

# UC Irvine

## UC Irvine Previously Published Works

### Title

Information-Theoretic Bounds and Phase Transitions in Clustering, Sparse PCA, and Submatrix Localization

### Permalink

<https://escholarship.org/uc/item/55m0q885>

### Authors

Banks, Jess  
Moore, Cristopher  
Vershynin, Roman  
[et al.](#)

### Publication Date

2017-06-01

### DOI

10.1109/isit.2017.8006706

### Copyright Information

This work is made available under the terms of a Creative Commons Attribution License, available at <https://creativecommons.org/licenses/by/4.0/>

Peer reviewed

# Information-theoretic bounds and phase transitions in clustering, sparse PCA, and submatrix localization

Jess Banks      Cristopher Moore      Roman Vershynin      Nicolas Verzelen  
 Jiaming Xu \*

January 24, 2017

## Abstract

We study the problem of detecting a structured, low-rank signal matrix corrupted with additive Gaussian noise. This includes clustering in a Gaussian mixture model, sparse PCA, and submatrix localization. Each of these problems is conjectured to exhibit a sharp information-theoretic threshold, below which the signal is too weak for any algorithm to detect. We derive upper and lower bounds on these thresholds by applying the first and second moment methods to the likelihood ratio between these “planted models” and null models where the signal matrix is zero. For sparse PCA and submatrix localization, we determine this threshold exactly in the limit where the number of blocks is large or the signal matrix is very sparse; for the clustering problem, our bounds differ by a factor of  $\sqrt{2}$  when the number of clusters is large. Moreover, our upper bounds show that for each of these problems there is a significant regime where reliable detection is information-theoretically possible but where known algorithms such as PCA fail completely, since the spectrum of the observed matrix is uninformative. This regime is analogous to the conjectured ‘hard but detectable’ regime for community detection in sparse graphs.

*Keywords:* First and second moment methods, clustering, information-theoretic bounds, sparse PCA, submatrix localization

## 1 Introduction

Many problems in machine learning, signal processing, and statistical inference have a common, unifying goal: reconstruct a low-rank signal matrix observed through a noisy channel. This framework can encompass a wide range of tasks as we vary the channel and low-rank signal, but we focus here on the case where the noise is additive and Gaussian, and the signal is relatively weak in comparison to the noise. To be precise, suppose we are given an  $m \times n$  data matrix

$$X = M + W \quad \text{with} \quad M = \frac{\text{snr}}{\sqrt{n}} UV^\dagger, \quad (1)$$

where  $\text{snr}$  is a fixed parameter characterizing the signal-to-noise ratio,  $U \in \mathbb{R}^{m \times k}$  and  $V \in \mathbb{R}^{n \times k}$  are generated from some known prior distribution independent of  $n$ , and  $W \in \mathbb{R}^{m \times n}$  is a noise matrix whose entries are independent Gaussians with unit variance. We will refer to this as the *planted model*: it consists of a noisy

---

\*J. Banks is with the Department of Mathematics, University of California, Berkeley, Berkeley, CA, [jess.m.banks@berkeley.edu](mailto:jess.m.banks@berkeley.edu). C. Moore is with the Santa Fe Institute, Santa Fe, NM, [moore@santafe.edu](mailto:moore@santafe.edu). R. Vershynin is with the Department of Mathematics, University of Michigan, Ann Arbor, MI, [romanv@umich.edu](mailto:romanv@umich.edu). N. Verzelen is with UMR 729 MISTEA, INRA, Montpellier. J. Xu is with the Krannert School of Management, Purdue University, West Lafayette, IN 47907, [xu972@purdue.edu](mailto:xu972@purdue.edu). This work was in part presented at the 54th Annual Allerton Conference on Communication, Control, and Computing, September 27-30, 2016, Monticello, IL, USA.

observation  $X$  of a signal matrix  $M$  of rank  $k$ , and may possess additional structure through the priors on  $U$  and  $V$ .

Given the observed matrix  $X$ , the problem of interest is to reconstruct  $M$ , or at least detect that it exists. For simplicity, we will work in the Bayes-optimal case where model parameters such as the true rank and signal-to-noise ratio are known to the estimators. In the low signal-to-noise ratio regime we consider, exact reconstruction of  $M$  is fundamentally impossible (see §2 for more details). Instead, we focus on the following two tasks: first, detecting that the signal  $M$  exists, i.e., telling with high probability whether  $X$  was indeed generated by the planted model as opposed to a *null model* where  $M = 0$  and  $X$  consists only of noise; and second, reconstructing  $M$  to some accuracy better than chance. We define these tasks formally as follows.

**Definition 1** (Detection). *Let  $\mathbb{P}(X)$  be the distribution of  $X$  in the planted model (1), and denote by  $\mathbb{Q}(X)$  the distribution of  $X$  in the null model where  $X = W$ . A test statistic  $\mathcal{T}(X)$  with a threshold  $\epsilon$  achieves detection if  $\lim_{n \rightarrow \infty} [\mathbb{P}(\mathcal{T}(X) < \epsilon) + \mathbb{Q}(\mathcal{T}(X) \geq \tau)] = 0$ , so that the criterion  $\mathcal{T}(X) \geq \epsilon$  determines with high probability whether  $X$  is drawn from  $\mathbb{P}$  or  $\mathbb{Q}$ .*

**Definition 2** (Reconstruction). *An estimator  $\widehat{M} = \widehat{M}(X)$  achieves reconstruction if  $\mathbb{E}_X \|\widehat{M}\|_F^2 = O(n)$  and there exists a constant  $\epsilon > 0$  such that  $\lim_{n \rightarrow \infty} (1/n) \mathbb{E}_{M,X} \langle M, \widehat{M} \rangle \geq \epsilon$ , where  $\langle A, B \rangle = \text{Tr } A^\dagger B$  denotes the matrix inner product and  $\|A\|_F^2 = \langle A, A \rangle$ .*

For many natural problems in this class, it is believed that there is a phase transition, i.e., a threshold value of *snr* below which both tasks are information-theoretically impossible: no test statistic can distinguish the null and planted models, and no estimator can beat the trivial one  $\widehat{M} = 0$ . This threshold is known as the *information-theoretic* threshold and it also depends on the structure of the problem, i.e., on the priors of  $U$  and  $V$ ; if this prior is more strongly structured, we expect the threshold to be lower.

We focus on three cases of (1) which arise in many applications. In *Sparse PCA*,  $k = 1$  and  $U = V = v$  for some vector  $v$ . We further assume that  $v$  is sparse, with a constant fraction of nonzero entries. This corresponds to the *sparse, spiked* Wigner model of [20, 38]. In *Submatrix Localization* (also known as submatrix detection and noisy clustering),  $U = V$  and  $M$  contains  $k \geq 2$  distinct blocks of elevated mean. This model arises in the analysis of social networks and gene expression, see e.g. [31, 15, 24]; it can also be thought of as a Gaussian version of the stochastic block model [19, 18]. Finally, in *Gaussian Mixture Clustering*, there are  $k \geq 2$  clusters, and each row of  $M$  is the center of the cluster to which the corresponding data point belongs. This model has been widely studied, see, e.g., [47, 46, 30, 29, 2].

For each of these three problems, our goal is to compute the information-theoretic threshold, and understand how it scales with the parameters of the problem: for instance, the sparsity of the underlying signal or the number of clusters. In particular, a simple upper bound on the information-theoretic threshold for each of these problems is the point at which spectral algorithms succeed, i.e., the point at which the likely spectrum of  $X$  becomes distinguishable from the spectrum of the random matrix  $W$ . The spectral thresholds for our problems are well known from the theory of Gaussian matrices with low-rank perturbations. However, based on compelling but non-rigorous arguments from statistical physics (e.g. [37, 36]), it has been conjectured that when the signal is sufficiently sparse, or its rank (the number of clusters or blocks) is sufficiently large, the information-theoretic threshold falls strictly below the spectral one.

