SUPPLEMENTARY MATERIAL: CONSISTENT SPECTRAL CLUSTERING OF NETWORK BLOCK MODELS UNDER LOCAL DIFFERENTIAL PRIVACY

JONATHAN HEHIR, ALEKSANDRA SLAVKOVIĆ, AND XIAOYUE NIU

Department of Statistics, Penn State University, University Park, PA, USA
e-mail address: jh@psu.edu
Department of Statistics, Penn State University, University Park, PA, USA
e-mail address: sesa@psu.edu
Department of Statistics, Penn State University, University Park, PA, USA
e-mail address: xiaoyue@psu.edu

APPENDIX A. PROOFS OF MAIN RESULTS

The proofs of the results from Section 5 closely follow the techniques of Lei and Rinaldo [2015]. For both SBM and DCBM, we will require the following notation. Let \( \text{eig}_k(\cdot): \mathbb{R}^{n \times n} \rightarrow \mathbb{R}^{n \times k} \) denote a function that returns the eigenvectors of its argument corresponding to the \( k \) largest eigenvalues in absolute value.

Let \( Y \sim \text{DCBM}(\theta, \psi, B) \), where \( \psi = 1 \) for SBM. Let \( P \) be the \( n \times n \) matrix with entries \( P_{ij} = \psi_i \psi_j B_{\theta_i \theta_j} \). Note that \( E[Y] = P - \text{diag}(P) \), as \( Y \) has zeros on the diagonal by construction. Let \( \hat{U} = \text{eig}_k(Y) \) denote the eigenvectors of the observed non-private adjacency matrix \( Y \), and \( U = \text{eig}_k(P) \) denote the eigenvectors of the expected adjacency matrix (plus a diagonal).

We will use a \( \downarrow \) subscript to denote private analogs to these quantities. Assuming \( \varepsilon < \infty \), let \( Y_\downarrow = (d_\varepsilon \circ M_\varepsilon)(Y) \) denote the edge-flipped and downshifted synthetic network. Since \( E[Y_\downarrow] = \varepsilon \frac{\varepsilon - 1}{\varepsilon^2 + 1} E[Y] \) (Corollary 3.9), we let \( \hat{P}_\downarrow = \varepsilon \frac{\varepsilon - 1}{\varepsilon^2 + 1} P \), and let \( \hat{U}_\downarrow = \text{eig}_k(Y_\downarrow) \) and \( U_\downarrow = \text{eig}_k(P_\downarrow) \). If \( \varepsilon = \infty \), we have no privacy, so we let \( Y_\downarrow = Y, P_\downarrow = P, \hat{U}_\downarrow = \hat{U}, U_\downarrow = U \).

A critical fact for the proofs of the main theorems is that the matrix \( U_\downarrow \) can be chosen to be precisely equal to \( U \), even if \( \varepsilon < \infty \), since if \( VAV^T \) is an eigendecomposition of \( P \), then \( V \left( \frac{\varepsilon - 1}{\varepsilon^2 + 1} A \right) V^T \) is an eigendecomposition of \( P_\downarrow \). For this reason, we will assume below that \( U_\downarrow = U \).

We begin with a lemma that captures the main technical distinction between our results and those of Lei and Rinaldo [2015].

Key words and phrases: community detection, differential privacy, spectral clustering, stochastic block model.
Lemma A.1. Suppose $Y \sim \text{DCBM}(\theta, \Psi, B)$ with $\max_{i \in C_j} \psi_i = 1$ for $j \in [k]$, $B$ full rank, $\text{max} B \geq \log n/n$, and minimum absolute eigenvalue $\lambda_B > 0$. Let $\varepsilon \in (0, \infty]$, and let $g_\varepsilon(B)$ as defined in eq. (5.1). There exists a universal constant $c_0$ and a $k \times k$ orthogonal matrix $Q$ such that:

$$P \left( \|\hat{U}_\perp - U_\perp Q\|_F \leq c_0 \frac{2\sqrt{2k}n\varepsilon g_\varepsilon(B)}{\tilde{n}_{\min} \lambda_B} \right) \geq 1 - n^{-1}.$$ 

