

Non-Reconstructability in the Stochastic Block Model

Joe Neeman ^{*1,2} and Praneeth Netrapalli ^{†1}

¹Dept. of Electrical and Computer Engg., UT Austin

²Dept. of Mathematics, UT Austin

April 28, 2014

Abstract

We consider the problem of clustering (or reconstruction) in the stochastic block model, in the regime where the average degree is constant. For the case of two clusters with equal sizes, recent results [MNS13, Mas14, MNS14] show that reconstructability undergoes a phase transition at the Kesten-Stigum bound of $\lambda_2^2 d = 1$, where λ_2 is the second largest eigenvalue of a related stochastic matrix and d is the average degree. In this paper, we address the general case of more than two clusters and/or unbalanced cluster sizes. Our main result is a sufficient condition for clustering to be impossible, which matches the existing result for two clusters of equal sizes. A key ingredient in our result is a new connection between non-reconstructability and non-distinguishability of the block model from an Erdős-Rényi model with the same average degree. We also show that it is some times possible to reconstruct even when $\lambda_2^2 d < 1$. Our results provide evidence supporting a series of conjectures made by Decelle et al. [DKMZ11] regarding reconstructability and distinguishability of stochastic block models (but do not settle them).

1 Introduction

Stochastic block models are popular models for random graphs that exhibit community structures. In these models, the vertices of a graph are divided into at least two different classes, and then edges are added between vertices with probabilities that depend on the classes of the vertices. We will consider sparse stochastic block models, where the average degree of each vertex is constant, while the number of vertices tends to infinity.

The fundamental problem in stochastic block models is the *community detection*, or *reconstruction* problem: if we are given a graph from a stochastic block model, but we are not told which vertex belongs to which class, then can we recover this information from the structure of the graph? In the sparse regime, straightforward probabilistic arguments show that it is not possible to correctly classify more than a certain fraction of the vertices correctly (unlike in the denser case, where it is sometimes possible to completely reconstruct the classes). Given this restriction, we say that a stochastic block model is reconstructible if there is some algorithm that recovers the classes more accurately than a random guess would.

^{*}joeneeman@gmail.com

[†]praneethn@utexas.edu

Decelle et al. [DKMZ11] stimulated the study of block model reconstructability with a series of striking conjectures, which were backed up by simulations and connections to statistics physics. They proposed three main scenarios: i) if the “signal” in the model is strong enough compared to the “noise,” then the model can be reconstructed efficiently, ii) if the signal is somewhat weaker, then the model is reconstructible, but it is computationally hard to actually carry out the reconstruction, and finally, iii) if the signal is too weak then the model is not reconstructible. Decelle et al. further divide this third scenario into two parts, depending on whether or not belief propagation has a fixed point that is correlated with the true classification.

Besides merely conjecturing the existence of these various scenarios, Decelle et al. gave estimates for the boundaries between them. Specifically, they conjectured that the boundary between the efficiently reconstructible and the computationally hard regions should always occur at the *Kesten-Stigum bound*, while the reconstructibility boundary corresponds to the condensation transition in spin glasses. In the special case of two classes with equal sizes, these conjectures have been verified by Mossel et al. [MNS13, MNS14] and Massoulié [Mas14]; in this special case, the two transitions coincide and so there is no reconstructible-but-hard regime.

Besides the reconstruction problem, it is natural to ask whether a stochastic block model can be distinguished from an Erdős-Rényi model with the same average degree. This is called the *distinguishability* problem, and it is intuitively easier than the reconstruction problem in the sense that an algorithm that finds communities in a block model should also be able to check whether there exist meaningful communities. However, we are not aware of a rigorous version of this statement; indeed, one of our main results shows that non-reconstructibility follows from something somewhat stronger than non-distinguishability (specifically, the existence of a certain second moment).

In addition to showing a connection between reconstruction and distinguishability, we explore the distinguishability problem in more detail. Specifically, we show that above the Kesten-Stigum bound a block model is orthogonal to the corresponding Erdős-Rényi model; on the other hand, the two models are mutually contiguous sufficiently far below the Kesten-Stigum bound. Except in the special case of two equal-sized classes (which was previously considered by Mossel et al. [MNS13]), we do not know whether the contiguity region extends all the way to the Kesten-Stigum bound – indeed we exhibit models with two highly unbalanced classes, where the contiguity region does not extend all the way to the Kesten-Stigum bound. We do derive sharp bounds for the region on which a certain second moment is finite, but the second moment condition in question is only sufficient, but not necessary, to prove contiguity.

2 Background and related work

Stochastic block models were introduced by Holland, Laskey and Leinhardt [HLL83] in the 1980s in order to study community detection in random networks, and then re-discovered independently by Dyer and Frieze [DF89] in the context of computational complexity. Their work and subsequent work by – to mention a few – Jerrum and Sorkin [JS98], Condon and Karp [CK01], and Snijders and Nowicki [SN97] focused primarily on the regime in which the graph is sufficiently dense, and the signal sufficiently strong, to exactly recover the communities with high probability.

More recent work has considered very sparse block models, where the average degree of each vertex is bounded as the number of vertices increases. In this regime, the first algorithm with provable guarantees was given by Coja-Oghlan [CO10]. More recently, Massoulié [Mas14] and Mossel et al. [MNS14] gave algorithms with better guarantees, but only in the case of two classes

with approximately equal size. The case of two classes with very unbalanced sizes was addressed recently by Verzelen and Arias-Castro [VAC14]; they do not study the problem of reconstructing communities, but only the problem of detecting whether a community exists. The sparse regime has also seen work without proven performance guarantees: Decelle et al. [DKMZ11] gave an algorithm based on belief propagation, while Krzakala et al. [KMM⁺13] proposed a spectral algorithm.

3 Definitions and results

A stochastic block model with $s \geq 2$ communities is parametrized by two quantities: the distribution $\pi \in \Delta_{s-1}$ of vertex classes and the symmetric matrix $M \in \mathbb{R}^{s \times s}$ of edge probabilities. Given these two parameters, a random graph from the block model $\mathcal{G}(n, M, \pi)$ is sampled as follows: for each vertex v , sample a label σ_v in $[s] = \{0, 1, \dots, s-1\}$ independently with distribution π . Then, for each pair (u, v) , include the edge (u, v) in the graph independently with probability $n^{-1}M_{\sigma_u, \sigma_v}$. Since we will work with a fixed M and π throughout, we denote $\mathcal{G}(n, M, \pi)$ by \mathbb{P}_n . Note that according to the preceding description, we have the following explicit form for the density of \mathbb{P}_n :

$$\mathbb{P}_n(G, \sigma) = \prod_{v \in V(G)} \pi_{\sigma_v} \prod_{(u, v) \in E(G)} \frac{M_{\sigma_u, \sigma_v}}{n} \prod_{(u, v) \notin E(G)} \left(1 - \frac{M_{\sigma_u, \sigma_v}}{n}\right).$$

We will assume throughout that every vertex in $G \sim \mathbb{P}_n$ has the same expected degree. (In terms of M and π , this means that $\sum_j M_{ij}\pi_j$ does not depend on i .) Without this assumption, reconstruction and distinguishability – at least in the way that we will phrase them – are trivial, since we gain non-trivial information on the class of a vertex just by considering its degree.

With the preceding assumption in mind, let $d = \sum_j M_{ij}\pi_j$ be the expected degree of an arbitrary vertex. In order to discuss distinguishability, we will compare \mathbb{P}_n with the Erdős-Rényi distribution $\mathbb{Q}_n := \mathcal{G}(n, d/n)$.

Throughout this work, we will make use of the matrix T defined by

$$T_{ij} = \frac{1}{d}\pi_i M_{ij},$$

or in other words, $T = \frac{1}{d}\text{diag}(\pi)M$. Note that T is a stochastic matrix, in the sense that it has non-negative elements and all its rows sum to 1. The Perron-Frobenius eigenvectors of T are π on the left, and $\mathbf{1}$ on the right (where $\mathbf{1}$ denotes the vector of ones), and the corresponding eigenvalue is 1. We let $\lambda_1, \dots, \lambda_s$ be the eigenvalues of T , arranged in order of decreasing absolute value (so that $\lambda_1 = 1$ and $|\lambda_2| \leq 1$).

There is an important probabilistic interpretation of the matrix T relating to the local structure of $G \sim \mathbb{P}_n$; although we will not rely on this interpretation in the current work, it played an important role in [MNS13]. Indeed, using an argument similar to the one in [MNS13], one can show that for any fixed radius R , the R -neighborhood of a vertex in $G \sim \mathbb{P}_n$ has almost the same distribution as a Galton-Watson tree with radius R and offspring distribution $\text{Poisson}(d)$. Then, the class labels on the neighborhood can be generated by first choosing the label of the root according to π and then, conditioned on the root's label being i , choosing its children's labels independently to be j with probability T_{ij} . This procedure continues down the tree: any vertex with parent u has probability $T_{\sigma_u j}$ to receive the label j . Thus, T is the transition matrix of a certain Markov process that describes a procedure for approximately generating a local neighborhood in G .

3.1 Positive results

3.1.1 Distinguishability

It is not hard to show that if $d\lambda_2^2 > 1$ then the block model \mathbb{P}_n is asymptotically orthogonal to the Erdős-Rényi model \mathbb{Q}_n , in the sense that there is a sequence of events Ω_n such that $\mathbb{P}_n(\Omega_n) \rightarrow 1$ and $\mathbb{Q}_n(\Omega_n) \rightarrow 0$. Indeed, this statement follows fairly easily from the following cycle-counting result, due to Bollobás et al. [BJR07]

Proposition 3.1. *Let X_k be the number of k -cycles in G . Then*

$$\begin{aligned} X_k &\xrightarrow{d} \text{Pois}\left(\frac{1}{2k}d^k\right) \text{ under } \mathbb{Q}_n, \text{ and} \\ X_k &\xrightarrow{d} \text{Pois}\left(\frac{1}{2k}d^k \text{tr}(T^k)\right) \text{ under } \mathbb{P}_n. \end{aligned}$$

We remark that the X_k are also asymptotically independent, in the sense that for any positive numbers j_3, \dots, j_m , the moment $\mathbb{E} \prod_{i=3}^m X_i^{j_i}$ converges as $n \rightarrow \infty$ to $\mathbb{E} \prod_{i=3}^m Y_i^{j_i}$, for independent Poisson variables Y_3, \dots, Y_m .

Now, Chebyshev's inequality implies that $X_k \leq \frac{1}{2k}d^k + O(k^{-1/2}d^{k/2})$ under \mathbb{Q}_n , while $X_k \geq \frac{1}{2k}d^k \text{tr}(T^k) - O(k^{-1/2}d^{k/2})$ under \mathbb{P}_n . If $d\lambda_2^2 > 1$, then these ranges are disjoint for large enough k ; in particular, the event $\Omega_n = \{X_k \geq \frac{1}{2k}d^k \text{tr}(T^k) - O(k^{-1/2}d^{k/2})\}$ satisfies $\mathbb{P}_n(\Omega_n) \rightarrow 1$ and $\mathbb{Q}_n(\Omega_n) \rightarrow 0$. The details of this argument are contained in [MNS13] in the case $s = 2$, $\pi = (1/2, 1/2)$, but exactly the same argument applies in the general case:

Theorem 3.2. *If $d\lambda_2^2 > 1$ then \mathbb{P}_n and \mathbb{Q}_n are asymptotically orthogonal.*

3.1.2 Reconstructability

Let σ and τ denote labellings in $[s]^n$, and let

$$\begin{aligned} N_i(\sigma) &= \#\{v : \sigma_v = i\} \\ N_{ij}(\sigma, \tau) &= \#\{v : \sigma_v = i, \tau_v = j\}. \end{aligned}$$

We define the *overlap* between σ and τ by

$$\text{overlap}(\sigma, \tau) = \frac{1}{n} \max_{\rho} \sum_{i=1}^s \left(N_{i\rho(i)}(\sigma, \tau) - \frac{1}{n} N_i(\sigma) N_{\rho(i)}(\tau) \right),$$

where the supremum runs over all permutations ρ of $[s]$. In words, σ and τ have a positive overlap if there is some relabelling of $[s]$ so that they are positively correlated.