In this paper, we prove upper and lower bounds on information-theoretic thresholds of all three problems, determining the threshold within a multiplicative constant in interesting regimes. For sparse PCA, we determine the precise threshold in the limit where the signal matrix is very sparse; similarly, for the submatrix localization problem, we determine the threshold when the number of blocks is large. For the clustering problem, our bounds differ by a factor of  $\sqrt{2}$  in the limit where the number of clusters is large. Moreover, our results verify the conjecture that the information-theoretic threshold dips below the spectral one when the signal is sufficiently sparse, or when the number of clusters or blocks is sufficiently large. This corresponds to recent results [1, 9, 17, 23] showing that, in the stochastic block model, the information-theoretic detectability threshold falls below the Kesten-Stigum bound above which efficient spectral and message-passing algorithms succeed [19, 18, 39, 33, 14]. We consider this evidence for the conjecture that these problems possess a ‘hard but detectable’ regime where detection and reconstruction are information-theoretically possible but take at least exponential time. Although our computations are specific to these models, our proof techniques are

quite general and may be applied with mild adjustment to a broad range of similar problems. We present our results in §2, an overview of our proof techniques in §3, and full proofs in §4.

Since the initial posting of this paper as an arXiv preprint, a number of interesting papers [44, 43, 35] have appeared, some extending or improving our results. Sharp lower bounds for sparse PCA were also obtained recently in [43] using a conditional second moment method similar to ours. Complete, but not explicit, characterizations of information-theoretic reconstruction thresholds were obtained in [34, 35] for sparse PCA and submatrix localization through the Guerra interpolation technique and cavity method. However, their characterization of reconstruction thresholds does not directly apply to detection.

## 2 Models and results

### 2.1 Sparse PCA

Consider the following *spiked Wigner* model, where the underlying signal is a rank-one matrix:

$$X = \frac{\lambda}{\sqrt{n}}vv^\dagger + W, \quad (2)$$

Here,  $v \in \mathbb{R}^n$ ,  $\lambda > 0$  and  $W \in \mathbb{R}^{n \times n}$  is a Wigner random matrix with  $W_{ii} \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(0, 2)$  and  $W_{ij} = W_{ji} \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(0, 1)$  for  $i < j$ . We assume  $v$  is drawn from the sparse Rademacher prior, although many alternatives may be imposed. Specifically, for some  $\gamma \in [0, 1]$  the support of  $v$  is drawn uniformly from all  $\binom{n}{\gamma n}$  subsets  $S \subset [n]$  with  $|S| = \gamma n$  (when  $n$  is finite, we assume that  $\gamma n$  is an integer). Once the support is chosen, each nonzero component  $v_i$  is drawn independently and uniformly from  $\{\pm\gamma^{-1/2}\}$ , so that  $\|v\|_2^2 = n$ . When  $\gamma$  is small, the data matrix  $X$  is a sparse, rank-one matrix observed through Gaussian noise.

One natural approach for this problem is PCA: that is, diagonalize  $X$  and use its leading eigenvector  $\hat{v}$  as an estimate of  $v$ . The threshold at which this algorithm succeeds can be computed using the theory of random matrices with rank-one perturbations [8, 42, 11]:

- (1) When  $\lambda > 1$ , the leading eigenvalue of  $X/\sqrt{n}$  converges almost surely to  $\lambda + \lambda^{-1}$ , and  $\langle v, \hat{v} \rangle^2$  converges almost surely to  $1 - \lambda^{-2}$ ; thus PCA succeeds in reconstructing better than chance;
- (2) When  $\lambda \leq 1$ , the leading eigenvalue of  $X/\sqrt{n}$  converges almost surely to 2, and  $\langle v, \hat{v} \rangle^2$  converges almost surely to 0; thus PCA fails to reconstruct better than chance.

Because the leading eigenvalue of  $W$  is 2 w.h.p., detection is only possible when  $\lambda > 1$ . Intuitively, PCA only exploits the low-rank structure of the underlying signal, and not the sparsity of  $v$ ; it is natural to ask whether one can succeed in detection or reconstruction for some  $\lambda < 1$  by taking advantage of this additional structure. Through analysis of an approximate message-passing algorithm and the free energy, the following conjecture was made in statistical physics [38, 34]:

**Conjecture 1.** *Let the computational threshold be the minimum of  $\lambda$  so that reconstruction or detection can be attained in polynomial-time in  $n$  for a given  $\gamma$ . There exists  $\gamma^* \in (0, 1)$  such that*

- (1) *If  $\gamma \geq \gamma^*$ , then both the information-theoretic and computational thresholds are given by  $\lambda = 1$ .*
- (2) *If  $\gamma < \gamma^*$ , then the computational threshold is given by  $\lambda = 1$ , but the information-theoretic threshold for  $\lambda$  is strictly smaller.*

We derive the following upper and lower bounds on the information-theoretic threshold in terms of  $\lambda$  and  $\gamma$ , and confirm that the threshold is  $\lambda = 1$  when  $\gamma$  is relatively large and falls strictly below  $\lambda = 1$  when  $\gamma$  is sufficiently small. Throughout, we use

$$h(\gamma) = -\gamma \log \gamma - (1 - \gamma) \log(1 - \gamma)$$

to denote the entropy function, and  $\mathcal{W}(y)$  for the root  $x$  of  $xe^x = y$ . All our logarithms are natural.

**Theorem 1.** *Let*

$$\lambda^{\text{upper}} = 2\sqrt{h(\gamma) + \gamma \log 2} \quad (3)$$

$$\lambda^{\text{lower}} = \begin{cases} 1 & \gamma \geq 0.6 \\ \sqrt{2\gamma \mathcal{W}\left(\frac{1}{2\gamma\sqrt{e}}\right)} & e^{-41}/81 \leq \gamma < 0.6 \\ \sqrt{4\gamma \left(-\log \gamma - 2.1\sqrt{-2\log \gamma} - \frac{3}{2} \log\left(\frac{3e}{1-\gamma}\right)\right)} & \gamma < e^{-41}/81. \end{cases} \quad (4)$$

*Then detection and reconstruction are information-theoretically possible when  $\lambda > \lambda^{\text{upper}}$  and are impossible when  $\lambda < \lambda^{\text{lower}}$ .*

In our proof, we give tighter lower bounds, but these are analytically convenient.

Note that  $\lambda^{\text{upper}}$  falls below the spectral threshold  $\lambda = 1$  whenever  $\gamma \leq 0.054$ , and  $\lambda^{\text{lower}}$  matches the spectral threshold whenever  $\gamma \geq 0.6$ . Hence, Theorem 1 proves Conjecture 1 on information-theoretic threshold, albeit without pinning down  $\gamma^*$  exactly. In addition, in the limit  $\gamma \rightarrow 0$ , both  $\lambda^{\text{upper}}$  and  $\lambda^{\text{lower}}$  give an information-theoretic threshold of

$$\lambda_c = 2(1 + o_\gamma(1))\sqrt{-\gamma \log \gamma}, \quad (5)$$

determining the threshold fully in the limit where the low-rank matrix is very sparse. Independent of the present work, and building on our preprint [10], Perry et al. [43] obtained the same tight threshold in this limit with a smaller error term. Previous work [16] had determined that threshold scales as  $\lambda = \Theta(\sqrt{-\gamma \log \gamma})$  up to a constant factor.

In passing, we note that there is a very interesting line of work on *exact or approximate support reconstruction* for sparse PCA, i.e., estimating correctly or consistently the positions of non-zeros in  $v$ , in a regime where the size of the support is sublinear in  $n$  (see e.g., [28, 5, 12, 32, 21] and references therein)<sup>1</sup>. In an influential paper [28], it was shown that while the estimate via the classical PCA is inconsistent, a simple diagonal thresholding procedure consistently estimates  $v$  provided that  $v$  is sufficiently sparse. Assuming  $\lambda = \Theta(1)$ , it is later proved in [5] that diagonal thresholding exactly recovers the support of  $v$  with high probability if  $\gamma \lesssim 1/(n \log n)$ , and the information-theoretic threshold for exact support recovery is given by  $\gamma \asymp 1/\log n$  up to a constant factor. In contrast, we focus on the regime where the size of the support is linear in  $n$ , i.e.,  $\gamma = \Theta(1)$ , and  $\lambda = \Theta(1)$ . In this regime it is impossible to correctly or consistently estimate the support of  $v$ , and hence we instead focus on detection and reconstruction better than chance.

