i.e., if $E(H)$ has parallel edges). The number of occurrences of G in H is

$$\sum_{\pi \text{ injective from } V(G) \text{ to } V(H)} \text{number of occurrences of } G \text{ in } H \text{ under } \pi$$

Proposition C.7. *Let S be a graph with α vertices and β edges for constant α, β. The expected number of occurrences of S in $\mathbf{G}$ is $O(n^{\alpha-\beta})$. In particular, if $\alpha \geq \beta$, the expected number of occurrences is $O(1)$.*

Proof. Define $\Pi := \{\pi : V(S) \to V(\mathbf{G}) : \pi \text{ injective}\}$, fix $\pi \in \Pi$ and consider the set $\pi(V(S))$. For each $v \in V(S)$ let $U_{\pi,v} := \{u_1, \ldots, u_d\}$ be the collection of d vertices of V prior to being collapsed to $\pi(v)$ in step 2. Let $\mathcal{M}_\pi$ be the collection of partial matchings M on $\cup_{v \in V(S)} U_v$ such that the number of edges between U_v and $U_{v'}$ is equal to the number of edges between v and v' in S. Observe that π is an occurrence of S in $\mathbf{G}$ if and only if there is $M \in \mathcal{M}$ for which $M \subseteq \mathbf{P}$. The size of $\mathcal{M}_\pi$ is at most d^α. For a given $M \in \mathcal{M}_\pi$, we know from Proposition C.3 that

$$\Pr[M \subseteq \mathbf{P}] = (1 \pm o(1)) \left(\frac{k}{dn(k-1)}\right)^\beta$$

and the expected number of M in $\mathcal{M}_\pi$ is thus at most

$$(1 \pm o(1)) \left(\frac{k}{dn(k-1)}\right)^\beta d^\alpha$$

Finally, the expected number of occurrences of S in $\mathbf{G}$ is

$$(1 \pm o(1))|\Pi| \left(\frac{k}{n(k-1)}\right)^\beta d^{\alpha-\beta} \leq (1 \pm o(1)) n^\alpha \left(\frac{k}{n(k-1)}\right)^\beta d^{\alpha-\beta} = O(n^{\alpha-\beta})$$

□

Finally, we are set to prove

Proposition C.8. $\mathbb{E}\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle = (1 \pm o(1)) d(d-1)^{\ell-1} \left(-\frac{1}{k-1}\right)^\ell n$

Proof. Let $\mathcal{U}$ be the collection of sequences of vertices $u_0, \ldots, u_\ell$ such that u_i and u_{i+1} are in different clusters and $u_i \neq u_{i+2}$. For such a sequence, assign weight $w(u_0, u_\ell)$ as 1 if u_0 and u_ℓ are in the same cluster and $\frac{-1}{k-1}$ if they are in different clusters. Let $\mathcal{U}_{\text{distinct}} \subseteq \mathcal{U}$ be the subcollection of sequences for which the vertices $u_0, \ldots, u_\ell$ are distinct. We have,

$$\begin{aligned}
\mathbb{E}\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle &= \sum_{(u_0,\ldots,u_\ell) \in \mathcal{U}} w(u_0, u_\ell)\, \mathbb{E}[\text{number of paths on } u_0, \ldots, u_\ell] \\
&= \sum_{(u_0,\ldots,u_\ell) \in \mathcal{U}_{\text{distinct}}} w(u_0, u_\ell)\, \mathbb{E}[\text{number of paths on } u_0, \ldots, u_\ell] \\
&+ \sum_{(u_0,\ldots,u_\ell) \in \mathcal{U} \setminus \mathcal{U}_{\text{distinct}}} w(u_0, u_\ell)\, \mathbb{E}[\text{number of paths on } u_0, \ldots, u_\ell]
\end{aligned}$$

Applying Proposition C.4 on the first term tells us that it is

$$(1 \pm o(1))d(d-1)^{\ell-1}\left(\frac{1}{k-1}\right)^{\ell}\left(\frac{k}{n}\right)^{\ell}\sum_{(u_0,\ldots,u_\ell)\in\mathcal{U}_{\text{distinct}}} w(u_0,u_\ell)$$

and then from Proposition C.5 we can write the above as

$$(1 \pm o(1))d(d-1)^{\ell-1}\left(\frac{1}{k-1}\right)^{\ell}\left(\frac{k}{n}\right)^{\ell}\left(\frac{n}{k}\right)^{\ell+1}k = (1 \pm o(1))d(d-1)^{\ell-1}\left(\frac{1}{k-1}\right)^{\ell}n$$

The second term is in $\left[-\frac{1}{k-1},\ 1\right]\sum_{(u_0,\ldots,u_\ell)\in\mathcal{U}\setminus\mathcal{U}_{\text{distinct}}}\mathbb{E}[\text{number of paths on } u_0,\ldots,u_\ell]$, which from Proposition C.7 is in range $\pm O(1)$ since the above sum over $\mathcal{U}\setminus\mathcal{U}_{\text{distinct}}$ counts the expected number of occurrences of subgraphs in a constant sized collection, each of which have at least as many vertices as edges.