We say that the block model $\mathbb{P}_n = \mathcal{G}(n, M/n, \pi)$ is *reconstructable* if there is some $\delta > 0$ and an algorithm \mathcal{A} mapping graphs to labellings such that if $(G, \sigma) \sim \mathbb{P}_n$ then

$$\lim_{n \rightarrow \infty} \Pr(\text{overlap}(\mathcal{A}(G), \sigma) > \delta) > 0.$$

In other words, we are looking for an algorithm that guarantees a non-trivial overlap, with a non-trivial probability, as $n \rightarrow \infty$.

Mossel et al. [MNS13, MNS14] and Massoulié [Mas14] show that for balanced two cluster case, $d\lambda_2^2 = 1$ is the threshold for reconstructability. It was not known if this is also the threshold for unbalanced two cluster case. The following result shows that this is not the case.

Proposition 3.3. *For every $\epsilon > 0$, there exist (unbalanced) 2-cluster models with $d\lambda_2^2 < \epsilon$ where reconstruction is possible.*

The proof is a simple application of Bernstein's inequality and can be found in Section 4. We remark, however, that our reconstruction algorithm for proving Proposition 3.3 is not computationally efficient. Indeed, if Decelle et al.'s [DKMZ11] are correct then no computationally efficient reconstruction is possible when $d\lambda_2^2 < 1$.

3.2 Negative results

At the other extreme of asymptotic orthogonality is contiguity: we say that \mathbb{P}_n is asymptotically contiguous to \mathbb{Q}_n if for any sequence of events Ω_n , $\mathbb{Q}_n(\Omega_n) \rightarrow 1$ implies $\mathbb{P}_n(\Omega_n) \rightarrow 1$. We say that \mathbb{P}_n and \mathbb{Q}_n are mutually asymptotically contiguous if \mathbb{P}_n is asymptotically contiguous to \mathbb{Q}_n and \mathbb{Q}_n is asymptotically contiguous to \mathbb{P}_n . From the statistical perspective of distinguishing \mathbb{P}_n and \mathbb{Q}_n , mutual asymptotic contiguity implies that no test could ever be sure whether a given sample came from \mathbb{P}_n or \mathbb{Q}_n .

In the case $s = 2$, $\pi = (1/2, 1/2)$, Mossel et al. [MNS13] gave a converse to Theorem 3.2: they showed that if $d\lambda_2^2 < 1$ then \mathbb{P}_n and \mathbb{Q}_n are mutually asymptotically contiguous. In the general case, we still lack a sharp converse to Theorem 3.2 (indeed the proof of Proposition 3.3 shows that there can not be one). Nevertheless, we give a sufficient condition for \mathbb{P}_n and \mathbb{Q}_n to be mutually asymptotically contiguous.

3.2.1 The uniform integrability condition

At a crucial point in our analysis, we require that the exponential of a certain multinomial quadratic form be uniformly integrable. This is the main place in which our analysis differs from the special case considered in [MNS13]: in the case of two balanced classes, Mossel et al. were led to consider $\exp(\lambda Z_n^2)$, where $Z_n = 2n^{-1/2}(\text{Binom}(n, 1/2) - n/2)$. This is a particularly nice special case because $\exp(\lambda Z_n^2)$ is uniformly integrable for all $\lambda < 1/2$, which is exactly the set of λ for which $\mathbb{E} \exp(\lambda Z^2) < \infty$, where $Z \sim \mathcal{N}(0, 1)$. The situation is more complicated for general binomial and multinomial variables, and it leads us to the following definitions:

Definition 3.4. *Let Δ_k to denote the simplex in k -dimensions,*

$$\Delta_k := \left\{ p \in \mathbb{R}^k : p_i \geq 0, \sum_{i=1}^k p_i = 1 \right\}.$$

Define $D : \Delta_k \times \Delta_k \rightarrow \mathbb{R}$ by

$$D(p, q) = \sum_{i=1}^k p_i \log(p_i/q_i).$$

Note that if we interpret $p, q \in \Delta_k$ as probability distributions on a k -point set, then $D(p, q)$ is exactly the Kullback-Leibler divergence between them.

Definition 3.5. *For $\pi \in \Delta_s$, define*

$$\Delta_{s^2}(\pi) := \left\{ (p_{ij})_{i,j=1}^s \in \Delta_{s^2} : \sum_{i=1}^s p_{ij} = \pi_j \text{ and } \sum_{j=1}^s p_{ij} = \pi_i \text{ for all } i, j \right\}.$$

In other words, elements of $\Delta_{s^2}(\pi)$ are probability distributions on $[s]^2$ that have π as their marginal distributions.

Definition 3.6. For $\pi \in \Delta_s$ and an $s \times s$ matrix A , let $p = \pi \otimes \pi$ and define

$$Q(\pi, A) = \sup_{\alpha \in \Delta_{s^2}(\pi)} \frac{(\alpha - p)^T (A \otimes A)(\alpha - p)}{D(\alpha, p)}.$$

The preceding definition may not seem well-motivated, but we will show that $Q(\pi, A) < 1$ is exactly the right condition for a certain exponentiated quadratic form involving A to be uniformly integrable. Moreover, although we do not know any simple algebraic expression for Q , one can easily compute numerical approximations; see Figure 1.

3.2.2 Non-distinguishability

Theorem 3.7. Let $\mathbb{P}_n = \mathcal{G}(n, M/n, \pi)$ and $\mathbb{Q}_n = \mathcal{G}(n, d/n)$, where $d = \sum_j M_{ij}\pi_j$. Define $A = M - d\mathbf{1}\mathbf{1}^T$. If $Q(\pi, A/\sqrt{2d}) < 1$ then \mathbb{P}_n and \mathbb{Q}_n are mutually contiguous.

For comparison with Theorem 3.2, note that $Q(\pi, A/\sqrt{2d}) < 1$ implies that $\lambda_2^2 d < 1$. This comes from comparing the second derivatives in the numerator and denominator of Q : if $Q < 1$ then the Hessian of the numerator must be smaller (in the semidefinite order) than the denominator, and this turns out to be equivalent to $\lambda_2^2 d < 1$.

We remark that while $Q(\pi, A/\sqrt{2d}) < 1$ is only a sufficient condition for the contiguity of \mathbb{P}_n and \mathbb{Q}_n , it is actually a sharp condition for a certain second moment to exist:

Theorem 3.8. Fix a sequence a_n with $a_n = o(n)$ and $a_n = \omega(\sqrt{n})$. Let Ω_n be the event that for all $i \in [s]$, $|\{u : \sigma_u = i\}| = n\pi_i \pm a_n$. With the notation of Theorem 3.7, take $\tilde{\mathbb{P}}_n$ to be \mathbb{P}_n conditioned on Ω . If $Q(\pi, A/\sqrt{2d}) < 1$ then

$$\lim_{n \rightarrow \infty} \mathbb{E}_{\mathbb{Q}_n} \left(\frac{d\tilde{\mathbb{P}}_n}{d\mathbb{Q}_n} \right)^2 = (1 + o(1)) \prod_{i,j=2}^s \psi(d\lambda_i \lambda_j) < \infty, \quad (1)$$

where $\psi(x) = (1 - x)^{-1/2} e^{-x/2 - x^2/4}$. On the other hand, if $Q(\pi, A/\sqrt{2d}) > 1$ then

$$\lim_{n \rightarrow \infty} \mathbb{E}_{\mathbb{Q}_n} \left(\frac{d\tilde{\mathbb{P}}_n}{d\mathbb{Q}_n} \right)^2 = \infty.$$

In fact, Theorem 3.8 is the important technical step in the proof of Theorem 3.7; it is easy to see that (1) implies that \mathbb{P}_n is asymptotically contiguous to \mathbb{Q}_n ; the other direction (i.e., \mathbb{Q}_n is asymptotically contiguous to \mathbb{P}_n) follows from a conditional second-moment argument, of which (1) is the most challenging step.

We remark that one can also prove a version of Theorem 3.8 without conditioning on Ω_n ; however, one would need to replace $\Delta_{s^2}(\pi)$ in Definition 3.6 by the larger set Δ_{s^2} . This turns out to increase Q , and therefore gives a weaker result. In other words, there is a regime in which

$$\mathbb{E}_{\mathbb{Q}_n} \left(\frac{d\mathbb{P}_n}{d\mathbb{Q}_n} \right)^2$$

tends to infinity, but only because the integrand explodes on the rare event that the labelling σ is very unbalanced.

3.2.3 Non-reconstructability

The following theorem is our main result on non-reconstructability.

Theorem 3.9. *With the notation of Theorem 3.7, if $Q(\pi, A/\sqrt{2d}) < 1$ then \mathbb{P}_n is not reconstructable.*

Existing results on non-reconstructability of the balanced two cluster model have been obtained by reducing the problem to one of non-reconstructability on trees [MNS13]. However, finding the non-reconstructable region of trees in the more general case has been a long standing open problem. Instead, we obtain Theorem 3.9 by showing a connection between distinguishability and reconstructability. Intuitively, detecting communities in G seems harder than merely distinguishing $G \sim \mathbb{P}_n$ from $G \sim \mathbb{Q}_n$; however, it is not known whether Theorem 3.7 implies Theorem 3.9. Instead, we give a reduction from Theorem 3.8: we show that the condition (1) implies non-reconstructability.

3.3 Numerical results

We present some numerical description of Theorem 3.7's uniform integrability condition in the case of two clusters with unequal sizes. In the case of two clusters, for a fixed probability vector π , the uniform integrability condition turns out to be just a threshold on $\lambda_2^2 d$. To see this, we first note that the matrix A is rank-1 and hence, so is $A^{\otimes 2}$. Moreover, fixing π also fixes the eigenvector of A , and so it fixes the numerator of Q up to a scaling. On the other hand, for a fixed π , the denominator of Q is a function only of α . So, we see that:

$$Q(\pi, A/\sqrt{2d}) = c(\pi) \lambda_2^2 d \sup_{\alpha \in \Delta_{s^2}(\pi)} \frac{|(\pi^{\otimes 2} - \alpha)^\top a^{\otimes 2}|^2}{2D(\alpha, \pi^{\otimes 2})},$$

where a is the unit-eigenvector of A . Figure 1 shows how the threshold on $\lambda_2^2 d$ varies with π .