## 2.2 Submatrix Localization

In the submatrix localization problem, our task is to detect within a large Gaussian matrix a small block or blocks with atypical mean. Let  $\sigma : [n] \rightarrow [k]$  be a *balanced* partition, i.e. one for which  $|\sigma^{-1}(t)| = n/k$  for all  $t \in [k]$ , chosen uniformly from all such partitions. This terminology will recur through the paper. Construct a  $n \times n$  matrix  $Y$  such that  $Y_{i,j} = \mathbf{1}_{\sigma(i)=\sigma(j)}$ . In the planted model,

$$X = \frac{\mu}{\sqrt{n}} \left( Y - \frac{1}{k} \mathbb{J} \right) + W, \quad (6)$$

where  $W$  is again a Wigner matrix and  $\mathbb{J}$  is the all-ones matrix. In the null model,  $X = W$ . The subtraction of  $\mathbb{J}/k$  centers the signal matrix so that  $\mathbb{E}X = 0$  in both the null and planted models. In the planted model,  $(\mu/\sqrt{n})(Y - \mathbb{J}/k)$  is a rank- $(k-1)$  matrix with the largest  $(k-1)$  eigenvalues all equal to  $\mu\sqrt{n}/k$ , making  $X$  a Wigner matrix with a rank- $(k-1)$  additive perturbation. Matrices of this type exhibit the following spectral phase transition:

<sup>1</sup>To be precise, those references mostly study the spiked Wishart model:  $X = (\lambda/\sqrt{n})uv^\top + W$ , where  $u \in \mathbb{R}^m$  with i.i.d.  $\mathcal{N}(0,1)$  entries and  $W$  is a  $m \times n$  Gaussian matrix with i.i.d.  $\mathcal{N}(0,1)$  entries; the results can be readily extended to the spiked Wigner model.

- (1) When  $\mu > k$ , the  $k$  leading eigenvalues of  $X/\sqrt{n}$  converge to  $\mu/k + k/\mu$  almost surely;
- (2) When  $\mu \leq k$ , the  $k$  leading eigenvalues of  $X/\sqrt{n}$  converge to 2 almost surely.

Hence, it is possible to detect the presence of the additive perturbation from the spectrum of  $X$  alone when  $\mu > k$ . We prove the following upper and lower bounds on the information-theoretic threshold:

**Theorem 2.** *Let*

$$\mu^{\text{upper}} = 2k\sqrt{\frac{\log k}{k-1}} \quad (7)$$

$$\mu^{\text{lower}} = \begin{cases} 2 & k = 2 \\ k\sqrt{\frac{2\log(k-1)}{k-1}} & 3 \leq k \leq \exp(22^4) \\ 2\sqrt{k \log k - 11k \log^{3/4}(k)} & k > \exp(22^4). \end{cases} \quad (8)$$

*Then detection and reconstruction are information-theoretically possible when  $\mu > \mu^{\text{upper}}$  and impossible when  $\mu < \mu^{\text{lower}}$ .*

Note that  $\mu^{\text{upper}}$  dips below the spectral threshold  $\mu = k$  when  $k \geq 11$ , indicating a regime where standard spectral methods fail but detection is information-theoretically possible. Also, Theorem 2 proves the conjecture in [37] that as  $k \rightarrow \infty$ , the information-theoretic threshold is given by  $\mu = 2\sqrt{k \log k}$ .

Previous work in *submatrix detection* and *localization*, also known as *noisy biclustering*, mostly focuses on finding a single submatrix, see, e.g., [31, 15, 24] and the references therein. Notably, [17] considers a general setting where the number of blocks  $k$  could grow with  $n$ , and proves that if  $\mu \geq c\sqrt{k \log n}$  for some large constant  $c$ , then it is informationally possible to exactly reconstruct the support of the planted submatrices with high probability; if  $\mu \leq c'\sqrt{k \log n}$ , then exact support reconstruction is informationally impossible. In our setting,  $\mu = \Theta(1)$  and  $k = \Theta(1)$ , so it is impossible to consistently estimate the support and we instead resort to detection and reconstruction better than the chance.

### 2.3 Gaussian Mixture Clustering

Finally, we study a model of clustering with limited data in high dimension. Let  $v_1, \dots, v_k$  be independently and identically distributed as  $\mathcal{N}(0, k/(k-1) \mathbb{I}_{n,n})$ , and define  $\bar{v} = (1/k) \sum_s v_s$  to be their mean. The scaling of the expected norm of each  $v_s$  with  $k$  ensures that  $\mathbb{E}\|v_s - \bar{v}\|_2^2 = n$  for all  $1 \leq s \leq k$ . For a fixed parameter  $\alpha > 0$ , we then generate  $m = \alpha n$  points  $x_i \in \mathbb{R}^n$  which are partitioned into  $k$  clusters of equal size by a balanced partition  $\sigma : [n] \rightarrow [k]$ , again chosen uniformly at random from all such partitions. For each data point  $i$ , let  $\sigma_i \in [k]$  denote its cluster index, and generate  $x_i$  independently according to Gaussian distribution with mean  $\sqrt{\rho/n}(v_{\sigma_i} - \bar{v})$  and identity covariance matrix, where  $\rho > 0$  is a fixed parameter characterizing the cluster separation. We can put this in the form of model (1) by constructing an  $n \times k$  matrix  $V = [v_1, \dots, v_k]$ , an  $m \times k$  matrix  $S$  with  $S_{i,t} = \mathbf{1}_{\sigma_i=t}$ , and setting

$$X = \sqrt{\frac{\rho}{n}} \left( S - \frac{1}{k} \mathbb{J}_{m,k} \right) V^\dagger + W, \quad (9)$$

where  $W_{i,j} \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)$ . In the null model, there is no cluster structure and  $X = W$ . The subtraction of  $\mathbb{J}_{m,k}/k$  once again centers the signal matrix so that  $\mathbb{E}X = 0$  in both models. The following spectral phase transition follows from the celebrated BBP phase transition [8, 41]:

- (1) When  $\rho\sqrt{\alpha} > k - 1$ , then the largest eigenvalue of  $(1/m)X^\dagger X$  converges to  $(1 + \frac{\rho}{k-1})(1 + \frac{k-1}{\rho\alpha})$  almost surely;
- (2) When  $\rho\sqrt{\alpha} \leq k - 1$ , then the largest eigenvalue of  $(1/m)X^\dagger X$  converges to  $(1 + 1/\sqrt{\alpha})^2$  almost surely.

Thus spectral detection is possible if  $\rho\sqrt{\alpha} > (k - 1)$ .

We prove the following upper and lower bounds on the information-theoretic threshold, which differ by a factor of  $\sqrt{2}$  when  $k$  is large.

**Theorem 3.** *Let*

$$\rho^{\text{upper}} = 2\sqrt{\frac{k \log k}{\alpha}} + 2 \log k \quad (10)$$

$$\rho^{\text{lower}} = \begin{cases} \sqrt{1/\alpha} & k = 2 \\ \sqrt{\frac{2(k-1) \log(k-1)}{\alpha}} & k \geq 3. \end{cases} \quad (11)$$

*Then detection and reconstruction are possible when  $\rho > \rho^{\text{upper}}$  and impossible when  $\rho < \rho^{\text{lower}}$ .*

We conjecture that in the limit  $k \rightarrow \infty$ , the information-theoretic threshold is  $\rho = 2\sqrt{k \log k/\alpha}$ , but we do not find a proof.

Most previous work in Gaussian mixture clustering focuses exact or near-exact reconstruction, see e.g., [46, 30]. As in the §2.1, a popular approach is PCA, which identifies the clusters based on the first  $k$  principal components of the data matrix. It is shown in [47] that PCA allows identification of clusters with a cluster separation  $\sqrt{\rho} = \Omega(k^{1/4} \log n)$  and a sample of size  $m = \Omega(d^3 \log d)$ . This technique was extended to non-Gaussian distributions [29, 2], and for Gaussian, the cluster separation is improved to be  $\sqrt{\rho} = \Omega(\sqrt{k \log n})$  and the sample complexity reduced to  $m = \Omega(k^2 d)$  in [2]. In our setting, since  $\rho$  is a fixed constant, the cluster separation is not sufficient for exact reconstruction and we turn to detection and reconstruction better than chance. Somewhat surprisingly, we find that if the number of clusters is large, clustering is informationally possible even when below the spectral phase transition threshold, and we conjecture that in this regime it is computationally hard to identify the clusters. We note that a similar “hard-but-detectable” regime has been determined empirically in [46].