Proof. By Lemma 5.1 of Lei and Rinaldo [2015], there exists a $k \times k$ orthogonal matrix $Q$ such that:

$$\|\hat{U}_\perp - U_\perp Q\|_F \leq \frac{2\sqrt{2k}n\varepsilon}{\lambda_{P_{\perp}}} \|Y_\perp - P_{\perp}\|$$

$$= \frac{2\sqrt{2k}}{\lambda_{P_{\perp}}} \|M_\varepsilon(Y) - E[M_\varepsilon(Y)] - \text{diag}(P_{\perp})\|$$

$$\leq \frac{2\sqrt{2k}}{\lambda_{P_{\perp}}} \left(\|M_\varepsilon(Y) - E[M_\varepsilon(Y)]\| + 1\right),$$

where the last inequality follows from the fact that $\|\text{diag}(P_{\perp})\| \leq 1$, as every entry of $P_{\perp}$ is bounded in the unit interval. From here, it remains to find a lower bound for $\lambda_{P_{\perp}}$ and an upper bound for $\|M_\varepsilon(Y) - E[M_\varepsilon(Y)]\|$.

We begin with the simpler task of bounding $\lambda_{P_{\perp}}$. Consider first the case when $\varepsilon = \infty$. In this case, $P_{\perp} = P$. From the proof of Lei and Rinaldo [2015] Lemma 4.1, we know that the nonzero eigenvalues of $P$ are precisely those of $\Psi B \Psi$, where $\Psi = \text{diag}(\sqrt{n_1}, \ldots, \sqrt{n_k})$. Since both $B$ and $\Psi$ are symmetric and invertible, we can say that:

$$\|(\Psi B \Psi)^{-1}\| \leq \|\Psi^{-1}\| \|B^{-1}\| \|\Psi^{-1}\|$$

$$= \lambda_\Psi^{-1} \lambda_B^{-1} \lambda_\Psi^{-1}$$

$$= \tilde{n}_{\min}^{-1} \lambda_B^{-1}.$$ 

The fact that $\|(\Psi B \Psi)^{-1}\|$ is the largest absolute eigenvalue of $(\Psi B \Psi)^{-1}$ further implies that the smallest absolute eigenvalue of $\Psi B \Psi$ satisfies:

$$\lambda_P = \lambda_{\Psi B \Psi} \geq \tilde{n}_{\min} \lambda_B.$$ 

When $\varepsilon < \infty$, recall that $P_{\perp} = \frac{\varepsilon^{-1} - 1}{\varepsilon + 1} P$, so:

$$\lambda_{P_{\perp}} \geq \begin{cases} 
\tilde{n}_{\min} \lambda_B, & \varepsilon = \infty \\
\frac{\varepsilon^{-1} - 1}{\varepsilon + 1} \tilde{n}_{\min} \lambda_B, & \varepsilon < \infty.
\end{cases}$$

Next, we can upper bound $\|M_\varepsilon(Y) - E[M_\varepsilon(Y)]\|$ using Theorem 5.2 of Lei and Rinaldo [2015]. First, we establish necessary bounds on the entries of $E[M_\varepsilon(Y)]$. Let:

$$\mu = \begin{cases} 
\text{max} B, & \varepsilon = \infty \\
\frac{\varepsilon^{-1} - 1}{\varepsilon + 1} (\text{max} B) + \frac{2}{\varepsilon + 1} \left(\frac{1}{2}\right), & \varepsilon < \infty.
\end{cases}$$

In both cases, we can see that $\mu$ is an upper bound for $\text{max} E[M_\varepsilon(Y)]$, per the definition of DCBM and Lemma 3.7. Additionally, we can view $\mu$ as an affine combination of $\text{max} B$ and $\frac{1}{2}$, from which it is clear that $\mu \geq \min\{\frac{1}{2}, \text{max} B\} \geq \log n/n$ (for $n \geq 1$). So by Lei and Rinaldo [2015] Theorem 5.2, with probability at least $1 - n^{-1}$:

$$\|M_\varepsilon(Y) - E[M_\varepsilon(Y)]\| \leq C \sqrt{\tilde{n} \mu},$$

where
where \( C = C(1, 1) \) for \( C(\cdot, \cdot) \) defined in Lei and Rinaldo [2015]. Combining some facts, we now have that with probability at least \( 1 - n^{-1} \):

\[
\| \hat{U}_\downarrow - U_\downarrow Q \|_F \leq 2\sqrt{2k}\frac{C\sqrt{\mu}}{\lambda P_1} + 1.
\]