3.4 An example showing looseness

Figure 1 shows that as the clusters become very unbalanced (i.e., $p \rightarrow 0$), Theorem 3.9 only guarantees non-reconstructability when $d\lambda_2^2$ is very small. One might ask whether the true reconstructability threshold has this behavior. Proposition 3.3 shows that it does for some models. We now present another family of examples for which the behavior of the threshold is quite different:

Proposition 3.10. *Consider the block model given by*

$$M = d \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{1}{1-p} \end{pmatrix}.$$

If $d < 1$ then the above model is not reconstructable.

Note that the above block model has $\lambda_2 = 1$. Hence Proposition 3.10 shows that there exist arbitrarily unbalanced models, where we can not reconstruct for $d\lambda_2^2 < 1$.

The main idea behind Proposition 3.10 is that for $d < 1$, the largest component is of size $O(\log n)$. Even if we can reconstruct the labels of nodes in the same cluster very well, we can not predict the labels of nodes in different clusters better than random guessing. We use a lemma from Mossel et al. [MNS13] that captures this intuition.

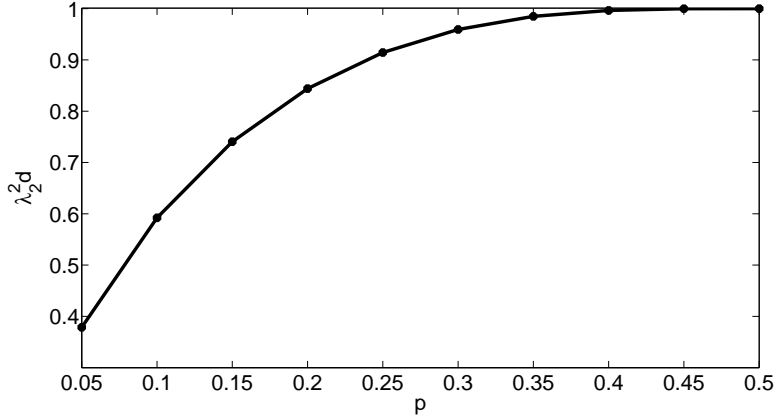


Figure 1: This plot shows how the threshold on $\lambda_2^2 d$ from the uniform integrability condition varies with the probability vector π in the two cluster case. The x-axis shows p where $\pi = [p, 1 - p]$ and the y-axis shows the value of the threshold computed using numerical optimization. The plot shows that our bound is tight as the clusters become balanced (where the threshold is close to 1). However, the threshold decreases as the clusters get more unbalanced.

4 Reconstruction below the Kesten-Stigum bound

In this section, we prove Proposition 3.3. We consider a 2-cluster model with

$$M := d \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \quad \pi := [p \ 1 - p]^\top,$$

with $pa + (1 - p)b = pb + (1 - p)c = 1$. The second eigenvalue of T turns out to be

$$\lambda_2 = \frac{(a - 1)p}{1 - p}.$$

Our first lemma shows that if two assignments have very small overlap, then they are almost uncorrelated.

Lemma 4.1. *Suppose σ and τ are $(pn, (1 - p)n)$ and $(qn, (1 - q)n)$ partitions respectively. Define*

$$p_1 := \frac{|\{u | \sigma_u = \tau_u = 1\}|}{qn}.$$

If $\text{overlap}(\sigma, \tau) < 2q\epsilon$ then $|p_1 - p| < \epsilon$.

Proof. We prove by contradiction. Suppose $p_1 \geq p + \epsilon$. Let $p_2 := \frac{|\{u | \sigma_u = 1, \tau_u = 2\}|}{(1 - q)n}$. Since $p_1 q + p_2(1 - q) = p$,

we get $p_2 = \frac{p-p_1q}{1-q}$. We have

$$\begin{aligned}
\text{overlap}(\sigma, \tau) &= \frac{1}{n} \max_{\rho} \sum_{i=1}^2 \left(N_{i\rho(i)}(\sigma, \tau) - \frac{1}{n} N_i(\sigma) N_{\rho(i)}(\tau) \right) \\
&\geq \frac{1}{n} \sum_{i=1}^2 \left(N_{ii}(\sigma, \tau) - \frac{1}{n} N_i(\sigma) N_i(\tau) \right) \\
&= (p_1q - pq) + ((1-p_2)(1-q) - (1-p)(1-q)) \\
&= 2q(p_1 - p) \geq 2q\epsilon.
\end{aligned}$$

This is a contradiction. Similarly, we can show that $p_1 \geq p - \epsilon$. \square

We are now ready to prove Proposition 3.3. Its proof is a simple application of Bernstein's inequality.

Proof of Proposition 3.3. The reconstruction algorithm is an exhaustive search over all $(pn, (1-p)n)$ partitions. For each such partition, it looks at the number of edges within the pn block. If the number of edges is in $\left[\left(\frac{dap^2}{2} - \delta\right)n, \left(\frac{dap^2}{2} + \delta\right)n\right]$, then it outputs (one such) partition. It is easy to show that the true partition will satisfy the above property with high probability and so, there is at least one partition that the algorithm can output. The rest of the proof is to show that any partition which has low enough overlap with the true partition does not satisfy the above property.

Let σ be the true partition. Let τ be a $(pn, (1-p)n)$ partition such that $\text{overlap}(\sigma, \tau) < \delta$. Let $S_1 := \{u | \tau_u = 1\}$, and $p_1 := \frac{|\{u | \sigma_u = \tau_u = 1\}|}{pn}$. From Lemma 4.1, we see that $|p_1 - p| < O(\delta)$. Consider the random variable

$$E_1 := \sum_{\substack{u, v \in S_1 \\ u < v}} X_{uv} = \# \text{ edges within } S_1 - \left(\frac{dp^2}{2} + O(\delta)\right)n,$$

where $X_{uv} = \mathbb{1}_{\{uv \in G\}} - \frac{dM_{\sigma_u \sigma_v}}{n}$. We see that

- $\mathbb{E}(X_{uv}) = 0$,
- $\text{Var}(E_1) = \left(\frac{dp^2}{2} + O(\delta)\right)n$, and
- $X_{uv} < 1$ a.s.

Using Bernstein's inequality, we have:

$$\begin{aligned}
\mathbb{P}_n \left[|E_1| > \left(\frac{d|a-1|p^2}{2} + O(\delta)\right)n \middle| \sigma \right] &< \exp \left(\frac{-\frac{1}{2} \left(\frac{d|a-1|p^2}{2} + O(\delta)\right)^2 n^2}{\left(\frac{dp^2}{2} + O(\delta)\right)n + \frac{1}{3} \left(\frac{d|a-1|p^2}{2} + O(\delta)\right)n} \right) \\
&\leq \exp \left(\frac{-3}{4} \left(\frac{d(a-1)^2 p^2}{a+3} + O(\delta) \right) n \right) \\
&= \exp \left(\frac{-3}{4} \left(\frac{d\lambda_2^2(1-p)^2}{a+3} + O(\delta) \right) n \right)
\end{aligned}$$

So with high probability, τ will not be output by the algorithm. Since each such τ is a $(pn, (1-p)n)$ partition, the total number of such τ is at most $\exp((H(p) + o(1))n)$, where $H(\cdot)$ is the entropy function, $H(p) := p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$. If

$$\frac{3d\lambda_2^2(1-p)^2}{4(a+3)} > H(p),$$

then taking a small enough δ and union bound gives us the result. In other words, all we need is

$$\lambda_2^2 d > \frac{4(a+3)H(p)}{3(1-p)^2}.$$

The right hand side can be made as small as we wish by choosing, say $a = 2$ and p small enough. \square

5 Non-distinguishability

In this section, we will assume Theorem 3.8 and use it to prove Theorem 3.7. Our main tool is the conditional second moment method, which was originally developed by Robinson and Wormald [RW92] in their study of Hamiltonian cycles in d -regular graphs. Janson [Jan95] was the first to apply this method for proving contiguity. We use a formulation from [Wor99, Theorem 4.1]:

Theorem 5.1. *Consider two sequences $\mathbb{P}_n, \mathbb{Q}_n$ of probability distributions. Suppose that there exist random variables $\{X_{k,n} : k \geq 3\}$ such that for every k ,*

$$X_{k,n} \xrightarrow{d} \text{Pois}(\mu_k) \text{ under } \mathbb{Q}_n, \text{ as } n \rightarrow \infty; \text{ and} \quad (2)$$

$$X_{k,n} \xrightarrow{d} \text{Pois}(\mu_k(1 + \delta_k)) \text{ under } \mathbb{P}_n, \text{ as } n \rightarrow \infty. \quad (3)$$

Suppose also that for any k^ , the collection $X_{3,n}, \dots, X_{k^*,n}$ are asymptotically independent as $n \rightarrow \infty$, under both \mathbb{P}_n and \mathbb{Q}_n . If*

$$\mathbb{E}_{\mathbb{Q}_n} \left(\frac{d\mathbb{P}_n}{d\mathbb{Q}_n} \right)^2 \leq (1 + o(1)) \exp \left(\sum_{k \geq 3} \mu_k \delta_k^2 \right) < \infty \quad (4)$$

then \mathbb{P}_n and \mathbb{Q}_n are mutually contiguous.

We will apply Theorem 5.1 with \mathbb{P}_n replaced by $\hat{\mathbb{P}}_n = (\mathbb{P}_n \mid \Omega_n)$; i.e., the block model conditioned on having almost the expected label frequencies.

We note that (2), (3), and the asymptotic independence property are already verified by Proposition 3.1, with $\mu_k = \frac{1}{2k} d^k$ and $\delta_k = \text{tr}(T^k) - 1$. Recalling that $1 = \lambda_1 \geq \dots \geq \lambda_s$ are the eigenvalues of T , we have $\delta_k = \sum_{i \geq 2} \lambda_i^k$. Hence,

$$\begin{aligned} \sum_{k=3}^{\infty} \mu_k \delta_k^2 &= \frac{1}{2} \sum_{k=3}^{\infty} \frac{d^k}{k} \sum_{i,j=2}^s \lambda_i^k \lambda_j^k \\ &= \frac{1}{2} \sum_{i,j=2}^s \sum_{k=3}^{\infty} \frac{(d\lambda_i \lambda_j)^k}{k} \\ &= \sum_{i,j=2}^s \log \psi(d\lambda_i \lambda_j), \end{aligned}$$

where $\psi(x) = (1-x)^{-1/2}e^{-x/2-x^2/4}$. In particular, condition (4) follows immediately from Theorem 3.8, which in turn proves that $\tilde{\mathbb{P}}_n$ and \mathbb{Q}_n are mutually contiguous. Since $\mathbb{P}_n(\Omega_n) \rightarrow 1$, \mathbb{P}_n and $\tilde{\mathbb{P}}_n$ are mutually contiguous, and Theorem 3.7 follows.

6 Second moment

In this section, we will prove our main result calculating the second moment under the uniform integrability condition (Theorem 3.8). Our first lemma expresses the second moment in terms of (centered and normalized) multinomial random variables. In order to state the lemma, we make the following notation. Given two assignments $\sigma, \tau \in [s]^n$, let $N_{ij} := N_{ij}(\sigma, \tau) := |\{v : \sigma_v = i, \tau_v = j\}|$, and $X_{ij} := X_{ij}(\sigma, \tau) := n^{-1/2}(N_{ij} - n\pi_i\pi_j)$. Recall that Ω_n is the event that the label frequencies are approximately their expected values, and let Y_n denote the restricted density $\mathbb{1}_{\{\Omega_n\}} \frac{d\mathbb{P}_n}{d\mathbb{Q}_n}$. With a slight overloading of notation, we write $\sigma \in \Omega_n$ if for all $i \in [s]$, $|\{u : \sigma_u = i\}| = n\pi_i \pm a_n$. Recall that $A := M - d\mathbf{1}\mathbf{1}^\top$.