### 3 Proof techniques

This section gives a brief overview of our proof techniques; the full proof will be presented in the next section.

#### 3.1 The likelihood ratio and hypothesis testing

Detection is a classic hypothesis testing problem. Given a test statistic  $\mathcal{T}(X)$ , we consider its distribution under the planted and null models. If these two distributions are asymptotically disjoint, i.e., their total variation distance tends to 1 in the limit of large datasets, then it is information-theoretically possible to distinguish the two models with high probability by measuring  $\mathcal{T}(X)$ . A classic choice of statistic for binary hypothesis testing is the likelihood ratio,

$$\frac{\mathbb{P}(X)}{\mathbb{Q}(X)} = \frac{\sum_M \mathbb{P}(X, M)}{\mathbb{Q}(X)} = \frac{\sum_M \mathbb{P}(X|M) \mathbb{P}(M)}{\mathbb{Q}(X)}.$$

This object will figure heavily in both our upper and lower bounds. By the Neyman-Pearson lemma [27], the likelihood ratio is the most powerful test statistic of a given significance level; that is, if we set the threshold  $\epsilon$  at the point such that  $\mathbb{Q}(\mathcal{T}(X) < \epsilon) = \alpha$  for any fixed  $\alpha$ , it maximizes  $\mathbb{P}(\mathcal{T}(X) \geq \epsilon)$ .

Our upper bounds do not use the likelihood ratio directly, since it is hard to furnish lower bounds on the typical value of  $\mathbb{P}(X)/\mathbb{Q}(X)$  when  $X$  is drawn from  $\mathbb{P}$ . Instead, we use the generalized likelihood ratio,

$$\max_M \frac{\mathbb{P}(X|M)}{\mathbb{Q}(X)}.$$

In the planted model where the true underlying signal matrix is  $M_0$ , this quantity is trivially bounded below by  $\mathbb{P}(X|M_0)/\mathbb{Q}(X)$ . We will use simple first moment arguments to show that, with high probability in the null model  $\mathbb{Q}$ , this lower bound is not achieved by any  $M$ . An easy extension of this argument shows that, in the planted model, the maximum likelihood estimator (MLE)  $\widehat{M} = \operatorname{argmax}_M \mathbb{P}(X|M)$  has nonzero correlation with  $M_0$ . Thus we can output a good estimate of  $M_0$  by exhaustive search.

The conditional likelihood ratio has a particularly elegant form when the noise is additive and Gaussian. It is first useful to write down the probability distribution of a Wigner random matrix in the space of symmetric matrices (also known as the Gaussian Orthogonal Ensemble) as

$$\mathbb{Q}(W) = \frac{1}{Z_n} e^{-\frac{1}{4}\|W\|_F^2} \quad (12)$$

where  $Z_n$  is a normalization constant depending only on  $n$ . Similarly, if  $W$  is a Gaussian random matrix whose entries are independently distribution as  $\mathcal{N}(0, 1)$ , then

$$\mathbb{Q}(W) = \frac{1}{Z'_n} e^{-\frac{1}{2}\|W\|_F^2}. \quad (13)$$

Thus, for Wigner noise the conditional likelihood ratio is

$$\frac{\mathbb{P}(X|M)}{\mathbb{Q}(X)} = \frac{\mathbb{Q}(X-M)}{\mathbb{Q}(X)} = e^{\frac{1}{4}(\|X\|_F^2 - \|X-M\|_F^2)} = e^{\frac{1}{2}\langle X, M \rangle - \frac{1}{4}\|M\|_F^2} \quad (14)$$

and identical for Gaussian noise except for a factor of two in the exponent.

The conditional *log* likelihood is a weighted sum of the entries of  $X$ , and is therefore itself Gaussian. Our first moment bounds now proceed as follows. In the planted model, when  $X = M_0 + W$ , the conditional log likelihood of the planted signal  $M_0$  is  $\frac{1}{2}\langle W, M_0 \rangle + \frac{1}{4}\|M_0\|_F^2$ . We can use standard Gaussian concentration results to bound the typical deviation of this quantity around its mean of  $\frac{1}{4}\|M_0\|_F^2$ . On the other hand, in the null model where  $X = W$ , the conditional log likelihood of any  $M$  is  $\frac{1}{2}\langle W, M \rangle - \frac{1}{4}\|M\|_F^2$ , and we can combine Gaussian concentration bounds with a union bound over all possible  $M$  to compute when, with high probability in the null model, *no*  $M$  will beat the conditional log likelihood of the planted signal  $M_0$ .

As above, this argument can be nominally modified to show that the MLE estimate is positively correlated with  $M_0$ . This technique must be altered slightly for the case of Gaussian Mixture Clustering, since  $M \propto SV^\dagger$  and  $V$  is chosen from a continuous prior. We could take a union bound over  $V$  by suitably discretizing; instead we use the fact that for any  $S$  we can analytically maximize the conditional likelihood of  $SV^\dagger$  with respect to  $V$  by setting the  $i$ th cluster center to be the empirical center of the data points assigned to cluster  $i$  by  $S$ . This alters the distribution of the likelihood ratio, but we proceed analogously to above with the proper concentration results.

### 3.2 Second moment bounds and contiguity

Intuitively, if the planted model  $\mathbb{P}$  and the null model  $\mathbb{Q}$  have asymptotically disjoint support, then the likelihood ratio  $\mathbb{P}/\mathbb{Q}$  is almost always either very large or very small. In particular, its variance in  $\mathbb{Q}$  must diverge. This suggests that we can derive lower bounds on the threshold by bounding its second moment in  $\mathbb{Q}$ , or equivalently its expectation in  $\mathbb{P}$ . Suppose the second moment is bounded by some constant  $C$ , i.e.,

$$\mathbb{E}_{X \sim \mathbb{Q}} \left[ \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 \right] = \mathbb{E}_{X \sim \mathbb{P}} \left[ \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right] = \int_X dX \frac{\mathbb{P}(X)^2}{\mathbb{Q}(X)} \leq C. \quad (15)$$

This implies a bound on the Kullback-Leibler divergence between  $\mathbb{P}$  and  $\mathbb{Q}$ , since Jensen's inequality gives

$$D_{\text{KL}}(\mathbb{P} \parallel \mathbb{Q}) = \mathbb{E}_{X \sim \mathbb{P}} \log \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \leq \log \mathbb{E}_{X \sim \mathbb{P}} \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \leq \log C = O(1). \quad (16)$$

Moreover, it also implies that detection is impossible. To see this, consider the following definition:

**Definition 3.** Let  $\mathbb{P} = (\mathbb{P}_n), \mathbb{Q} = (\mathbb{Q}_n)$  be sequences of distributions defined on the same sequence of spaces  $\Omega_n$ . We write  $\mathbb{P} \trianglelefteq \mathbb{Q}$ , and say that  $\mathbb{P}$  is contiguous to  $\mathbb{Q}$ , if for any sequence of events  $E = (E_n)$  such that  $\mathbb{Q}(E) \rightarrow 0$ , we also have  $\mathbb{P}(E) \rightarrow 0$ .



If  $\mathbb{P} \trianglelefteq \mathbb{Q}$  then detection is impossible, since no algorithm can return “yes” with high probability (or even positive probability) in the planted model, and “no” with high probability in the null model.

The following simple argument shows that (15) implies  $\mathbb{P} \trianglelefteq \mathbb{Q}$  and hence non-detectability. Let  $E$  be a sequence of events such that  $\mathbb{Q}(E) \rightarrow 0$ , and let  $\mathbf{1}_E$  denote the indicator random variable for  $E$ . Then Cauchy-Schwarz gives

$$\mathbb{P}(E) = \mathbb{E}_{X \sim \mathbb{P}} \mathbf{1}_E = \mathbb{E}_{X \sim \mathbb{Q}} \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \mathbf{1}_E \leq \sqrt{\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2} \times \mathbb{E}_{X \sim \mathbb{Q}} \mathbf{1}_E^2 \leq \sqrt{C\mathbb{Q}(E)} \rightarrow 0. \quad (17)$$

We note that showing that  $\mathbb{Q} \trianglelefteq \mathbb{P}$  often requires additional arguments such as the small subgraph conditioning method [40, 9].