Since \( \mu \geq \log n/n \), then \( 1 \leq (\log 2)^{-1/2}\sqrt{\mu} \) (for \( n > 1 \)). Thus if we let \( c_0 = C + (\log 2)^{-1/2} \), we can simplify the above to:

\[
\| \hat{U}_\downarrow - U_\downarrow Q \|_F \leq c_0 \frac{2\sqrt{2kn\mu}}{\lambda P_1}.
\]

Finally, it remains to put these results in terms of \( g_\varepsilon(B) \) and \( \lambda_B \). When \( \varepsilon = \infty \), it is clear that:

\[
\frac{\sqrt{\mu}}{\lambda P_1} \leq \frac{\sqrt{\max B}}{n_{\min} \lambda B} = \frac{\sqrt{g_\varepsilon(B)}}{n_{\min} \lambda B}.
\]

When \( \varepsilon < \infty \), this same inequality holds, albeit with different intermediate steps:

\[
\frac{\sqrt{\mu}}{\lambda P_1} \leq \frac{1}{n_{\min} \lambda B} \frac{e^\varepsilon + 1}{e^\varepsilon - 1} \sqrt{\left( e^\varepsilon - 1 \right) \max B + 1} = \frac{1}{n_{\min} \lambda B} \frac{e^\varepsilon + 1}{e^\varepsilon - 1} \left( \max B + \frac{1}{e^\varepsilon - 1} \right) \leq \frac{\sqrt{g_\varepsilon(B)}}{n_{\min} \lambda B}.
\]

Thus, we conclude that with probability at least \( 1 - n^{-1} \):

\[
\| \hat{U}_\downarrow - U_\downarrow Q \|_F \leq c_0 \frac{2\sqrt{2kn_\varepsilon(B)}}{n_{\min} \lambda_B}.
\]

\[\square\]

A.1. The \( k \)-means and \( k \)-medians Problems. Recall that Algorithm 1 requires solving an approximate \( k \)-means problem, while Algorithm 2 requires solving an approximate \( k \)-medians problem. The proofs of Theorems 5.1 and 5.2 rely on some additional notation and properties surrounding these problems.

Let \( G^{n \times k} \) denote the set of \( n \times k \) membership matrices consisting of a single one in each row with zeroes elsewhere. In both the \( k \)-means and \( k \)-medians problems applied to the rows of the matrix \( \hat{U} \), we seek a membership matrix \( \Theta \in G^{n \times k} \) and set of centroids \( X \in \mathbb{R}^{k \times k} \) that minimize the distance \( \| \Theta X - \hat{U} \|_F \) for a suitable norm \( \| \cdot \|_* \). In \( k \)-means, the norm chosen is the Frobenius norm, while in the \( k \)-medians problem, the norm chosen is the \( (2,1) \) norm, \( \| A \|_{2,1} = \sum_i \| A_{i*} \|_2 \). Finding an exact solution for each of these problems is difficult, but efficient approximation algorithms exist. We will call a solution \( \hat{\Theta}X \) a \((1 + \gamma)\)-approximate solution to the \( k \)-means problem if:

\[
\| \hat{\Theta}X - \hat{U} \|_F^2 \leq (1 + \gamma) \inf_{\Theta' \in G^{n \times k}, X'} \| \Theta'X' - \hat{U} \|_F^2.
\]
Similarly, we will call $\hat{\Theta} \hat{X}$ a $(1 + \gamma)$-approximate solution to the $k$-medians problem if:

$$
\|\hat{\Theta} \hat{X} - \hat{U}\|_{2,1} \leq (1 + \gamma) \left[ \inf_{\Theta' \in \mathbb{G}^{n,k}, X'_{k \times k}} \|\Theta' X' - \hat{U}\|_{2,1} \right].
$$

(A.1)

In the main text, we denote the membership parameter $\theta$ as a vector. One can easily convert a membership matrix $\Theta \in \mathbb{G}^{n,k}$ to a membership vector $\theta \in [k]^n$ by choosing $\theta_i = \arg\max_j \Theta_{ij}$.