Lemma 6.1. *We have:*

$$\mathbb{E}_{\mathbb{Q}_n} Y_n^2 = (1 + O(n^{-1})) \sum_{\sigma, \tau \in \Omega_n} \mathbb{P}_n(\sigma) \mathbb{P}_n(\tau) \exp \left(\frac{1}{2d} \sum_{ijkl} X_{ij} X_{kl} A_{ik} A_{jl} + \nu_1 + \nu_2 + \xi_n \right),$$

where

$$\begin{aligned} \nu_1 &= -\frac{1}{2d} \sum_{ij} A_{ii} A_{jj} \pi_i \pi_j, \\ \nu_2 &= -\frac{1}{2d^2} \sum_{ijkl} A_{ik}^2 A_{jl}^2 \pi_i \pi_j \pi_k \pi_\ell, \text{ and} \\ \xi_n &= O(n^{-1/2}) \sum_{ij} |X_{ij}| + O(n^{-1}) \left(\sum_{ij} |X_{ij}| \right)^2. \end{aligned}$$

Proof. Define

$$W_{uv}(G, \sigma) = \begin{cases} \frac{M_{\sigma_u, \sigma_v}}{d} & \text{if } (u, v) \in E(G) \\ \frac{1 - \frac{M_{\sigma_u, \sigma_v}}{d}}{1 - \frac{d}{n}} & \text{if } (u, v) \notin E(G). \end{cases}$$

Then we may write out

$$\begin{aligned} Y_n &= \sum_{\sigma \in \Omega_n} \frac{\mathbb{P}_n(G, \sigma)}{\mathbb{Q}_n(G)} \\ &= \sum_{\sigma \in \Omega_n} \mathbb{P}_n(\sigma) \prod_{u,v} W_{uv}(G, \sigma). \end{aligned}$$

Squaring both sides and taking expectations,

$$\begin{aligned} \mathbb{E}_{\mathbb{Q}_n} Y_n^2 &= \mathbb{E}_{\mathbb{Q}_n} \sum_{\sigma, \tau \in \Omega_n} \mathbb{P}_n(\sigma) \mathbb{P}_n(\tau) \prod_{u,v} W_{uv}(G, \sigma) W_{uv}(G, \tau) \\ &= \sum_{\sigma, \tau \in \Omega_n} \mathbb{P}_n(\sigma) \mathbb{P}_n(\tau) \prod_{u,v} \mathbb{E}_{\mathbb{Q}_n} [W_{uv}(G, \sigma) W_{uv}(G, \tau)], \end{aligned} \tag{5}$$

where the last equality holds because under \mathbb{Q}_n , and for any fixed σ , the variables $W_{uv}(G, \sigma)$ are independent as u and v vary.

Let us compute the inner expectation in (5). Recall that under \mathbb{Q}_n , $(u, v) \in E(G)$ with probability $\frac{d}{n}$. Writing (for brevity) s for $M_{\sigma_u \sigma_v}$ and t for $M_{\tau_u \tau_v}$, we have

$$\begin{aligned} \mathbb{E}_{\mathbb{Q}_n} W_{uv}(G, \sigma) W_{uv}(G, \tau) &= \frac{st}{d^2} \cdot \frac{d}{n} + \frac{(1 - \frac{s}{n})(1 - \frac{t}{n})}{(1 - \frac{d}{n})^2} (1 - \frac{d}{n}) \\ &= \frac{st}{nd} + \left(1 - \frac{s}{n}\right) \left(1 - \frac{t}{n}\right) \left(1 + \frac{d}{n} + \frac{d^2}{n^2} + O(n^{-3})\right) \\ &= 1 + \frac{(s-d)(t-d)}{nd} + \frac{(s-d)(t-d)}{n^2} + O(n^{-3}) \end{aligned}$$

Setting $q = (s-d)(t-d)$, and using the fact that $1 + x = \exp(x - x^2/2 + O(x^3))$, we have

$$\mathbb{E}_{\mathbb{Q}_n} W_{uv}(G, \sigma) W_{uv}(G, \tau) = \exp\left(\frac{q}{dn} + \frac{q}{n^2} - \frac{q^2}{2d^2n^2} + O(n^{-3})\right).$$

Now, if $(\sigma_u, \tau_u, \sigma_v, \tau_v) = (i, j, k, \ell)$ then $(s-d)(t-d) = (M_{ik} - d)(M_{j\ell} - d) = A_{ik}A_{j\ell}$. Hence,

$$\mathbb{E}_{\mathbb{Q}_n} W_{uv}(G, \sigma) W_{uv}(G, \tau) = \exp\left(\frac{A_{ik}A_{j\ell}}{dn} + \frac{A_{ik}A_{j\ell}}{n^2} - \frac{(A_{ik}A_{j\ell})^2}{2d^2n^2} + O(n^{-3})\right). \quad (6)$$

Let $N_{ijkl} = |\{\{u, v\} : \sigma_u = i, \tau_u = j, \sigma_v = k, \tau_v = \ell\}|$. Plugging (6) into (5), we have

$$\mathbb{E}_{\mathbb{Q}_n} Y_n^2 = (1 + O(n^{-1})) \sum_{\sigma, \tau \in \Omega_n} \mathbb{P}_n(\sigma) \mathbb{P}_n(\tau) \exp\left(\sum_{ijkl=1}^s N_{ijkl} \left(\frac{A_{ik}A_{j\ell}}{dn} + \frac{A_{ik}A_{j\ell}}{n^2} - \frac{(A_{ik}A_{j\ell})^2}{2d^2n^2}\right)\right) \quad (7)$$

where the $(1 + O(n^{-1}))$ term arises because $\sum_{ijkl} N_{ijkl} \leq n^2$. Applying Lemma 6.2 (below) now finishes the proof. \square

The last step in the proof of Lemma 6.1 requires us to replace N_{ijkl} by its normalized version, X_{ij} , and then rearrange the sums in (7). We will do this step in slightly more generality, where we allow N_{ijkl} to be defined on a subset of the vertices. For the purposes of this section it suffices to consider $S = [n]$, but the general form will be useful when we consider non-reconstruction.

Lemma 6.2. *Let $S \subseteq [n]$ such that $|S| = n - o(n)$. Further, let*

$$\begin{aligned} N_{ijkl} &:= N_{ijkl}(\sigma, \tau) := |\{\{u, v\} : u, v \in S, \sigma_u = i, \tau_u = j, \sigma_v = k, \tau_v = \ell\}|, \\ N_{ij} &:= N_{ij}(\sigma, \tau) := |\{u : u \in S, \sigma_u = i, \tau_u = j\}| \text{ and,} \\ X_{ij} &:= X_{ij}(\sigma, \tau) := n^{-1/2} (N_{ij} - n\pi_i\pi_j) \\ t_{ijkl} &:= \frac{A_{ik}A_{j\ell}}{dn} + \frac{A_{ik}A_{j\ell}}{n^2} - \frac{(A_{ik}A_{j\ell})^2}{2d^2n^2} \end{aligned}$$

Then, we have:

$$\sum_{ijkl} N_{ijkl} t_{ijkl} = \frac{1}{2d} \sum_{ijkl} X_{ij} X_{kl} A_{ik} A_{j\ell} + \nu_1 + \nu_2 + \xi_n,$$

where

$$\begin{aligned}\nu_1 &= -\frac{1}{2d} \sum_{ij} A_{ii} A_{jj} \pi_i \pi_j, \\ \nu_2 &= -\frac{1}{4d^2} \sum_{ijk\ell} A_{ik}^2 A_{j\ell}^2 \pi_i \pi_j \pi_k \pi_\ell, \text{ and} \\ \xi_n &= O(n^{-1/2}) \sum_{ij} |X_{ij}| + O(n^{-1}) \left(\sum_{ij} |X_{ij}| \right)^2 + O(n^{-1}).\end{aligned}$$

Proof. We see that $N_{ijk\ell} = \frac{1}{2} N_{ij} N_{k\ell}$ unless $i = k$ and $j = \ell$, in which case $N_{ijk\ell} = \binom{N_{ij}}{2} = \frac{1}{2} N_{ij} N_{k\ell} - \frac{1}{2} N_{ij}$. So, we have

$$\sum_{ijk\ell} N_{ijk\ell} t_{ijk\ell} = \frac{1}{2} \sum_{ijk\ell} N_{ij} N_{k\ell} t_{ijk\ell} - \frac{1}{2} \sum_{ij} N_{ij} t_{ijij} \quad (8)$$

Recall that $\sum_i \pi_i M_{ik} = d$ for any fixed k and $\sum_k \pi_k M_{ik} = d$ for any fixed i . It follows that $\sum_i \pi_i A_{ij} = \sum_j \pi_j A_{ij} = 0$. Hence,

$$\sum_i \pi_i t_{ijk\ell} = - \sum_i \pi_i \frac{(A_{ik} A_{j\ell})^2}{2d^2 n^2}.$$

Writing $N_{ij} = \sqrt{n} X_{ij} + n \pi_i \pi_j$, we have

$$\begin{aligned}\sum_{ijk\ell} N_{ij} N_{k\ell} t_{ijk\ell} &= n \sum_{ijk\ell} X_{ij} X_{k\ell} t_{ijk\ell} - \sum_{ijk\ell} \frac{(A_{ik} A_{j\ell})^2}{2d^2 n^2} (n^{3/2} X_{ij} \pi_k \pi_\ell + n^{3/2} X_{k\ell} \pi_i \pi_j + n^2 \pi_i \pi_j \pi_k \pi_\ell) \\ &= n \sum_{ijk\ell} X_{ij} X_{k\ell} t_{ijk\ell} - \sum_{ijk\ell} \frac{(A_{ik} A_{j\ell})^2}{2d^2} \pi_i \pi_j \pi_k \pi_\ell + O(n^{-1/2}) \sum_{ij} |X_{ij}|,\end{aligned}$$

Next, note that $t_{ijk\ell} = \frac{1}{dn} A_{ik} A_{j\ell} + O(n^{-2})$, and so

$$\begin{aligned}\sum_{ijk\ell} N_{ij} N_{k\ell} t_{ijk\ell} &= \frac{1}{d} \sum_{ijk\ell} X_{ij} X_{k\ell} A_{ik} A_{j\ell} - \frac{1}{2d^2} \sum_{ijk\ell} (A_{ik} A_{j\ell})^2 \pi_i \pi_j \pi_k \pi_\ell \\ &\quad + O(n^{-1/2}) \sum_{ij} |X_{ij}| + O(n^{-1}) \left(\sum_{ij} |X_{ij}| \right)^2;\end{aligned}$$

we recognize the second term as $2\nu_2$, and the last two terms as being part of ξ_n . This takes care of first term in (8); for the second term,

$$\sum_{ij} N_{ij} t_{ijij} = \sqrt{n} \sum_{ij} X_{ij} t_{ijij} + n \sum_{ij} \pi_i \pi_j t_{ijij} = O(n^{-1/2}) \sum_{ij} |X_{ij}| + \frac{1}{d} \sum_{ij} A_{ii} A_{jj} \pi_i \pi_j + O(n^{-1});$$

here, the second term is $2\nu_1$ and the others are part of ξ_n . \square

The following lemma gives a simpler form for ν_1 and ν_2 appearing above. We define $B := \frac{1}{d} \text{diag}(\pi) A = T - \pi \otimes \mathbf{1}$. In particular, this will allow us to relate ν_1 and ν_2 to the eigenvalues of T .