Thus, $\mathbb{E}\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle = (1 \pm o(1))d(d-1)^{\ell-1}\left(-\frac{1}{k-1}\right)^{\ell}n$ as desired.

□

In order to show concentration of $\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle$, we bound its variance.

Proposition C.9. $\mathbb{V}\left[\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle\right] = o(n^2)$.

Proof. For a nonbacktracking sequence of vertices in $V(\mathbf{G})$ (also equal to $\widetilde{V}$) $\underline{u} := (u_0, u_1, \ldots, u_\ell)$, i.e. a sequence satisfying $u_i \neq u_{i+2}$ for all i, define $\mathcal{M}_{\underline{u}}$ is the collection of matchings on V such that when V is collapsed to $\widetilde{V}$, each $M \in \mathcal{M}_{\underline{u}}$ collapses to the nonbacktracking walk $u_0u_1u_2\ldots u_\ell$. Each M also comes associated with a weight w_M, which is 1 if u_1 and u_ℓ are in the same cluster and $-\frac{1}{k-1}$ otherwise. Let $\mathcal{M}$ be the collection of all pairs $(M, \underline{u})$ where $\underline{u}$ is a nonbacktracking sequence and $M \in \mathcal{M}_{\underline{u}}$ over all such sequences. Then,

$$\begin{aligned}
\mathbb{E}\left[\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle^2\right] &= \sum_{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq\mathbf{P}}\mathbf{1}_{M_2\subseteq\mathbf{P}}\right] w_{M_1}w_{M_2} \\
&= \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}}} \mathbb{E}\left[\mathbf{1}_{M_1\cup M_2\subseteq\mathbf{P}}\right] w_{M_1}w_{M_2} \\
&= \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ \underline{u_1},\underline{u_2} \text{ disjoint}}} \mathbb{E}[\mathbf{1}_{M_1\subseteq\mathbf{P}}\mathbf{1}_{M_2\subseteq\mathbf{P}}]w_{M_1}w_{M_2} + \\
&\quad \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\cup M_2\subseteq\mathbf{P}}\right] w_{M_1}w_{M_2}
\end{aligned}$$

On the other hand,

$$\mathbb{E}\left[\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle\right]^2 = \sum_{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq\mathbf{P}}\right]\mathbb{E}\left[\mathbf{1}_{M_2\subseteq\mathbf{P}}\right] w_{M_1}w_{M_2}$$

which can similarly be broken into

$$= \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ disjoint}}} \mathbb{E}[\mathbf{1}_{M_1\subseteq\mathbf{P}}]\,\mathbb{E}[\mathbf{1}_{M_2\subseteq\mathbf{P}}] w_{M_1} w_{M_2} + \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq\mathbf{P}}\right]\mathbb{E}\left[\mathbf{1}_{M_2\subseteq\mathbf{P}}\right] w_{M_1} w_{M_2}$$

Towards computing $\mathbb{V}\left[\langle A_{\mathbf{G}}^{(\ell)}, X_p\rangle\right]$, we first calculate

$$\begin{aligned} &\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ disjoint}}} w_{M_1} w_{M_2} \left(\mathbb{E}[\mathbf{1}_{M_1\subseteq\mathbf{P}}\mathbf{1}_{M_2\subseteq\mathbf{P}}] - \mathbb{E}[\mathbf{1}_{M_1\subseteq\mathbf{P}}]\,\mathbb{E}[\mathbf{1}_{M_2\subseteq\mathbf{P}}]\right) \\ = &\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ disjoint}}} w_{M_1} w_{M_2} \left(\Pr[M_1\cup M_2\subseteq\mathbf{P}] - \Pr[M_1\subseteq\mathbf{P}]\Pr[M_2\subseteq\mathbf{P}]\right) \end{aligned}$$

which, by an application of Proposition C.3, is

$$\begin{aligned} &= \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ disjoint}}} w_{M_1} w_{M_2} \cdot o(1) \left(\frac{k}{dn(k-1)}\right)^{|M_1|+|M_2|} \\ &\leq \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ disjoint}}} o(1) \left(\frac{k}{dn(k-1)}\right)^{2\ell} \end{aligned}$$