The following lemma gives a general expression for the second moment of the likelihood ratio whenever the model consists of a symmetric signal matrix with Wigner noise or an asymmetric signal matrix with Gaussian noise.

**Lemma 1.** *Let  $\mathbb{P}(X)$  and  $\mathbb{Q}(X)$  be the planted and null models  $X = M + W$  and  $X = W$  respectively, where  $M$  is drawn from some prior over symmetric matrices and  $W$  is a Wigner matrix. Then*

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_{M, M'} e^{\frac{1}{2} \langle M, M' \rangle},$$

where  $M$  and  $M'$  are drawn independently from the prior. Similarly, if  $M$  is drawn from some prior over asymmetric matrices and  $W$  is a Gaussian random matrix,

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_{M, M'} e^{\langle M, M' \rangle}.$$

Thus the second moment method boils down to calculating an exponential moment of the correlation between two independent draws from the prior  $\mathbb{P}(M)$ . Depending on  $\mathbb{P}(M)$ , these draws can correlate in complicated ways, and the remainder of our second moment computations consist of combinatorially analyzing the various events in  $\mathbb{P}(M)$  that give rise to these correlations.

### 3.3 Conditional second moment method

Sometimes, rare events can cause the second moment to explode even when two models are truly contiguous. We circumvent this by computing the second moment conditioned on a sequence of high-probability events  $F$  which rule out the catastrophic rare ones.

In the planted model, these events can occur both in the prior distribution of the planted signal, and in the additive Gaussian noise of the channel. To address atypical events in the prior, we will condition on some high probability property of the signal  $M$ , choosing an appropriate event  $\{M \in F\}$  such that  $\mathbb{P}(F) = 1 + o(1)$ , and form the corresponding conditional distribution

$$\mathbb{P}'(X) = \frac{\mathbb{E}_M[\mathbb{P}(X|M)\mathbf{1}_F]}{\mathbb{P}(F)}. \quad (18)$$

The case where the problematic events occur in the noise distribution is similar; we define an event  $\{X - M \in F_M\}$  such that  $\mathbb{P}(F_M|M) = 1 + o(1)$  uniformly over  $M$ , and the corresponding conditional distribution

$$\mathbb{P}'(X) = \mathbb{E}_M[\mathbb{P}'(X|M)], \quad \text{where} \quad \mathbb{P}'(X|M) = \frac{\mathbb{P}(X|M)\mathbf{1}_{F_M}}{\mathbb{P}(F_M|M)}. \quad (19)$$

In both cases, it is straightforward to show that  $\mathbb{P} \trianglelefteq \mathbb{P}'$ , and therefore that if the conditional second moment  $\mathbb{E}_{X \sim \mathbb{Q}} (\mathbb{P}'(X)/\mathbb{Q}(X))^2$  is bounded, then  $\mathbb{P} \trianglelefteq \mathbb{P}' \trianglelefteq \mathbb{Q}$ .

In the Gaussian mixture clustering problem, we use the first type of conditional second moment method by conditioning on the typical value of cluster centers  $\|V\|_2$ . In the sparse PCA problem and the submatrix localization problem, we instead use the second type of conditional second moment method to close the factor of  $\sqrt{2}$  between the direct second moment lower bound and the first moment upper bound. A similar method was used in [43] to derive the sharp constant of the detection lower bound in the sparse PCA problem. Previous work [6, 49] used the conditional second moment method in deriving the sharp detection threshold in community detection problem.

As a high-level motivation for this conditioning, let  $\mathbb{P}(X)$  and  $\mathbb{Q}(X)$  be the planted and null models  $X = M + W$  and  $X = W$  respectively, where  $M$  is drawn from some prior over symmetric matrices and  $W$  is a Wigner matrix. Using Fubini's theorem,

$$\begin{aligned} \mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 &= \mathbb{E}_{M, M'} \left[ \frac{\mathbb{P}(X|M)\mathbb{P}(X|M')}{\mathbb{Q}^2(X)} \right] \\ &= \mathbb{E}_{M, M'} \mathbb{E}_{X \sim \mathbb{Q}} \left[ e^{-\frac{1}{4}\|M\|_F^2 - \frac{1}{4}\|M'\|_F^2 + \frac{1}{2}\langle X, M+M' \rangle} \right] \\ &= \mathbb{E}_{M, M'} e^{\frac{1}{2}\langle M, M' \rangle} \end{aligned}$$

where  $M$  and  $M'$  are drawn independently from the prior, and in the last line we have carried out the integration with respect to  $X \sim \mathbb{Q}$  directly. The reader may refer to the proof of Lemma 1 for the intervening lines. However, it is possible to decrease the second moment by conditioning on the typical value of  $\langle X, M + M' \rangle$  in the planted model.

Specifically, suppose that  $\mathbb{P}[\langle X, M \rangle \approx \|M\|_F^2 \mid M] = 1 + o(1)$  uniformly over  $M$ . Then, by letting  $F_M = \{\langle X, M \rangle \approx \|M\|_F^2\}$ , we get that

$$\begin{aligned} \mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}'(X)}{\mathbb{Q}(X)} \right)^2 &\approx \mathbb{E}_{M, M'} \mathbb{E}_{X \sim \mathbb{Q}} \left[ \exp\left(-\frac{1}{4}\|M\|_F^2 - \frac{1}{4}\|M'\|_F^2 + \frac{1}{2}\langle X, M + M' \rangle\right) \mathbf{1}_{\{F_M\}} \mathbf{1}_{\{F_{M'}\}} \right] \\ &\approx \mathbb{E}_{M, M'} \mathbb{E}_{X \sim \mathbb{Q}} \left[ \exp\left(-\frac{1}{4}\|M\|_F^2 - \frac{1}{4}\|M'\|_F^2 + \frac{1}{2}\langle X, M + M' \rangle\right) \mathbf{1}_{\{\langle X, M+M' \rangle \approx \|M\|_F^2 + \|M'\|_F^2\}} \right] \\ &\approx \mathbb{E}_{M, M'} \left[ \exp\left(\frac{1}{2}\langle M, M' \rangle - \frac{\|M + M'\|_F^2}{4} \left(1 - \frac{\|M\|_F^2 + \|M'\|_F^2}{\|M + M'\|_F^2}\right)_+\right) \right] \\ &= \mathbb{E}_{M, M'} \left[ \exp\left(\frac{1}{2}\langle M, M' \rangle \frac{\|M\|_F^2 + \|M'\|_F^2}{\|M + M'\|_F^2}\right) \right] \end{aligned}$$

where we used the fact that for  $Y \sim \mathcal{N}(0, \sigma^2)$ ,  $\mathbb{E}[e^Y \mathbf{1}_{\{Y \leq b\}}] \leq \exp(\frac{1}{2}\sigma^2 - \frac{1}{2}\sigma^2(1 - \frac{b}{\sigma^2})_+^2)$  and  $\frac{1}{2}\langle X, M + M' \rangle \sim \mathcal{N}(0, \|M + M'\|_F^2/2)$ . Comparing this conditional second moment with the unconditional one, there is a correction term  $(\|M\|_F^2 + \|M'\|_F^2) / \|M + M'\|_F^2$ , which is most effective if  $M = M'$ . It will turn out that in the sparse PCA problem, when the sparsity  $\gamma \rightarrow 0$  or in the submatrix localization problem, when the number of blocks  $k \rightarrow \infty$ , the second moment is dominated by the event that  $M = M'$ . Hence,

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}'(X)}{\mathbb{Q}(X)} \right)^2 \approx \exp\left(\frac{1}{4}\|M\|_F^2\right) \mathbb{P}_{M, M'}[M = M'],$$

as opposed to  $\exp(\frac{1}{2}\|M\|_F^2) \mathbb{P}_{M, M'}[M = M']$  in the absence of conditioning, a factor of two gain in the exponent. Notice that there is one slight difference between this informal description and our proofs. Instead of conditioning on the typical value of  $\langle X, M \rangle \approx \|M\|_F^2$ , we condition on the typical value of  $\|(X - M)_S\|_2$ , where  $S = \text{supp}(M)$  and  $X_S$  denotes the matrix by setting entries of  $X$  outside of  $S$  to be zero. The reader may refer to Section 4.2.3 and Section 4.3.3 for details.