A.2. SBM.

Proof of Theorem 5.1. We begin by recalling that $\text{SBM}(\theta, B) \overset{D}{=} \text{DCBM}(\theta, 1_n, B)$ (per eq. 2.1), and so by Lemma A.1, there exists a universal constant $c_0$ and orthogonal matrix $Q$ such that with probability at least $1 - n^{-1}$:

$$
\|\hat{U}_\downarrow - U_\downarrow Q\|_F \leq c_0 \frac{2\sqrt{2kng_e(B)}}{n_{\min} \lambda_B}.
$$

(A.2)

From here, the proof follows the same line of argument as Lei and Rinaldo [2015] Theorem 3.1 and Corollary 3.2. For completeness, and since our parameterization is a bit different, we include the remainder of the proof here.

Since $U_\downarrow = U$, we know from Lei and Rinaldo [2015] Lemma 3.1 that $U_\downarrow Q = \Theta X'$ for some $\Theta \in \mathbb{G}^{n,k}$ and $X'_{k \times k}$ satisfying:

$$
\|X'_j - X'_{\ell}\|_2 = \sqrt{n_j^{-1} + n_{\ell}^{-1}}
$$

for $j \neq \ell$. Now we wish to apply Lemma 5.3 of Lei and Rinaldo [2015]. For $j \in [k]$, choose $\delta_j = \sqrt{n_j^{-1} + (\max_{\ell \neq j, \ell} n_{\ell})^{-1}}$, and define $S_j$ as in Lemma 5.3 of Lei and Rinaldo [2015]. We want to show that $(16 + 8\gamma)\|\hat{U}_\downarrow - U_\downarrow Q\|^2_F / \delta_j^2 < n_j$ for $j \in [k]$. Since $\delta_j^2 n_j > 1$ for all $j$, it suffices to show that $(16 + 8\gamma)\|\hat{U}_\downarrow - U_\downarrow Q\|^2_F \leq 1$. Under the condition that (A.2) holds, we have that:

$$
(16 + 8\gamma)\|\hat{U}_\downarrow - U_\downarrow Q\|^2_F \leq \frac{64c_0^2(2 + \gamma)kng_e(B)}{n_{\min}^2 \lambda_B^2}
$$

Choosing $c_1 = 64c_0^2$, then (5.2) implies that the above is $\leq 1$, as desired. Thus, for each community $j \in [k]$, the set of nodes that are possibly misclassified by Algorithm 1 must be a subset of $S_j$, and since $\delta_j^2 > n_j^{-1}$:

$$
\sum_{j=1}^k \frac{|S_j|}{n_j} \leq \sum_{j=1}^k |S_j| \delta_j^2 \leq 4(4 + 2\gamma)\|\hat{U}_\downarrow - U_\downarrow Q\|^2_F \leq \frac{64c_0^2(2 + \gamma)kng_e(B)}{n_{\min}^2 \lambda_B^2} = \frac{(2 + \gamma)kng_e(B)}{n_{\min}^2 \lambda_B^2}.
$$
So then we have that:
\[
\tilde{L}(\theta, \tilde{\theta}_\varepsilon) \leq \max_{j:k} \frac{|S_j|}{n_j} \leq c_1 \frac{(2 + \gamma)kn}{\lambda_B^2} g_\varepsilon(B)
\]
\[
L(\theta, \tilde{\theta}_\varepsilon) \leq \frac{1}{n} \sum_{j=1}^{k} |S_j| \leq c_1 \frac{(2 + \gamma)kn'}{\lambda_B^2} g_\varepsilon(B).
\]

\[
A.3. \ DCBM.
\]