Lemma 6.3. *Let ν_1 and ν_2 be as in Lemma 6.2. Then, we have:*

$$\begin{aligned}\nu_1 &= -\frac{d}{2} \operatorname{tr}(B)^2 \\ \nu_2 &= -\frac{d^2}{4} \operatorname{tr}(B^2)^2.\end{aligned}$$

Proof. Note that $A_{ii}\pi_i = dB_{ii}$. Hence,

$$\nu_1 = -\frac{1}{2d} \sum_{ij} A_{ii} A_{jj} \pi_i \pi_j = -\frac{d}{2} \sum_{ij} B_{ii} B_{jj} = -\frac{d}{2} \operatorname{tr}(B)^2.$$

Similarly, since $A_{ik}\pi_i = B_{ik}$ and $A_{ik}\pi_k = A_{ki}\pi_k = B_{ki}$,

$$\nu_2 = -\frac{d^2}{4} \sum_{ijkl} B_{ik} B_{ki} B_{jl} B_{lj} = -\frac{d^2}{4} \operatorname{tr}((B^{\otimes 2})^2) = -\frac{d^2}{4} \operatorname{tr}(B^2)^2. \quad \square$$

The following lemma shows that ξ_n in Lemma 6.2 is very small in an appropriate sense.

Lemma 6.4. *Let ξ_n be as in Lemma 6.2. If $a_n = o(n^{1/2})$ then $\mathbb{E} \exp(a_n \xi_n) \rightarrow 1$.*

Proof. By the central limit theorem, each X_{ij} has a limit in distribution as $n \rightarrow \infty$; hence $a_n \xi_n \rightarrow 0$ in probability. It is therefore enough to show that the sequence $\exp(a_n \xi_n)$ is uniformly integrable, but this follows from Hoeffding's inequality. \square

We now state the following three results before we prove the main result of this section. The following proposition characterizes when the exponential of a quadratic form of a sequence of multinomial random variables is uniformly integrable. Its proof can be found in Section A.

Proposition 6.5. *Define X_{ij} as in Lemma 6.4. Then*

$$\exp\left(\frac{1}{2d} \sum X_{ij} X_{kl} A_{ik} A_{jl}\right)$$

is uniformly integrable if $Q(\pi, A/\sqrt{2d}) < 1$, and fails to be uniformly integrable if $Q(\pi, A/\sqrt{2d}) > 1$.

Using Hölder's inequality, it is fairly straightforward to introduce the ξ_n term:

Lemma 6.6. *Define X_{ij} as in Lemma 6.4. Then*

$$\exp\left(\frac{1}{2d} \sum X_{ij} X_{kl} A_{ik} A_{jl} + \xi_n\right)$$

is uniformly integrable if $Q(\pi, A/\sqrt{2d}) < 1$, and fails to be uniformly integrable if $Q(\pi, A/\sqrt{2d}) > 1$.

Proof. Supposing that $Q(\pi, A/\sqrt{2d}) < 1$, we find some $\epsilon > 0$ such that $Q(\pi, \sqrt{1+\epsilon}A/\sqrt{2d}) < 1$. Set $a_n = n^{1/3}$ and $b_n = \frac{a_n}{a_n-1}$ to be the Hölder conjugate of a_n . Setting

$$W = \operatorname{vec}(X), \quad (9)$$

Hölder's inequality and Lemma 6.4 give

$$\begin{aligned}
& \mathbb{E}_{\sigma, \tau} \exp \left(\left(1 + \frac{\epsilon}{2}\right) \left(\frac{1}{2d} \sum_{ijk\ell} X_{ij} X_{k\ell} A_{ik} A_{j\ell} + \xi_n \right) \right) \\
& \leq \left(\mathbb{E}_{\sigma, \tau} \exp \left(\frac{(1 + \frac{\epsilon}{2})b_n}{2d} W^T (A^{\otimes 2}) W \right) \right)^{1/b_n} \left(\mathbb{E} \exp((1 + \frac{\epsilon}{2})a_n \xi_n) \right)^{1/a_n} \\
& \leq \left(\mathbb{E}_{\sigma, \tau} \exp \left(\frac{(1 + \frac{\epsilon}{2})b_n}{2d} W^T (A^{\otimes 2}) W \right) \right)^{1/b_n}.
\end{aligned}$$

To check uniform integrability, we apply Proposition 6.5. For sufficiently large n , we have $b_n \leq \frac{1+\epsilon}{1+\frac{\epsilon}{2}}$ and

$$\exp \left(\frac{(1 + \frac{\epsilon}{2})b_n}{2d} W^T A^{\otimes 2} W \right) \leq \max \left\{ 1, \exp \left(\frac{(1 + \epsilon)}{2d} W^T A^{\otimes 2} W \right) \right\}.$$

We see from the fact that $Q(\pi, \sqrt{1 + \epsilon}A/\sqrt{2d}) < 1$ and Proposition 6.5 that the right hand side above has a finite expectation.

To summarize, we have shown that if $Z = \exp(\frac{1}{2d} \sum X_{ij} X_{k\ell} A_{ik} A_{j\ell} + \xi_n)$ then $\mathbb{E} Z^{(1+\epsilon/2)} < \infty$ for some $\epsilon > 0$. It follows that Z is uniformly integrable, as claimed.

To show that $Q(\pi, A/\sqrt{2d}) > 1$ implies non-uniform integrability, requires an almost identical argument, but using the reverse Hölder inequality instead of the usual Hölder inequality. We omit the details. \square

The following lemma calculates the expected value of the exponential of a quadratic form of a Gaussian random vector.

Lemma 6.7. *Take $Z \sim \mathcal{N}(0, \Sigma)$, where $\Sigma = \text{diag}(\pi)^{\otimes 2} - \pi^{\otimes 4}$. Recall that λ_i denote the eigenvalues of T , with $1 = \lambda_1 \geq |\lambda_2| \geq \dots \geq |\lambda_s|$. If $d\lambda_2^2 < 1$ then*

$$\mathbb{E} \exp \left(\frac{1}{2d} Z^T A^{\otimes 2} Z \right) = \prod_{i,j=2}^s \frac{1}{\sqrt{1 - d\lambda_i \lambda_j}}.$$

Otherwise, $\mathbb{E} \exp \left(\frac{1}{2d} Z^T A^{\otimes 2} Z \right) = \infty$.

Proof. A standard computation (see, e.g. [MP92]) shows that if μ_1, \dots, μ_k denote the eigenvalues of $\Sigma \tilde{A}$ then $\mathbb{E} \exp(Z^T \tilde{A} Z/2) = \prod_i \frac{1}{\sqrt{1 - \mu_i}}$. Now,

$$\Sigma A^{\otimes 2} = (\text{diag}(\pi)^{\otimes 2} - \pi^{\otimes 4}) A^{\otimes 2} = (\text{diag}(\pi) A)^{\otimes 2} - (\pi \pi^T A)^{\otimes 2}.$$

Recall, however, that $A\pi = 0$. Hence, we are interested in the eigenvalues of $(\text{diag}(\pi) A)^{\otimes 2} = (dB)^{\otimes 2}$. Since the top eigenvalue of T is 1 (with 1 as its right-eigenvector and π as its left-eigenvector), we see that if $\lambda_1, \dots, \lambda_s$ are the eigenvalues of T with $\lambda_1 = 1$, then

$$\{d\lambda_i \lambda_j : i, j = 2, \dots, s\}$$

are the eigenvalues of $\frac{1}{d} \Sigma(A \otimes A)$. \square

Proof of Theorem 3.8. First of all, note that

$$\frac{d\tilde{\mathbb{P}}_n(G, \sigma)}{d\mathbb{Q}_n} = \frac{Y_n}{\mathbb{P}_n(\Omega_n)} = (1 + o(1))Y_n.$$

Hence, it suffices to compute the limit of $\mathbb{E}_{\mathbb{Q}_n} Y_n^2$.

From Lemma 6.1, we see that we need to calculate the limit of the quantity

$$\mathbb{E}_{\sigma, \tau \in \Omega_n} \exp \left(\frac{1}{2d} \sum_{ijk\ell} X_{ij} X_{k\ell} A_{ik} A_{j\ell} + \xi_n \right).$$

Lemma 6.6 establishes that the above sequence is uniformly integrable.

Now, note that $(N_{ij})_{i,j=1}^s$ is distributed as a multinomial random vector with n trials and probabilities $\pi_i \pi_j$. In particular, $\mathbb{E} N_{ij} = \pi_i \pi_j$, $\text{Var}(N_{ij}) = \pi_i \pi_j - (\pi_i \pi_j)^2$, and $\text{Cov}(N_{ij} N_{k\ell}) = -\pi_i \pi_j \pi_k \pi_\ell$ if $\{i, j\} \neq \{k, \ell\}$. Since $X_{ij} = n^{-\frac{1}{2}} (N_{ij} - n \pi_i \pi_j)$, central limit theorem implies that W converges in distribution to a Gaussian random vector, Z with mean 0 and covariance matrix $\text{diag}(\pi)^{\otimes 2} - \pi^{\otimes 4}$. Using Lemma 6.7 shows us that

$$\mathbb{E}_{\mathbb{Q}_n} Y_n^2 \rightarrow \exp(\nu_1 + \nu_2) \prod_{i,j=2}^s \frac{1}{\sqrt{1 - d\lambda_i \lambda_j}}. \quad (10)$$

Going back to Lemma 6.3, we have

$$\nu_1 = -\frac{d}{2} \text{tr}(B)^2 = -\frac{1}{2} \sum_{i,j=2}^s d\lambda_i \lambda_j$$

and

$$\nu_2 = -\frac{d^2}{4} \text{tr}(B^2)^2 = -\frac{1}{4} \sum_{i,j=2}^s (d\lambda_i \lambda_j)^2.$$

Hence, the right hand side of (10) is equal to

$$\prod_{i,j} \psi(d\lambda_i \lambda_j),$$

as claimed. □

7 Non-reconstructability

In this section, we prove Theorem 3.9. The following proposition is the main technical result that we use to prove Theorem 3.9. It shows that under the uniform integrability condition, for any two fixed configurations on a finite set of nodes, the total variation distance between the distribution on graphs conditioned on these two configurations respectively goes to zero.

Proposition 7.1. *Suppose $Q(\pi, A/\sqrt{2d}) < 1$. Then, for any fixed $r > 0$, and for any two configurations (a_1, a_2, \dots, a_r) and (b_1, b_2, \dots, b_r) , we have:*

$$TV(\mathbb{P}_n(G|\sigma_u = a_u \text{ for } u \in [r]), \mathbb{P}_n(G|\sigma_u = b_u \text{ for } u \in [r])) = o(1),$$

where $TV(\mathbb{P}_1, \mathbb{P}_2)$ denotes the total variation distance between the two distributions \mathbb{P}_1 and \mathbb{P}_2 .