### 3.4 Non-reconstructibility

Without further embellishment, contiguity is a statement about detection and not reconstruction. It is tempting to believe that whenever contiguity holds—that is, whenever we cannot tell whether a particular sample was generated from the null or planted model—we also cannot infer the planted signal  $M_0$  better than chance. This is not the case. Consider a strange situation in which the null and planted models are identical and noiseless: in  $\mathbb{P}$  we observe  $X = M_0$  drawn from a prior  $\mathbb{P}_0$ , and in  $\mathbb{Q}$  we observe a random draw  $M$  from  $\mathbb{P}_0$ . Detection is patently impossible because these models are contiguous, but if we know that  $X$  is drawn from the planted model, the reconstruction problem is trivial since we observe the ground truth  $M_0$  directly.

However, in the model described by (1) where the noise is additive and Gaussian, we can show that a bounded KL divergence implies that reconstruction is impossible as well. If  $M$  is the planted signal, the mean squared error of an estimator  $\widehat{M}$  is  $\mathbb{E}\|M - \widehat{M}\|_F^2$ . The following theorem shows that whenever the KL divergence  $D_{\text{KL}}(\mathbb{P}\|\mathbb{Q}) = o(n)$ , the estimator  $\widehat{M}$  that minimizes the mean squared error tends to the trivial estimator  $\widehat{M} = 0$ . By (16) a bounded second moment (15) implies a bounded KL divergence; hence a bounded second moment also implies non-reconstruction.

**Theorem 4.** *Let  $\mathbb{P}(X)$  and  $\mathbb{Q}(X)$  be the planted and null models  $X = M + W$  and  $X = W$  respectively, where  $M$  is drawn from some prior such that  $\mathbb{E}[M] = 0$  and  $\lim_{n \rightarrow \infty} (1/n)\mathbb{E}[\|M\|_F^2]$  exists, and where  $W$  is a Gaussian or Wigner matrix. The MMSE estimator in the planted model is the mean of the posterior distribution:  $\widehat{E}(X) = \mathbb{E}[M|X]$ . If the KL divergence  $D_{\text{KL}}(\mathbb{P}\|\mathbb{Q}) = o(n)$ , then*

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{X \sim \mathbb{P}} \|\widehat{E}(X)\|_F^2 = 0. \quad (20)$$

It further follows that for any estimator  $\widehat{M} = \widehat{M}(X)$  such that  $\mathbb{E}_X \|\widehat{M}\|_F^2 = O(n)$ , we have that

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M, X} \langle M, \widehat{M} \rangle = 0. \quad (21)$$

When  $M = (\text{snr}/\sqrt{n})UV^\dagger$ , where the rows of  $U$  and  $V$  are independently and identically distributed according to some priors, then the liminf in (20) and (21) can be replaced by lim.

In cases where we use the conditional second moment method by conditioning on events  $F$  that depend only on the signal  $M$ , i.e.,  $F = \{M \in F\}$ , the conditional distribution  $\mathbb{P}'$  given in (18) is still an additive Gaussian model. Hence, we can still apply Theorem 4 with  $\mathbb{P}'$  and  $\mathbb{Q}$ , concluding that a bounded conditional second moment  $\mathbb{E}_{X \sim \mathbb{Q}} (\mathbb{P}'(X)/\mathbb{Q}(X))^2$  implies non-reconstruction in  $\mathbb{P}'$  and hence non-reconstruction in  $\mathbb{P}$ .

When we need to condition on events  $F_M$  that depend on both  $M$  and  $X$ , i.e.,  $F = \{X - M \in F\}$ , the conditional distribution  $\mathbb{P}'$  given in (19) may no longer be an additive Gaussian model, and hence Theorem 4 cannot be directly invoked. Fortunately, we are able to prove that  $(1/n)D_{\text{KL}}(\mathbb{P}'\|\mathbb{Q})$  is an asymptotic upper bound to  $(1/n)D_{\text{KL}}(\mathbb{P}\|\mathbb{Q})$ . As a consequence, by (16) a bounded conditional second moment  $\mathbb{E}_{X \sim \mathbb{Q}} (\mathbb{P}'(X)/\mathbb{Q}(X))^2$  implies  $D_{\text{KL}}(\mathbb{P}\|\mathbb{Q}) = o(n)$  and hence non-reconstruction in  $\mathbb{P}$  by invoking Theorem 4.

Let  $\|M\|_*$  denote the nuclear norm of  $M$ , which equals to the sum of all the singular values of  $M$ .

**Theorem 5.** *Let  $\mathbb{P}(X)$  and  $\mathbb{Q}(X)$  be the planted and null models  $X = M + W$  and  $X = W$  respectively, where  $M$  is drawn from some prior such that  $\|M\|_2 = O(\sqrt{n})$  and  $\|M\|_* = O(\sqrt{n})$  uniformly over all  $M$ , and where  $W$  is a Gaussian or Wigner matrix. Suppose  $\mathbb{P}'$  is given in (19) with  $\mathbb{P}(F_M|M) = 1 + o(1)$  uniformly over all  $M$ . Then*

$$D_{\text{KL}}(\mathbb{P}\|\mathbb{Q}) \leq D_{\text{KL}}(\mathbb{P}'\|\mathbb{Q}) + o(n).$$

Theorem 5 needs the technical assumptions that  $\|M\|_2 = O(\sqrt{n})$  and  $\|M\|_* = O(\sqrt{n})$ . These assumptions are satisfied in the sparse PCA and submatrix localization problems, but not in the Gaussian mixture clustering problem, which has a prior distribution of unbounded support. This last fact does not impact our results, because the conditioning we employ for the clustering lower bound is on the signal  $M$  and not the noise, meaning that as above we can invoke Theorem 4. To deal with prior distribution of unbounded support, one could employ a truncation argument.

## 4 Proofs

### 4.1 Notation and preliminary lemmas

We begin by proving Lemma 1. The proof is discussed in [26, p.97]; we give the full proof here for completeness.

*Proof of Lemma 1.* We focus on the Wigner noise case as the proof for Gaussian noise case is identical except for a factor of 2. As we noted in equation (14), the conditional likelihood ratio is

$$\frac{\mathbb{P}(X|M)}{\mathbb{Q}(X)} = \frac{\mathbb{Q}(X-M)}{\mathbb{Q}(X)} = e^{\frac{1}{2}\langle X, M \rangle - \frac{1}{4}\|M\|_F^2}. \quad (22)$$

We have  $\mathbb{P}(X) = \mathbb{E}_M \mathbb{P}(X|M)$ . Reversing the order of the expectations and applying (14) gives

$$\begin{aligned} \mathbb{E}_{X \sim \mathbb{Q}} \frac{\mathbb{P}(X)^2}{\mathbb{Q}(X)^2} &= \mathbb{E}_{X \sim \mathbb{Q}} \mathbb{E}_{M, M'} \frac{\mathbb{P}(X|M) \mathbb{P}(X|M')}{\mathbb{Q}(X)^2} \\ &= \mathbb{E}_{M, M'} \mathbb{E}_{X \sim \mathbb{Q}} \frac{\mathbb{P}(X|M) \mathbb{P}(X|M')}{\mathbb{Q}(X)^2} \\ &= \mathbb{E}_{M, M'} e^{-\frac{1}{4}(\|M\|_F^2 + \|M'\|_F^2)} \mathbb{E}_{X \sim \mathbb{Q}} e^{\frac{1}{2}\langle X, M+M' \rangle} \\ &= \mathbb{E}_{M, M'} e^{-\frac{1}{4}(\|M\|_F^2 + \|M'\|_F^2 - \|M+M'\|_F^2)} \\ &= \mathbb{E}_{M, M'} e^{\frac{1}{2}\langle M, M' \rangle}, \end{aligned}$$

where in the second-to-last line we used the moment generating function  $\mathbb{E}_{X \sim \mathbb{Q}} e^{\langle X, A \rangle} = e^{\|A\|_F^2}$ . This completes the proof.  $\square$

In the submatrix localization and Gaussian mixture clustering problems, the underlying low-rank signal matrix  $M$  arises from a balanced partition  $\sigma_0 : [n] \rightarrow [k]$ . In these cases we can equivalently frame results about reconstruction in terms of how well we can infer this original partition. Given  $\sigma_0$  and an estimated partition  $\hat{\sigma}$ , we define the *overlap matrix* as a  $k \times k$  matrix  $\omega(\sigma_0, \hat{\sigma})$  which has  $s, t$  entry equal to the fraction of integers in  $[n]$  assigned by  $\sigma_0$  to group  $s$  and by  $\hat{\sigma}$  to group  $t$ , i.e.

$$\omega(\sigma_0, \hat{\sigma})_{s,t} = \frac{|\sigma_0^{-1}(s) \cap \hat{\sigma}^{-1}(t)|}{n/k}$$

and we drop the dependence on  $\sigma_0$  and  $\hat{\sigma}$  whenever clear. Our assumption that the partitions are balanced implies that  $\omega$  is doubly stochastic.