The number of ways to pick a disjoint pair $\underline{u_1}, \underline{u_2}$ is at most the number of ways to pick a pair of nonbacktracking sequences, which is at most $n^2\left(\frac{n}{k}(k-1)\right)^{\ell}$. For a given nonbacktracking sequence, there are at most $d^{\ell+1}$ matchings that collapse to it, and hence the above sum can be upper bounded by,

$$o(1)\cdot\left(\frac{k}{dn(k-1)}\right)^{2\ell}\cdot n^2\left(\frac{n}{d}(k-1)\right)^{2\ell} d^{2\ell+2} = o(1)n^2 = o(n^2)$$

Thus, in order to finish the proof, it suffices to upper bound

$$\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ M_1\cup M_2 \text{ valid matching} \\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\cup M_2\subseteq\mathbf{P}}\right] w_{M_1} w_{M_2} - \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq\mathbf{P}}\right]\mathbb{E}\left[\mathbf{1}_{M_2\subseteq\mathbf{P}}\right] w_{M_1} w_{M_2}$$

by $o(n^2)$. We can immediately upper bound the above by

$$\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ M_1\cup M_2 \text{ valid matching} \\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\cup M_2\subseteq\mathbf{P}}\right] + \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M} \\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq\mathbf{P}}\right]\mathbb{E}\left[\mathbf{1}_{M_2\subseteq\mathbf{P}}\right]$$

and then bound each term separately.

First, consider the random variable

$$\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbf{1}_{M_1\cup M_2\subseteq P} \tag{18}$$

We will prove an upper bound of $O(n)$ that always holds on the random variable, thereby giving that upper bound on

$$\mathbb{E}\left[\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbf{1}_{M_1\cup M_2\subseteq \mathbf{P}}\right] = \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\cup M_2\subseteq \mathbf{P}}\right]$$

The number of nonbacktracking walks of length ℓ in any d-regular graph is exactly $skd(d-1)^{\ell-1}$, and the number of nonbacktracking walks in a fixed d-regular graph that intersect a fixed nonbacktracking walk $\underline{u}$ is bounded by a constant C. Hence, the number of choices for pairs $\underline{u_1}, \underline{u_2}$ such that they intersect is $O(n)$. (18) can be written as

$$\sum_{\underline{u_1},\underline{u_2} \text{ intersect}} \sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ M_1\cup M_2 \text{ valid matching}}} \mathbf{1}_{M_1\cup M_2\subseteq P} \leq \sum_{\underline{u_1},\underline{u_2} \text{ intersect}} d^{2\ell+2}\mathbf{1}_{M_1\cup M_2\subseteq P} = d^{2\ell+1} \sum_{\underline{u_1},\underline{u_2} \text{ intersect}} \mathbf{1}_{M_1\cup M_2\subseteq P}$$

which results in an overall bound of $O(n)$.

Finally, we upper bound the last piece by $O(n)$,

$$\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} \mathbb{E}\left[\mathbf{1}_{M_1\subseteq \mathbf{P}}\right]\mathbb{E}\left[\mathbf{1}_{M_2\subseteq \mathbf{P}}\right] \tag{19}$$

Applying Proposition C.3 to the above tells us that the quantity is

$$\sum_{\substack{(M_1,\underline{u_1}),(M_2,\underline{u_2})\in\mathcal{M}\\ \underline{u_1},\underline{u_2} \text{ intersect}}} (1\pm o(1))\left(\frac{1}{ds(k-1)}\right)^{2\ell}$$

Combining the facts that (i) for a fixed $\underline{u}$, there are $d^{\ell+1}$ matchings that collapse to it, (ii) there are at most $sk(s(k-1))^{\ell}$ choices for $\underline{u_1}$, (iii) there are $C(s(k-1))^{\ell}$ choices for $\underline{u_2}$ once $\underline{u_1}$ is fixed, we can bound (19) by

$$(1\pm o(1))C\left(\frac{1}{ds(k-1)}\right)^{2\ell} d^{2\ell+2}n\left(\frac{n}{k}(k-1)\right)^{2\ell} = O(n)$$

which completes the proof of the variance bound. □

As an upshot of Proposition C.9 and Chebyshev's inequality, we can conclude:

Theorem C.10. $\langle A_{\mathbf{G}}^{\ell}, X_p\rangle = (1\pm o(1))d(d-1)^{\ell-1}\left(-\frac{1}{k-1}\right)^{\ell} n$ *with probability* $1-o(1)$.