Proof. We will first prove the statement of the proposition with \mathbb{P}_n replaced by $\hat{\mathbb{P}}_n = (\mathbb{P}_n \mid \Omega_n)$; i.e., the block model conditioned on having almost the expected label frequencies.

We start by using the definition of total variation distance:

$$\begin{aligned}
& TV(\hat{\mathbb{P}}_n(G|\sigma_u = a_u \text{ for } u \in [r]), \hat{\mathbb{P}}_n(G|\sigma_u = b_u \text{ for } u \in [r])) \\
&= \sum_G |\hat{\mathbb{P}}_n(G|\sigma_u = a_u \text{ for } u \in [r]) - \hat{\mathbb{P}}_n(G|\sigma_u = b_u \text{ for } u \in [r])| \\
&= \sum_G |\hat{\mathbb{P}}_n(G|\sigma_u = a_u \text{ for } u \in [r]) - \hat{\mathbb{P}}_n(G|\sigma_u = b_u \text{ for } u \in [r])| \frac{\sqrt{\mathbb{Q}_n(G)}}{\sqrt{\mathbb{Q}_n(G)}} \\
&\stackrel{(a)}{\leq} \left(\sum_G \mathbb{Q}_n(G) \right)^{1/2} \left(\sum_G \frac{(\hat{\mathbb{P}}_n(G|\sigma_u = a_u \text{ for } u \in [r]) - \hat{\mathbb{P}}_n(G|\sigma_u = b_u \text{ for } u \in [r]))^2}{\mathbb{Q}_n(G)} \right)^{1/2} \\
&= \left(\sum_G \frac{(\sum_{\tilde{\sigma}} \hat{\mathbb{P}}_n(\tilde{\sigma}) (\hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) - \hat{\mathbb{P}}_n(G|b, \tilde{\sigma})))^2}{\mathbb{Q}_n(G)} \right)^{1/2},
\end{aligned}$$

where (a) follows from Cauchy-Schwartz inequality and $\tilde{\sigma}$ denotes an assignment on $[n] \setminus [r]$. We can expand the numerator as follows:

$$\begin{aligned}
& \left(\sum_{\tilde{\sigma}} \hat{\mathbb{P}}_n(\tilde{\sigma}) (\hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) - \hat{\mathbb{P}}_n(G|b, \tilde{\sigma})) \right)^2 \\
&= \sum_{\tilde{\sigma}, \tilde{\tau}} \hat{\mathbb{P}}_n(\tilde{\sigma}) \hat{\mathbb{P}}_n(\tilde{\tau}) (\hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|a, \tilde{\tau}) + \hat{\mathbb{P}}_n(G|b, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|b, \tilde{\tau}) \\
&\quad - \hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|b, \tilde{\tau}) - \hat{\mathbb{P}}_n(G|b, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|a, \tilde{\tau})).
\end{aligned}$$

We will now show that the value of

$$\sum_{\tilde{\sigma}, \tilde{\tau}} \hat{\mathbb{P}}_n(\tilde{\sigma}) \hat{\mathbb{P}}_n(\tilde{\tau}) \sum_G \frac{\hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|b, \tilde{\tau})}{\mathbb{Q}_n(G)},$$

is independent of a and b (upto $o(1)$). This will prove our claim. Define

$$W_{uv}(G, \sigma) := \begin{cases} \frac{M_{\sigma_u, \sigma_v}}{\frac{d}{n}} & \text{if } (u, v) \in E(G), \\ \frac{1 - \frac{M_{\sigma_u, \sigma_v}}{n}}{1 - \frac{d}{n}} & \text{if } (u, v) \notin E(G), \end{cases}$$

and let $q_{ijk\ell} = (M_{ik} - d)(M_{j\ell} - d)/n = A_{ik}A_{j\ell}/n$, and $t_{ijk\ell} = \frac{q_{ijk\ell}}{d} + \frac{q_{ijk\ell}}{n} - \frac{q_{ijk\ell}^2}{2d^2}$. We have:

$$\begin{aligned}
& \sum_{\tilde{\sigma}, \tilde{\tau}} \hat{\mathbb{P}}_n(\tilde{\sigma}) \hat{\mathbb{P}}_n(\tilde{\tau}) \sum_G \frac{\hat{\mathbb{P}}_n(G|a, \tilde{\sigma}) \hat{\mathbb{P}}_n(G|b, \tilde{\tau})}{\mathbb{Q}_n(G)} \\
&= \sum_{\tilde{\sigma}, \tilde{\tau}} \hat{\mathbb{P}}_n(\tilde{\sigma}) \hat{\mathbb{P}}_n(\tilde{\tau}) \prod_{u, v \in [n]} \mathbb{E}_{\mathbb{Q}_n}[W_{uv}(G, a, \tilde{\sigma}) W_{uv}(G, b, \tilde{\tau})] \\
&= \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \prod_{u, v \in [n] \setminus [r]} \left(1 + t_{\tilde{\sigma}_u \tilde{\tau}_u \tilde{\sigma}_v \tilde{\tau}_v} + O\left(\frac{1}{n^3}\right)\right) \prod_{\substack{u \in [r] \\ v \in [n] \setminus [r]}} \left(1 + t_{a_u b_u \tilde{\sigma}_v \tilde{\tau}_v} + O\left(\frac{1}{n^3}\right)\right) \prod_{u, v \in [r]} \left(1 + t_{a_u b_u a_v b_v} + O\left(\frac{1}{n^3}\right)\right) \\
&= \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \prod_{i, j, k, \ell \in [s]} \left(1 + t_{ijk\ell} + O\left(\frac{1}{n^3}\right)\right)^{\tilde{N}_{ijk\ell}} \prod_{\substack{u \in [r] \\ i, j \in [s]}} \left(1 + t_{a_u b_u ij} + O\left(\frac{1}{n^3}\right)\right)^{\tilde{N}_{ij}} \prod_{u, v \in [r]} \left(1 + t_{a_u b_u a_v b_v} + O\left(\frac{1}{n^3}\right)\right),
\end{aligned} \tag{11}$$

where $\tilde{N}_{ijk\ell} = |\{\{u, v\} : \tilde{\sigma}_u = i, \tilde{\tau}_u = j, \tilde{\sigma}_v = k, \tilde{\tau}_v = \ell\}|$, and $\tilde{N}_{ij} = |\{v : \tilde{\sigma}_v = i, \tilde{\tau}_v = j\}|$. We first note that the last term in (11) can be simplified as follows:

$$\prod_{u, v \in [r]} \left(1 + t_{a_u b_u a_v b_v} + O\left(\frac{1}{n^3}\right)\right) = \prod_{u, v \in [r]} \left(1 + O\left(\frac{1}{n}\right)\right) = \left(1 + O\left(\frac{1}{n}\right)\right)^{r^2} = 1 + O\left(\frac{1}{n}\right).$$

For the second term in (11), we have:

$$\begin{aligned}
\prod_{i, j \in [s]} \left(1 + t_{a_u b_u ij} + O\left(\frac{1}{n^3}\right)\right)^{\tilde{N}_{ij}} &= \prod_{i, j \in [s]} \left(1 + \frac{q_{a_u b_u ij}}{d} + O\left(\frac{1}{n^2}\right)\right)^{\tilde{N}_{ij}} \\
&\stackrel{(\zeta_1)}{=} \prod_{i, j \in [s]} \exp\left(\tilde{N}_{ij} \left(\frac{q_{a_u b_u ij}}{d} + O\left(\frac{1}{n^2}\right)\right)\right) \\
&\stackrel{(\zeta_2)}{=} (1 + o(1)) \prod_{i, j \in [s]} \exp\left(\frac{q_{a_u b_u ij}}{d} \cdot \tilde{N}_{ij}\right) \\
&= (1 + o(1)) \prod_{i, j \in [s]} \exp\left(\frac{n q_{a_u b_u ij}}{d} \cdot \left(\frac{\tilde{N}_{ij}}{n} - \pi_i \pi_j\right)\right) \cdot \exp\left(\frac{n q_{a_u b_u ij}}{d} \cdot \pi_i \pi_j\right),
\end{aligned} \tag{12}$$

where (ζ_1) follows from the fact that $1 + x = \exp(x + O(x^2))$ and (ζ_2) follows from the fact that $\tilde{N}_{ij} < n$. We first note that:

$$\begin{aligned}
\prod_{i, j \in [s]} \exp\left(\frac{n q_{a_u b_u ij}}{d} \cdot \pi_i \pi_j\right) &= \prod_{i, j \in [s]} \exp\left(\frac{\pi_i \pi_j A_{a_u i} A_{b_u j}}{d}\right) \\
&= \exp\left(\sum_{i, j \in [s]} \frac{\pi_i \pi_j A_{a_u i} A_{b_u j}}{d}\right) \\
&= \exp\left(\frac{(\sum_{i \in [s]} \pi_i A_{a_u i}) (\sum_{j \in [s]} \pi_j A_{b_u j})}{d}\right) = 1.
\end{aligned}$$

Looking now at the first two terms of (11) we obtain (using (12)):

$$\begin{aligned}
& \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \prod_{i,j,k,\ell \in [s]} \left(1 + t_{ijkl} + O\left(\frac{1}{n^3}\right) \right)^{\tilde{N}_{ijkl}} \prod_{\substack{u \in [r] \\ i,j \in [s]}} \exp\left(\frac{nq_{a_u b_u ij}}{d} \cdot \left(\frac{\tilde{N}_{ij}}{n} - \pi_i \pi_j \right) \right) \\
& \stackrel{(\zeta_1)}{=} (1 + o(1)) \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \exp\left(\sum_{ijkl} \tilde{N}_{ijkl} t_{ijkl} \right) \prod_{\substack{u \in [r] \\ i,j \in [s]}} \exp\left(\frac{nq_{a_u b_u ij}}{d} \cdot \frac{\tilde{X}_{ij}}{\sqrt{n}} \right) \\
& \stackrel{(\zeta_2)}{=} (1 + o(1)) \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \exp\left(\frac{1}{2d} \sum_{ijkl} \tilde{X}_{ij} \tilde{X}_{kl} A_{ik} A_{jl} + \nu_1 + \nu_2 + \tilde{\xi}_n \right) \prod_{\substack{u \in [r] \\ i,j \in [s]}} \exp\left(\frac{nq_{a_u b_u ij}}{d} \cdot \frac{\tilde{X}_{ij}}{\sqrt{n}} \right) \\
& = (1 + o(1)) \exp(\nu_1 + \nu_2) \hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \exp\left(\frac{1}{2d} \sum_{ijkl} \tilde{X}_{ij} \tilde{X}_{kl} A_{ik} A_{jl} + \tilde{\xi}_n \right) \prod_{\substack{u \in [r] \\ i,j \in [s]}} \exp\left(\frac{nq_{a_u b_u ij}}{d} \cdot \frac{\tilde{X}_{ij}}{\sqrt{n}} \right)
\end{aligned}$$