We can read off scalar measures of the correlation between two partitions  $\sigma$  and  $\tau$ —i.e. of how well we have reconstructed the planted signal—directly from  $\omega$ ; two will be particularly useful. It is typical in the literature to work with what we will call the *trace overlap* between  $\sigma$  and  $\tau$ ,  $T(\sigma, \tau) := \max_{\pi} \text{Tr } \pi \omega(\sigma, \tau)$ , where the maximum is taken over all permutation matrices. In our problems, however, it is analytically more convenient to use  $L(\sigma, \tau) := \|\omega(\sigma, \tau)\|_F^2$ , which we call the  *$L_2$  overlap*. Both  $L(\cdot)$  and  $T(\cdot)$  range from 1, when the two partitions are uncorrelated and  $\omega = \mathbb{J}/k$ , to  $k$ , when they are identical up to a permutation of the group labels, and  $\omega$  is the corresponding permutation matrix. The following lemma states that whenever the  $L_2$  overlap is bounded above 1, the trace overlap is as well.

**Lemma 2.** *For any doubly stochastic matrix  $\omega$ ,  $L(\omega) \leq T(\omega)$ .*

*Proof.* This lemma is an immediate consequence of Birkhoff's theorem. We simply expand  $\omega = \sum_{\pi} a_{\pi} \pi$  as a convex combination of permutation matrices  $\pi$  and observe that

$$L(\omega) = \text{Tr } \omega^\dagger \omega = \sum_{\pi} a_{\pi} \text{Tr } \pi^\dagger \omega \leq \max_{\pi} \text{Tr } \pi^\dagger \omega = T(\omega),$$

the final inequality following from  $\sum_{\pi} a_{\pi} = 1$ .  $\square$

Thus, to show that an estimator  $\hat{\sigma}$  achieves trace overlap with the planted partition  $\sigma_0$  bounded above one, it is sufficient to show that  $L(\hat{\sigma}, \sigma_0) > 1$ .

Finally, in the submatrix localization and Gaussian mixture clustering problems, our second moment calculations will reduce to the computation of  $\mathbb{E}_{\sigma, \tau} [\exp(\xi(\|\omega\|_F^2 - 1))/2]$  where the expectation is over uniformly random pairs of balanced partitions  $\sigma$  and  $\tau$  with overlap matrix  $\omega$ , and  $\xi$  is a parameter corresponding to the signal-to-noise ratio. By [3, Lemma 6], it is straightforward to prove the following lemma giving a sufficient condition to guarantee that this expectation, and therefore the second moment as a whole, is bounded by a constant. We will state the lemma in notation consistent with [3] and discuss afterwards.

**Lemma 3.** *Assume that  $\varphi(\omega)$  is an  $\mathbb{R}$ -valued function of doubly-stochastic  $k \times k$  matrices  $\omega$  with the properties that  $\varphi(\mathbb{J}/k) = 0$  and for some  $\delta > 0$  and every  $k \times k$  doubly stochastic matrices  $\omega$ ,*

$$H(\omega) + \varphi(\omega) \leq H(\mathbb{J}/k) + \varphi(\mathbb{J}/k) - \delta (\|\omega\|_F^2 - 1).$$

Then there exists a constant  $C$ , dependent on  $k$  and  $\delta$ , such that

$$\mathbb{E}_{\sigma, \tau} [e^{n\varphi(\omega)}] \leq C.$$

*Proof.* Let  $\Omega = (\Omega_{st})$  such that  $\Omega_{s,t} = |\sigma^{-1}(s) \cap \tau^{-1}(t)|$ . Then  $\omega = k\Omega/n$ . Denote by  $\mathcal{D}$  the set of all  $k \times k$  matrices  $\Omega = (\Omega_{st})$  of nonnegative integers such that the sum of each row and each column is  $n/k$ . Notice that for a given  $\Omega = (\Omega_{st})$ , there are precisely  $n! / \prod_{s,t} \Omega_{s,t}!$  pairs of balanced partitions  $(\sigma, \tau)$  with overlap matrix given by  $\Omega$ . Hence,

$$\begin{aligned} \mathbb{E}_{\sigma, \tau} [e^{n\varphi(\omega)}] &= \frac{(n/k)!^{2k}}{n!^2} \sum_{\Omega \in \mathcal{D}} \frac{n!}{\prod_{s,t} \Omega_{s,t}!} \exp(n\varphi(\omega)) \\ &\leq k^{-2n} \frac{e^{2k} n^{k-1}}{2\pi k^k} \sum_{\Omega \in \mathcal{D}} \frac{n!}{\prod_{s,t} \Omega_{s,t}!} \exp(\varphi(\omega)), \end{aligned} \quad (23)$$

where we have used Stirling's approximation  $\sqrt{2\pi n}(n/e)^n \leq n! \leq e\sqrt{n}(n/e)^n$  in the last step. In view of the assumption and [3, Lemma 6], there exists a constant  $C' > 0$  dependent on  $\delta$  and  $k$  such that

$$\sum_{\Omega \in \mathcal{D}} \frac{n!}{\prod_{s,t} \Omega_{s,t}!} e^{n\varphi(\omega)} \leq \frac{C'}{n^{k-1}} \left(k^2 e^{\varphi(\mathbb{J}/k)}\right)^n = \frac{C'}{n^{k-1}} k^{2n}.$$

Combing the last displayed equation with (23) yields that

$$\mathbb{E}_{\sigma, \tau} [e^{n\varphi(\omega)}] \leq \frac{C' e^{2k}}{2\pi k^k} := C,$$

which completes the proof.  $\square$

Let us unpack the conditions of the above lemma in the context of our problems. For us,  $\varphi(\omega) = (\xi/2)(\|\omega\|_F^2 - 1)$ , and since  $H(\mathbb{J}/k) = \log k$  and  $\|\mathbb{J}/k\|_F^2 = 1$ , it is in fact sufficient to study the function

$$\Phi(\omega) = H(\omega) - \log k + \frac{\xi}{2} (\|\omega\|_F^2 - 1). \quad (24)$$

In particular, the hypotheses of Lemma 3 are satisfied provided that  $\Phi(\omega) \leq -\delta(\|\omega\|_F^2 - 1)$  for every doubly stochastic matrix  $\omega$  and some  $\delta > 0$ . This is the case whenever  $\xi$  is sufficiently small. On the other hand, in the limit  $\xi \rightarrow \infty$ ,  $\Phi(\omega)$  is maximized by any permutation matrix, the doubly stochastic matrices with maximal Frobenius norm and minimal entropy. It has been conjectured that, for general  $\xi$ , the maximizer is a convex combination of  $\mathbb{J}/k$  and a permutation matrix, but this has not been proved.

The precise value of  $\xi$  up to which  $\Phi(\omega)$  is maximized by  $\omega = \mathbb{J}/k$  is not known. Fortunately, Achlioptas and Naor, in their second moment lower bound on the  $k$ -colorability threshold for Erdős-Rényi graphs [3], proved an upper bound on  $\Phi$  by relaxing to singly stochastic matrices.