**Proof of Theorem 5.2.** We begin with the results of Lemma A.1, which states that there exists a universal constant \(c_0\) and a \(k \times k\) orthogonal matrix \(Q\) such that with probability at least \(1 - n^{-1}\):
\[
\|\tilde{U}_\downarrow - U_\downarrow Q\|_F \leq c_0 \frac{2\sqrt{2nk}g_\varepsilon(B)}{\lambda_{\min}}.
\]

The remainder of the proof follows very closely from the proofs of Lemma A.1 and Theorem 4.2 from Lei and Rinaldo [2015]. We define the sets \(I_0, I_+, \text{ and } S\) as in the original proofs. Recall that Algorithm 2 requires separate handling of zero vs. non-zero rows of \(\tilde{U}_\downarrow\).

The set \(I_0 = \{i \in [n] \mid (\tilde{U}_\downarrow)_{is} = 0\}\) holds the set of nodes whose embeddings are zero, and \(I_+ = [n] \setminus I_0\) holds the remainder. We allow that the nodes in \(I_0\) will be misclassified, and we define a set \(S \subseteq I_+\) in which we also allow misclassification. Our goal, then, is to bound \(|I_0 \cup S|\). We start by bounding \(|I_0|\). Note that:
\[
\|\tilde{U}_\downarrow - U_\downarrow Q\|_F^2 \geq \sum_{i \in I_0} \|(U_\downarrow Q)_{is}\|_2^2 \\
\geq \frac{|I_0|^2}{\sum_{i \in I_0} \|(U_\downarrow Q)_{is}\|_2^2} \quad \text{(Cauchy-Schwarz)} \\
\geq \frac{|I_0|^2}{\sum_{i=1}^n \|U_{is}\|_2^2} \quad \text{\((U_\downarrow = U, Q\text{ orthogonal})\)}
\]

From Lei and Rinaldo [2015] Lemma 4.1, we know that \(\|U_{is}\|_2^2 = \tilde{\nu}_\theta \tilde{\psi}_i^{-2}\), so \(\sum_{i=1}^n \|U_{is}\|_2^2 = \sum_{j=1}^k n_j^2 \nu_j\). Thus:
\[
|I_0| \leq \|\tilde{U}_\downarrow - U_\downarrow Q\|_F \sqrt{\sum_{j=1}^k n_j^2 \nu_j}.
\]

Moving on to \(I_+\), we construct \(\tilde{U}'_\downarrow\) of size \(|I_+| \times k\) to be the row-normalized version of \(\tilde{U}_\downarrow\), excluding zero rows, i.e., for \(i = 1, \ldots, |I_+|\) and \(j = (I_+)_i\):
\[
(\tilde{U}'_\downarrow)_{is} = (\tilde{U}_\downarrow)_{j*}/\|\tilde{U}_\downarrow j*\|_2.
\]

Let \(U'_\downarrow\) be the \(n \times k\) row-normalized version of the expected embeddings \(\tilde{U}_\downarrow\), where zero rows in \(U_\downarrow\) are preserved as zero rows in \(U'_\downarrow\). Then let \(U''_\downarrow\) to be the \(|I_+| \times k\) matrix constructed from the non-zero rows of \(U'_\downarrow\), i.e., for \(i = 1, \ldots, |I_+|\) and \(j = (I_+)_i\):
\[
(U''_\downarrow)_{is} = (U'_\downarrow)_{j*}.
\]
By (A.1), if $\hat{\Theta}_+ \hat{X}$ is a $(1 + \gamma)$-approximate solution to the $k$-medians problem on $\hat{U}_+$, then

$$
\|\hat{\Theta}_+ \hat{X} - \hat{U}'_+ \|_{2,1} \leq (1 + \gamma) \|\hat{U}'_+ - U''_+ Q\|_{2,1},
$$

and so:

$$
\|\hat{\Theta}_+ \hat{X} - U''_+ Q\|_{2,1} \leq \|\hat{\Theta}_+ \hat{X} - \hat{U}'_+ \|_{2,1} + \|\hat{U}'_+ - U''_+ Q\|_{2,1}
$$