where $\tilde{X}_{ij} := n^{-1/2} (\tilde{N}_{ij} - n\pi_i \pi_j)$, (ζ_1) follows from the fact that $1 + x = \exp(x + O(x^2))$ and since $\tilde{N}_{ijkl} < n^2$, (ζ_2) follows from Lemma 6.2. Note that $\exp\left(\frac{1}{2d} \sum_{ijkl} \tilde{X}_{ij} \tilde{X}_{kl} A_{ik} A_{jl} + \tilde{\xi}_n\right)$ is independent of a and b and from Lemma 6.6, we also know that it is uniformly integrable. On the other hand, since $|\tilde{X}_{ij}| \leq \sqrt{n}$, we see that $\exp\left(\sum_{u \in [r], i,j \in [s]} \frac{nq_{a_u b_u ij}}{d} \cdot \frac{\tilde{X}_{ij}}{\sqrt{n}}\right)$ is uniformly bounded and hence is uniformly integrable. Moreover, $\tilde{X}_{ij} \rightarrow \mathcal{N}(0, \pi_i \pi_j - (\pi_i \pi_j)^2)$. So we see that,

$$\hat{\mathbb{E}}_{\tilde{\sigma}, \tilde{\tau}} \exp\left(\frac{1}{2d} \sum_{ijkl} \tilde{X}_{ij} \tilde{X}_{kl} A_{ik} A_{jl} + \tilde{\xi}_n \right) \cdot \prod_{\substack{u \in [r] \\ i,j \in [s]}} \exp\left(\frac{nq_{a_u b_u ij}}{d} \cdot \frac{\tilde{X}_{ij}}{\sqrt{n}} \right)$$

converges to a finite quantity that is independent of a and b . This proves the statement of the proposition with \mathbb{P}_n replaced by $\hat{\mathbb{P}}_n = (\mathbb{P}_n | \Omega_n)$. Noting that

$$TV(\mathbb{P}_n(G|\sigma_u = a_u \text{ for } u \in [r]), \hat{\mathbb{P}}_n(G|\sigma_u = a_u \text{ for } u \in [r])) = o(1), \quad \forall a$$

gives us the desired result. \square

In order to prove Theorem 3.9, we use the following lemma which is an easy consequence of Proposition 7.1.

Lemma 7.2. *Suppose $Q(\pi, A/\sqrt{2d}) < 1$. Then, for any set S such that $|S|$ is a constant, $u \notin S$, we have:*

$$\mathbb{E}(TV(\mathbb{P}_n(\sigma_u | G, \sigma_S), \pi) | \sigma_S) = o(1).$$

Proof.

$$\begin{aligned}
\mathbb{E}(TV(\mathbb{P}_n(\sigma_u | G, \sigma_S), \pi) | \sigma_S) &= \sum_{\sigma_u} \mathbb{P}_n(\sigma_u) \sum_G \left| \frac{\mathbb{P}_n(G|\sigma_u, \sigma_S)}{\mathbb{P}_n(G|\sigma_S)} - 1 \right| \mathbb{P}_n(G|\sigma_S) \\
&= \sum_i \pi(i) TV(\mathbb{P}_n(G|\sigma_u = i, \sigma_S), \mathbb{P}_n(G|\sigma_S)) = o(1),
\end{aligned}$$

where the last step follows from Proposition 7.1. \square

We are now ready to prove Theorem 3.9.

Proof of Theorem 3.9. We will show that $\lim_{n \rightarrow \infty} \mathbb{E}(\text{overlap}(\mathcal{A}(G), \sigma)) = 0$. Theorem 3.9 then follows from Markov's inequality. We first bound $\mathbb{E}(\text{overlap}(\mathcal{A}(G), \sigma))$ as follows:

$$\begin{aligned} \mathbb{E}(\text{overlap}(\sigma, \mathcal{A}(G))) &= \frac{1}{n} \mathbb{E} \left(\max_{\rho} \sum_{i=1}^s \left(N_{i\rho(i)}(\sigma, \mathcal{A}(G)) - \frac{1}{n} N_i(\sigma) N_{\rho(i)}(\mathcal{A}(G)) \right) \right) \\ &\leq \frac{1}{n} \sum_{\rho} \mathbb{E} \left(\left| \sum_{i=1}^s \left(N_{i\rho(i)}(\sigma, \mathcal{A}(G)) - \frac{1}{n} N_i(\sigma) N_{\rho(i)}(\mathcal{A}(G)) \right) \right| \right). \end{aligned} \quad (13)$$

We will now show that each of the terms in the above summation goes to zero. Wlog, let ρ be identity. Fix $i \in [s]$ and consider the term $\mathbb{E} \left| \left(N_{ii} - \frac{1}{n} N_i(\sigma) N_i(\mathcal{A}(G)) \right) \right|$ (for brevity, we suppress $\sigma, \mathcal{A}(G)$ in $N_{ii}(\sigma, \mathcal{A}(G))$). Using Jensen's inequality, it is sufficient to bound

$$\mathbb{E} \left(N_{ii} - \frac{1}{n} N_i(\sigma) N_i(\mathcal{A}(G)) \right)^2 = \mathbb{E} \left(N_{ii}^2 - \frac{2}{n} N_{ii} N_i(\sigma) N_i(\mathcal{A}(G)) + \frac{1}{n^2} N_i^2(\sigma) N_i^2(\mathcal{A}(G)) \right). \quad (14)$$

We will now calculate each of the above three terms.

$$\begin{aligned} \mathbb{E} N_{ii}^2 &= \mathbb{E} \left(\sum_u \mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \right)^2 = \sum_{u,v} \mathbb{E} \mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \\ &= \sum_{u,v} \mathbb{E} \mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \\ &= \sum_{u,v} \mathbb{E} \left(\mathbb{E} \left(\mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \middle| G \right) \right) \\ &= \sum_{u,v} \mathbb{E} \left(\mathbb{E} \left(\mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \middle| G \right) \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \right) \\ &= (\pi(i)^2 \mathbb{E} \left(\mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \right) + o(1)) n^2, \end{aligned} \quad (15)$$

where the last step follows from Lemma 7.2. Coming to the second term, we have:

$$\begin{aligned} \mathbb{E} N_{ii} N_i(\sigma) N_i(\mathcal{A}(G)) &= \mathbb{E} \left(\sum_u \mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \right) \left(\sum_u \mathbb{1}_{\{\sigma_u=i\}} \right) \left(\sum_u \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \right) \\ &= \sum_{u,v,w} \mathbb{E} \left(\mathbb{E} \left(\mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \mathbb{1}_{\{\mathcal{A}(G)_w=i\}} \middle| G \right) \right) \\ &= \sum_{u,v,w} \mathbb{E} \left(\mathbb{E} \left(\mathbb{1}_{\{\sigma_u=i\}} \mathbb{1}_{\{\sigma_v=i\}} \middle| G \right) \mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_w=i\}} \right) \\ &= (\pi(i)^2 \mathbb{E} \left(\mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \right) + o(1)) n^3, \end{aligned} \quad (16)$$

where the last step again follows from Lemma 7.2. A similar argument shows that

$$\mathbb{E} N_i^2(\sigma) N_i^2(\mathcal{A}(G)) = (\pi(i)^2 \mathbb{E} \left(\mathbb{1}_{\{\mathcal{A}(G)_u=i\}} \mathbb{1}_{\{\mathcal{A}(G)_v=i\}} \right) + o(1)) n^4. \quad (17)$$

Plugging (15), (16) and (17) in (14) shows that

$$\mathbb{E} \left(N_{ii} - \frac{1}{n} N_i(\sigma) N_i(\mathcal{A}(G)) \right)^2 = o(n^2).$$

This finishes the proof. \square

8 Examples

In this section, we will present a proof of Proposition 3.10. We use the following lemma, which is a restatement of Lemma 4.7 from Mossel et al. [MNS13]. It establishes an approximate Markov structure on the labels of two sets of nodes with a small separator.

Lemma 8.1. *(Restatement of Lemma 4.7 from [MNS13]) Let $A = A(G)$, $B = B(G)$ and $C = C(G) \subset V$ be a (random) partition of V such that B separates A and C in G . If $|A \cup B| = o(\sqrt{n})$ for a.a.e. G , then*

$$\mathbb{P}_n(\sigma_A | \sigma_{B \cup C}, G) = (1 + o(1)) \mathbb{P}_n(\sigma_A | \sigma_B, G_{A \cup B}),$$

for a.a.e. G and σ .

Remark: Lemma 4.7 from [MNS13] only states that

$$\mathbb{P}_n(\sigma_A | \sigma_{B \cup C}, G) = (1 + o(1)) \mathbb{P}_n(\sigma_A | \sigma_B, G).$$

However, its proof directly gives us the stronger statement above. We are now ready to prove Proposition 3.10.

Proof of Proposition 3.10. We will prove the proposition by showing that the conclusion of Lemma 7.2 holds i.e., for any set S of constant size and $u \notin S$,

$$\mathbb{E}(TV(\mathbb{P}_n(\sigma_u | G, \sigma_S), \pi) | \sigma_S) = o(1). \quad (18)$$

Since the size of the largest component is $O(\log n)$, u and S are disconnected a.a.s. Choosing A to be the component of u , B to be \emptyset and C to be $V \setminus A$ in Lemma 8.1, we see that σ_A and σ_S are a.a.s. independent given G_A . Hence σ_u and σ_S are also a.a.s. independent given G_A . So, we see that

$$TV(\mathbb{P}_n(\sigma_u | \sigma_S, G), \mathbb{P}_n(\sigma_u | G_A)) \rightarrow 0 \text{ for a.e. } G.$$

In order to show (18), it suffices to show that

$$TV(\mathbb{P}_n(\sigma_u | G_A), \pi) \rightarrow 0 \text{ for a.e. } G.$$

This in turn follows if we show that

$$TV(\mathbb{P}_n(G_A | \sigma_u = 1), \mathbb{P}_n(G_A | \sigma_u = 2)) \rightarrow 0 \text{ for a.e. } G.$$

This is clearly true since

- $\mathbb{P}_n(G_A | \sigma_u = 1) = \mathbb{Q}_{pn}(G_A)$ and $\mathbb{P}_n(G_A | \sigma_u = 2) = \mathbb{Q}_{(1-p)n}(G_A)$,
- $\lim_{r \rightarrow \infty} \mathbb{Q}_n(|G_A| > r) = 0$, and
- $\mathbb{Q}_n(G_A \mid |G_A| = r)$ converges in distribution for every fixed r .

This proves (18). The rest of the proof is the same as that of Theorem 3.9. \square

9 Open problems

Our results show that the Kesten-Stigum bound is not the threshold for reconstructability in the stochastic block model. Indeed, Propositions 3.3 and 3.10 show that even for the two cluster models with a fixed partition size, reconstructability does not have a threshold behavior in $\lambda_2^2 d$.

Question 9.1. *What is the precise boundary between reconstructability and non-reconstructability in unbalanced two cluster models?*

We obtain non-distinguishability and non-reconstructability by showing the existence of a certain second moment. The existence of any $(1 + \epsilon)$ moment suffices for part of our results. However, calculating such moments seems much harder.

Question 9.2. *Characterize the region where the $1 + \epsilon$ moment is finite for some $\epsilon < 1$.*

The function Q in our uniform integrability condition is not explicit. Currently, the only way we can estimate Q is via numerical optimization.

Question 9.3. *Can we evaluate Q explicitly? Can we obtain good bounds for it?*

Finally, we would like to stress that the most novel contribution of our work is to relate non-reconstructability with non-distinguishability. We believe that this connection might prove useful in other contexts where non-reconstructability results have so far proved elusive.