$$
\leq (2 + \gamma) \|\hat{U}'_+ - U''_+ Q\|_{2,1}
$$

Using the fact that, for any vectors $v_1, v_2$ of equal dimension, $\|\frac{v_1}{\|v_1\|} - \frac{v_2}{\|v_2\|}\| \leq 2 \|v_1 - v_2\| / \|v_1\|$ [Lei and Rinaldo, 2015], we can bound the above (2,1) norm as follows:

$$
\|\hat{U}'_+ - U''_+ Q\|_{2,1} = \sum_{i \in I_+} \|(\hat{U}'_+)_i - (U''_+ Q)_i\|_2 \quad \text{(norm definition)}
$$

$$
\leq 2 \sum_{i = 1}^n \frac{\|(\hat{U}'_+)_i - (U''_+ Q)_i\|_2}{\|(U''_+ Q)_i\|_2} \quad \text{(fact above)}
$$

$$
= 2 \sqrt{\left( \sum_{i = 1}^n \|(\hat{U}'_+)_i - (U''_+ Q)_i\|_2 \|(U''_+ Q)_i\|_2^{-1} \right)^2}
$$

$$
\leq 2 \sqrt{\left( \sum_{i = 1}^n \|(\hat{U}'_+)_i - (U''_+ Q)_i\|_2^2 \right) \left( \sum_{i = 1}^n \|(U''_+ Q)_i\|_2^{-2} \right)} \quad \text{(Cauchy-Schwarz)}
$$

$$
= 2 \sqrt{\|\hat{U}'_+ - U''_+ Q\|_F^2 \sum_{i = 1}^n \|(U''_+ Q)_i\|_2^{-2}} \quad \text{($U''_+ Q = U$)}
$$

$$
= 2 \sqrt{\|\hat{U}'_+ - U''_+ Q\|_F^2 \sum_{j = 1}^k n_j^2 \nu_j}
$$

Let $S = \{ i \in I_+ : \|(\hat{\Theta}_+)_i \hat{X} - (U''_+ Q)_i\|_2 \geq 2^{-1/2} \}$. These are the nodes in $I_+$ for which

$$
2^{-1/2} |S| \leq \sum_{i \in I_+} \|(\hat{\Theta}_+)_i \hat{X} - (U''_+ Q)_i\|_2 = \|\hat{\Theta}_+ \hat{X} - U''_+ Q\|_{2,1}
$$

Thus we can bound $|S|:

$$
|S| \leq \sqrt{2} \|\hat{\Theta}_+ \hat{X} - U''_+ Q\|_{2,1}
$$

$$
\leq \sqrt{2} (2 + \gamma) \|\hat{U}'_+ - U''_+ Q\|_{2,1}
$$

$$
\leq 2\sqrt{2} (2 + \gamma) \|\hat{U}'_+ - U''_+ Q\|_F \sqrt{\sum_{j = 1}^k n_j^2 \nu_j}
$$

And so we can bound $|I_0 \cup S|:

$$
|I_0 \cup S| = |I_0| + |S| \leq [1 + 2\sqrt{2} (2 + \gamma)] \|\hat{U}'_+ - U''_+ Q\|_F \sqrt{\sum_{j = 1}^k n_j^2 \nu_j}
$$
With probability $1 - n^{-1}$, this is further bounded:

$$|I_0 \cup S| \leq [1 + 2\sqrt{2}(2 + \gamma)]c_0 \frac{2\sqrt{2}kg_e(B)}{\hat{n}_{\min}\lambda_B} \sqrt{\sum_{j=1}^{k} n_j^2 \nu_j}$$

$$\leq 8c_0(2.5 + \gamma)\frac{\sqrt{kg_e(B)}}{\hat{n}_{\min}\lambda_B} \sqrt{\sum_{j=1}^{k} n_j^2 \nu_j}$$

Under the condition that the above is less than $n_{\min}$, which is implied by (5.4), then for each $j \in [k]$, there must exist $i \in (C_j \setminus (I_0 \cup S))$—i.e., every block has at least one node whose normalized spectral embedding is within $2^{-1/2}$ of its expectation (in $\ell_2$ norm). Because the expected cluster centers $U''_i$ are orthogonal and have unit norm, we have $\|U''_i - U''_j\|_2 = \sqrt{2}$ whenever $\theta_i \neq \theta_j$ (or 0 otherwise). Thus for any two nodes $i, j \notin I_0 \cup S$, we have:

$$(\hat{\Theta}_+)_{is} = (\hat{\Theta}_+)_{js} \implies \|U''_{is} - U''_{js}\|_2$$

$$\leq \|((\hat{\Theta}_+)_{is} \hat{X} - U''_{is} Q) + ((\hat{\Theta}_+)_{js} \hat{X} - U''_{js} Q)\|_2$$

$$\leq \sqrt{2}$$

$$\implies U''_{is} = U''_{js}$$

$$\implies \theta_i = \theta_j$$

In other words, the set of nodes that are misclassified must be a subset of $I_0 \cup S$, and so $L(\theta, \hat{\theta}_\varepsilon) \leq |I_0 \cup S|$. The final theorem statement is obtained by choosing $c_2 = 8c_0$.

Proof of Lemma 5.3. We begin by stating a few key facts under the assumed conditions:

$$\nu_j = \left(\frac{1}{n_j} \sum_{i \in C_j} \psi_i^2\right) \left(\frac{1}{n_j} \sum_{i \in C_j} \psi_i^{-2}\right) \in [a^2, a^{-2}]$$

$$\hat{n}_{\min} = \min_{j \in [k]} \sum_{i \in C_j} \psi_i^2 \in [a^2 n_{\min}, n_{\min}]$$

$$n_{\min} = \Theta(n/k)$$

From here, we apply Theorem 5.2. First, we want to show that under the assumed conditions, (5.4) is satisfied for large $n$. A lower bound for the RHS of (5.4) is:

$$c_2^{-1} \frac{n_{\min}}{\sqrt{\sum_{j=1}^{k} n_j^2 \nu_j}} = \Omega \left(\frac{n/k}{\sqrt{k(n/k)^2 a^{-2}}}\right) = \Omega \left(k^{-1/2} a\right)$$

Then looking at the LHS of (5.4), we can write:

$$\frac{(2.5 + \gamma)\sqrt{kn g_e(B)}}{\hat{n}_{\min}\lambda_B} = O \left(\frac{\sqrt{kn g_e(B)}}{a^2(n/k)\lambda(B)}\right) = O \left(k^{3/2} \frac{\sqrt{g_e(B)}}{a^2 \lambda(B) \sqrt{n}}\right)$$

Thus Theorem 5.2 is applicable for large $n$ if:

$$\frac{k^{3/2} \sqrt{g_e(B)}}{a^2 \lambda(B) \sqrt{n}} = o \left(k^{-1/2} a\right)$$
which is satisfied by assumption. Thus we conclude that with probability $1 - n^{-1}$:

$$L(\theta, \hat{\theta}_e) \leq c_2 \frac{(2.5 + \gamma)}{n \min \lambda_B} \sqrt{\frac{k}{n} \left( \sum_{j=1}^{k} n_j^2 v_j \right) g_\varepsilon(B)}$$

$$= O \left( \frac{1}{a^2 (n/k) \lambda_B} \sqrt{\frac{k}{n} (k(n/k)^2 a^{-2}) g_\varepsilon(B)} \right)$$

$$= O \left( \frac{k \sqrt{g_\varepsilon(B)}}{a^3 \lambda_B \sqrt{n}} \right).$$

A.4. Miscellaneous. Below we prove a useful inequality for $g_\varepsilon(B)$ claimed in Section 5.

Fact A.2. Let $k \in \mathbb{N}, \varepsilon \in (0, \infty), B \in [0, 1]^{k \times k}$. Then:

$$g_\infty(B) < g_\varepsilon(B) \leq \max B + 3\varepsilon^{-1} + 2\varepsilon^{-2}$$

where $\zeta_\varepsilon = e^\varepsilon - 1$.