References

- [BJR07] Béla Bollobás, Svante Janson, and Oliver Riordan. The phase transition in inhomogeneous random graphs. *Random Structures & Algorithms*, 31(1):3–122, 2007.
- [CK01] A. Condon and R.M. Karp. Algorithms for graph partitioning on the planted partition model. *Random Structures and Algorithms*, 18(2):116–140, 2001.
- [CO10] A. Coja-Oghlan. Graph partitioning via adaptive spectral techniques. *Combinatorics, Probability and Computing*, 19(02):227–284, 2010.
- [DF89] M.E. Dyer and A.M. Frieze. The solution of some random NP-hard problems in polynomial expected time. *Journal of Algorithms*, 10(4):451–489, 1989.
- [DKMZ11] A. Decelle, F. Krzakala, C. Moore, and L. Zdeborová. Asymptotic analysis of the stochastic block model for modular networks and its algorithmic applications. *Physics Review E*, 84:066106, Dec 2011.
- [HLL83] P.W. Holland, K.B. Laskey, and S. Leinhardt. Stochastic blockmodels: First steps. *Social Networks*, 5(2):109 – 137, 1983.
- [Jan95] Svante Janson. Random regular graphs: asymptotic distributions and contiguity. *Combinatorics, Probability and Computing*, 4(04):369–405, 1995.
- [JS98] M. Jerrum and G.B. Sorkin. The Metropolis algorithm for graph bisection. *Discrete Applied Mathematics*, 82(1-3):155–175, 1998.

- [KMM⁺13] F. Krzakala, C. Moore, E. Mossel, J. Neeman, A. Sly, Zdeborova L, and P. Zhang. Spectral redemption: clustering sparse networks. *arXiv:1306.5550*, 2013.
- [Mas14] L. Massoulié. Community detection thresholds and the weak Ramanujan property. *arXiv:1311.3085*, 2014.
- [MNS13] E. Mossel, J. Neeman, and A. Sly. Stochastic block models and reconstruction. *arXiv:1202.4124*, 2013.
- [MNS14] Elchanan Mossel, Joe Neeman, and Allan Sly. A proof of the block model threshold conjecture. *arXiv:1311.4115*, 2014.
- [MP92] A.M. Mathai and Serge B. Provost. *Quadratic Forms in Random Variables*. Statistics Series. Taylor & Francis, 1992.
- [RW92] R.W. Robinson and N.C. Wormald. Almost all cubic graphs are Hamiltonian. *Random Structures and Algorithms*, 3(2):117–125, 1992.
- [SN97] T.A.B. Snijders and K. Nowicki. Estimation and prediction for stochastic blockmodels for graphs with latent block structure. *Journal of Classification*, 14(1):75–100, 1997.
- [VAC14] Nicolas Verzelen and Ery Arias-Castro. Community detection in sparse random networks. *arXiv preprint arXiv:1308.2955*, 2014.
- [Wor99] N.C. Wormald. Models of random regular graphs. *London Mathematical Society Lecture Note Series*, pages 239–298, 1999.

A UI and multinomials

Here, we restate and prove Proposition 6.5. Recall that Δ_s denotes the set $\{(\alpha_1, \dots, \alpha_s) : \alpha_i \geq 0 \text{ and } \sum_i \alpha_i = 1\}$, and that $\Delta_{s^2}(\pi)$ denotes the set of $(\alpha_{11}, \dots, \alpha_{ss})$ such that

$$\begin{aligned} \alpha_{ij} &\geq 0 \text{ for all } i, j, \\ \sum_{i=1}^s \alpha_{ij} &= \pi_j \text{ for all } j, \text{ and} \\ \sum_{j=1}^s \alpha_{ij} &= \pi_i \text{ for all } i. \end{aligned}$$

In what follows, we fix an $s^2 \times s^2$ matrix A and some $\pi \in \Delta_s$. We define $p \in \Delta_{s^2}(\pi)$ by $p_{ij} = \pi_i \pi_j$ (or alternatively, $p = \pi^{\otimes 2}$), and we take $N \sim \text{Multinom}(n, p)$ and $X = (N - np)/\sqrt{n}$. Finally, fix a sequence a_n such that $\sqrt{n} \ll a_n \ll n$ and define Ω_n to be the event that

$$\max_j \left| \sum_i N_{ij} - n\pi_j \right| \leq a_n \tag{19}$$

$$\max_i \left| \sum_j N_{ij} - n\pi_i \right| \leq a_n. \tag{20}$$

Note that the condition $\sqrt{n} \ll a_n$ ensures that the probability of Ω_n converges to 1.

Proposition A.1. *Define*

$$\lambda = \sup_{\alpha \in \Delta_{s^2}(\pi)} \frac{(\alpha - p)^T A (\alpha - p)}{D(\alpha, p)}.$$

If $\lambda < 1$ then

$$\mathbb{E}[\mathbf{1}_{\Omega_n} \exp(Y^T A Y)] \rightarrow \mathbb{E} \exp(Z^T A Z) < \infty,$$

as $n \rightarrow \infty$, where $Z \sim \mathcal{N}(0, \text{diag}(p) - pp^T)$. On the other hand, if $\lambda > 1$ then

$$\mathbb{E}[\mathbf{1}_{\Omega_n} \exp(Y^T A Y)] \rightarrow \infty$$

as $n \rightarrow \infty$.

Lemma A.2. *For any $\epsilon > 0$, any $k = 2, 3, \dots$, and any $p \in \Delta_k$, there is a constant $C < \infty$ such that for any n ,*

$$n^{-k/2} \sum_{r_1 + \dots + r_k = n} \exp\left(-n\epsilon \left|\frac{r}{n} - p\right|^2\right) \leq C.$$

Proof. We have

$$\begin{aligned} n^{-k/2} \sum_{r_1 + \dots + r_k = n} \exp\left(-n\epsilon \left|\frac{r}{n} - p\right|^2\right) &\leq n^{-k/2} \sum_{r_1, \dots, r_k = 1}^n \exp\left(-n\epsilon \left|\frac{r}{n} - p\right|^2\right) \\ &= \prod_{i=1}^k \left[n^{-1/2} \sum_{r=1}^n \exp\left(-n\epsilon \left(\frac{r}{n} - p_i\right)^2\right) \right]. \end{aligned}$$

The problem has now reduced to the case $k = 1$; i.e., we need to show that

$$n^{-1/2} \sum_{r=1}^n \exp(-n\epsilon(r/n - p)^2) < C(p, \epsilon).$$

We do this by dividing the sum above into $\ell = \lceil \sqrt{n} \rceil$ different sums. Note that if $\frac{r}{n} \geq p$ then

$$\left(\frac{r+\ell}{n} - p\right)^2 = \left(\frac{r}{n} - p\right)^2 + \frac{\ell^2}{n^2} + \frac{2\ell}{n} \left(\frac{r}{n} - p\right) \geq \left(\frac{r}{n} - p\right)^2 + \frac{1}{n}. \quad (21)$$

Hence, $r \geq np$ implies

$$\exp\left(-n\epsilon\left(\frac{r+\ell}{n} - p\right)^2\right) \leq e^{-\epsilon} \exp\left(-n\epsilon\left(\frac{r}{n} - p\right)^2\right).$$

Stratifying the original sum into strides of length ℓ ,

$$n^{-1/2} \sum_{r=\lfloor pn \rfloor}^n \exp(-n\epsilon(r/n - p)^2) \leq n^{-1/2} \sum_{r=\lfloor pn \rfloor}^{\lfloor pn \rfloor + \ell - 1} \sum_{m=0}^{\infty} \exp(-n\epsilon((r+m\ell)/n - p)^2).$$

Now, (21) implies that the inner sum may be bounded by a geometric series with initial value less than 1, and ratio $e^{-\epsilon}$. Hence,

$$n^{-1/2} \sum_{r=\lfloor pn \rfloor}^n \exp(-n\epsilon(r/n - p)^2) \leq n^{-1/2} \ell \frac{1}{1 - e^{-\epsilon}},$$

which is bounded. A similar argument for the case $r \leq pn$ completes the proof. \square

Proof of Proposition A.1. First, recall that for any $\alpha = (\alpha_{11}, \dots, \alpha_{ss}) \in \Delta_{s^2}$, we have $\Pr(N = \alpha n) \asymp \exp(-nD(\alpha, p))$; this just follows from Stirling's approximation. Next, note that $D(\alpha, p)$ is zero only for $\alpha = p$, and that $D(\alpha, p)$ is strongly concave in α . Therefore, $\lambda < 1$ implies that there is some $\epsilon > 0$ such that

$$D(\alpha, p) \geq (1 + \epsilon)(\alpha - p)^T A(\alpha - p) + \epsilon|\alpha - p|^2$$

for all $\alpha \in \Delta_{s^2}(p)$. Hence, any $\alpha \in \Delta_{s^2}(p)$ satisfies

$$\Pr(N = \alpha n) \exp(n(1 + \epsilon)(\alpha - p)^T A(\alpha - p)) \leq C \exp(-n\epsilon|\alpha - p|^2). \quad (22)$$

Recalling the definition of Ω_n , we write (with a slight abuse of notation) $\alpha \in \Omega_n$ if $|\max_i \sum_j \alpha_{ij} - p_i| \leq n^{-1}a_n$ and similarly with i and j reversed. Note that for every $\alpha \in \Omega_n$, there is some $\tilde{\alpha} \in \Delta_{s^2}(\pi)$ with $|\alpha - \tilde{\alpha}|^2 = o(n^{-1})$; in particular, (22) also holds for all $\alpha \in \Omega_n$ (with a change in the constant C). Then

$$\begin{aligned} \mathbb{E}[\mathbf{1}_{\Omega_n} \exp((1 + \epsilon)X^T A X)] &= \sum_{\alpha \in \Omega_n} \Pr(N = \alpha n) \exp(n(1 + \epsilon)(\alpha - p)^T A(\alpha - p)) \\ &\leq \sum_{\alpha \in \Omega_n} \exp(-n\epsilon|\alpha - p|^2) \\ &\leq C < \infty, \end{aligned}$$

for some constant C independent of n , where the last line follows from Lemma A.2. In particular, $\exp(X^T AX)$ has $1 + \epsilon$ uniformly bounded moments, and so it is uniformly integrable as $n \rightarrow \infty$. Since $X \xrightarrow{d} \mathcal{N}(0, \text{diag}(p) - pp^T)$, it follows that $\mathbb{E} \exp(X^T AX) \rightarrow \mathbb{E} \exp(X^T AX)$.

In the other direction, if $\lambda > 1$ then there is some $\alpha \in \Delta_{s^2}(p)$, $\alpha \neq p$ and some $\epsilon > 0$ such that $D(\alpha, p) \leq (\alpha - p)^T A(\alpha - p) - 2\epsilon$. By the continuity of $D(\alpha, p)$ and $(\alpha - p)^T A(\alpha - p)$, we see that for sufficiently large n , there exists $r \in n\Delta_{s^2}(p)$ such that

$$D(r/n, p) \leq (r/n - p)^T A(r/n - p) - \epsilon.$$

For any n , let $r^* = r^*(n)$ be such an r . Then

$$\begin{aligned} \mathbb{E} \exp(X^T AX) &\geq \Pr(N = r^*(n)) \exp(n(r^*/n - p)^T A(r^*/n - p)) \\ &\asymp \exp(n((r^*/n - p)^T A(r^*/n - p) - D(r^*/n, p))) \\ &\geq \exp(n\epsilon) \rightarrow \infty. \end{aligned}$$

□