Proof. Note first that:

$$\frac{e^\varepsilon + 1}{e^\varepsilon - 1} = \frac{e^\varepsilon - 1}{e^\varepsilon - 1} + \frac{2}{e^\varepsilon - 1} = 1 + 2\zeta_\varepsilon^{-1}.$$

Thus:

$$g_\varepsilon(B) = \frac{e^\varepsilon + 1}{e^\varepsilon - 1} \left( \max B + \frac{1}{e^\varepsilon - 1} \right)$$

$$= (1 + 2\zeta_\varepsilon^{-1})(\max B + \zeta_\varepsilon^{-1})$$

$$= \max B + \zeta_\varepsilon^{-1} + 2\zeta_\varepsilon^{-1} \max B + 2\zeta_\varepsilon^{-2}$$

$$\leq \max B + 3\zeta_\varepsilon^{-1} + 2\zeta_\varepsilon^{-2}$$

where the last line follows from the fact that $\max B \leq 1$. The fact that $g_\infty(B) < g_\varepsilon(B)$ also follows from the above, as $\zeta_\varepsilon$ (and thus $\zeta_\varepsilon^{-1}$ and $\zeta_\varepsilon^{-2}$) is strictly positive. \qed

A.5. Privacy Guarantee. Finally, for completeness, we conclude with a formal proof of the privacy guarantee.

Proof of Theorem 3.6. Let $Y, Y'$ be two binary, undirected networks of $n$ nodes differing on one edge, $(i, j)$ with $1 \leq i < j \leq n$. Then for all $k \neq i$, we have that $\mathcal{M}_k(Y_{k*}) \overset{D}{=} \mathcal{M}_k(Y'_{k*})$. Thus, all that remains to show is that for any $a \in \{0, 1\}^n$:

$$P(\mathcal{M}_i(Y_{i*}) = a) \leq e^\varepsilon P(\mathcal{M}_i(Y'_{i*}) = a).$$

To simplify notation, we will write $\mathcal{M}_i$ in another form. Let $\mathcal{M}' : \{0, 1\} \rightarrow \{0, 1\}$ such that:

$$\mathcal{M}'(x) = \begin{cases} 1 - x & \text{w.p. } \frac{1}{1 + e^\varepsilon} \\ x & \text{w.p. } \frac{e^\varepsilon}{1 + e^\varepsilon}. \end{cases}$$
Then we can write:

\[ \mathcal{M}_i(Y_{is}) = \left( 0, \ldots, 0, \mathcal{M}'(Y_{i,i+1}), \ldots, \mathcal{M}'(Y_{in}) \right), \]

where the \( \mathcal{M}'(\cdot) \) are taken independently. Since the first \( i \) entries of \( \mathcal{M}_i(Y_{is}) \) are deterministic, we can safely restrict our attention to the case when \( a_k = 0 \) for \( k \leq i \) (since otherwise we have \( P(\mathcal{M}_i(Y_{is}) = a) = P(\mathcal{M}_i(Y_{is}') = a) = 0 \)). Thus:

\[
\frac{P(\mathcal{M}_i(Y_{is}) = a)}{P(\mathcal{M}_i(Y_{is}') = a)} = \frac{\prod_{i=1+1}^{n} P(\mathcal{M}'(Y_{ii}) = a_i)}{\prod_{i=1+1}^{n} P(\mathcal{M}'(Y_{ii}) = a_i)} = \frac{P(\mathcal{M}'(Y_{ij}) = a_j)}{P(\mathcal{M}'(Y_{ij}') = a_j)} \leq \frac{P(\mathcal{M}'(1) = 1)}{P(\mathcal{M}'(0) = 1)} = e^\varepsilon,
\]

where the inequality is taken by considering all combinations of \( Y_{ij}, Y_{ij}', \) and \( a_j \).

\[ \square \]

References

J. Lei and A. Rinaldo. Consistency of spectral clustering in stochastic block models. *Annals of Statistics*, 43(1):215–237, 2015.