**Lemma 4.** [3, Theorems 7,9] When  $\xi < 2 \log(k-1)/(k-1)$ ,  $\operatorname{argmax} \Phi(\omega) = \mathbb{J}/k$ .

One can obtain an even tighter bound in the special case  $k = 2$ . Recall that the  $2 \times 2$  doubly stochastic matrices are a one-parameter family—since the upper left entry uniquely determines the matrix. Consequently we can rewrite  $\Phi(\omega)$  in (24) as

$$\Phi(x) = h(x) + \frac{\xi}{2}(4x^2 - 4x + 1) - \log 2.$$

The second derivative of  $\Phi(x)$  is  $4\xi - 1/(x(1-x))$ . Hence, if  $\xi < 1$ , then  $\Phi(x)$  is strictly concave in  $x$  and  $\operatorname{argmax}_x \Phi(x) = 1/2$ .

**Lemma 5.** When  $k = 2$  and  $\xi < 1$ ,  $\operatorname{argmax}_\omega \Phi(\omega) = \mathbb{J}/2$ .

## 4.2 Sparse PCA

In this section we prove Theorem 1. First, we show that detection and reconstruction are possible if  $\lambda > \lambda^{\text{upper}}$  using a first moment argument as described in Section 3.1: specifically, if  $\lambda > \lambda^{\text{upper}}$  then with high probability in  $\mathbb{Q}$  there are no  $v$  with likelihood as high as that of the ground truth  $v_0$ , and with high probability in  $\mathbb{P}$  all such  $v$  are correlated with  $v_0$ . Then, we prove that the second moment of the likelihood ratio is bounded if  $\lambda < \lambda^{\text{lower}}$ ; as discussed in Section 3.2, this implies that detection and reconstruction are impossible if  $\lambda < \lambda^{\text{lower}}$ .

### 4.2.1 First moment upper bound for sparse PCA

Recall that  $X = (\lambda/\sqrt{n})v_0v_0^\dagger + W$ , where  $v_0$  is drawn uniformly from  $\mathcal{V} = \{v \in \{\pm\gamma^{-1/2}, 0\} : |\operatorname{supp}(v)| = \gamma n\}$  and  $W$  is a Wigner matrix. For any  $v \in \mathcal{V}$ , using (14), the conditional log likelihood ratio is

$$\begin{aligned} \log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} &= \frac{1}{2} \langle M, X \rangle - \frac{1}{4} \|M\|_F^2 \\ &= \frac{1}{2} \frac{\lambda}{\sqrt{n}} \langle v, Xv \rangle - \frac{1}{4} \frac{\lambda^2}{n} \|v\|_2^4 \\ &= \frac{1}{2} \frac{\lambda}{\sqrt{n}} \langle v, Xv \rangle - \frac{\lambda^2 n}{4}. \end{aligned}$$

In the null model,  $X = W$  and  $\langle v, Xv \rangle$  is distributed as  $\mathcal{N}(0, 2n^2)$ , giving

$$\log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} \sim \mathcal{N}\left(-\frac{\lambda^2 n}{4}, \frac{\lambda^2 n}{2}\right). \quad (25)$$

On the other hand, in the planted model

$$\langle v, Xv \rangle = \langle v, Wv \rangle + \frac{\lambda}{\sqrt{n}} \langle v, v_0v_0^\dagger v \rangle = \langle v, Wv \rangle + \frac{\lambda}{\sqrt{n}} \langle v, v_0 \rangle^2,$$

so the conditional log likelihood has a distribution which depends on the inner product between  $v$  and the ground truth  $v_0$ . We write this inner product as  $\langle v, v_0 \rangle = \theta n$ , for  $\theta \in [-1, 1]$  so that

$$\log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} \sim \mathcal{N}\left(\frac{(2\theta^2 - 1)\lambda^2 n}{4}, \frac{\lambda^2 n}{2}\right)$$

Whenever  $\theta = 0$  so that  $v$  is uncorrelated with  $v_0$ , this distribution is identical to that in the null model.

To show that detection is possible above (3), notice that in the planted model the maximum likelihood estimate  $\hat{v} = \operatorname{argmax}_{v \in \mathcal{V}} \mathbb{P}(X|v)$  has conditional log likelihood at least as large as the ground truth  $v_0$ . By standard Gaussian tail bounds and setting  $\theta = \pm 1$  above,

$$\mathbb{P} \left[ \log \frac{\mathbb{P}(X|v_0)}{\mathbb{Q}(X)} \leq \frac{\lambda^2 n}{4} - O(\sqrt{n \log n}) \right] \leq n^{-\Omega(1)}.$$

In the null model, Gaussian tail bounds give us

$$\mathbb{Q} \left[ \log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} \geq \frac{\lambda^2 n}{4} - O(\sqrt{n \log n}) \right] \leq \exp \left( -\frac{\lambda^2 n}{4} + O(\sqrt{n \log n}) \right).$$

Taking the union bound over all  $2^{\gamma n} \binom{n}{\gamma n}$  possible  $v$  and invoking Stirling's formula  $\binom{n}{\gamma n} \leq e^{nh(\gamma)}$ , we have

$$\mathbb{Q} \left[ \max_{v \in \mathcal{V}} \log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} \geq \frac{\lambda^2 n}{4} - O(\sqrt{n \log n}) \right] \leq \exp^n \left( -\frac{\lambda^2 n}{4} + h(\gamma) + \gamma \log 2 \right) + O(\sqrt{n \log n}). \quad (26)$$

When this expression is  $e^{-\Omega(n)}$ , we can with high probability distinguish the null and planted models with the generalized likelihood test. This occurs when  $\lambda < \lambda^{\text{upper}}$  where  $\lambda^{\text{upper}}$  is defined in (3), i.e.,

$$\frac{\lambda^2}{4} > h(\gamma) + \gamma \log 2. \quad (27)$$

Next, we prove that reconstruction is also possible above this bound. Suppose that  $X$  is generated from the planted model, and that  $\langle \hat{v}, v_0 \rangle = \theta n$ . We bound the probability that  $\hat{v}$  has conditional log likelihood as large as  $v_0$  with a union bound over  $\hat{v}$  correlated with  $v_0$ , but we bound the number of such vectors generously as  $2^{\gamma n} \binom{n}{\gamma n}$  once again. Combining this with the Gaussian tail bound and invoking Stirling gives

$$\begin{aligned} \mathbb{P} \left[ \max_{v \in \mathcal{V}: \langle v, v_0 \rangle \leq \theta n} \log \frac{\mathbb{P}(X|v)}{\mathbb{Q}(X)} > \frac{\lambda^2 n}{4} + O(\sqrt{n \log n}) \right] \\ \leq \exp \left[ n \left( \frac{(2\theta^2 - 1)\lambda^2}{4} + h(\gamma) + \gamma \log 2 \right) + O(\sqrt{n \log n}) \right]. \end{aligned}$$

Since the coefficient of  $n$  in the exponent is an analytic function of  $\theta$ , whenever (27) holds, the RHS of the last displayed equation is exponentially small unless  $\theta^2 > \varepsilon$  for some constant  $\varepsilon > 0$ . Therefore, with high probability the MLE estimator has overlap  $(\langle \hat{v}, v_0 \rangle / n)^2 = \theta^2 > \varepsilon > 0$  with the ground truth. Moreover, if  $\widehat{M} = (\lambda / \sqrt{n}) \widehat{v} \widehat{v}^\dagger$ , then  $\|\widehat{M}\|_F^2 = (\lambda^2 / n) \|\widehat{v}\|_2^4 = \lambda^2 n$ ; moreover, with high probability  $\langle \widehat{M}, M \rangle = (\lambda^2 / n) \langle \widehat{v}, v_0 \rangle^2 > \varepsilon \lambda^2 n$ . Hence, the estimator  $\widehat{M}$  reconstructs the signal matrix better than chance.

#### 4.2.2 Second moment lower bound for sparse PCA

In this subsection, we use the second moment method to prove a lower bound on the detectability transition for sparse PCA. We assume  $\lambda < 1$  throughout the proof; the boundary case  $\lambda = 1$  is not addressed. In the planted model, the signal matrix is  $M = (\lambda / \sqrt{n}) v v^\dagger$ , and in the null model it is zero. In both cases, we have  $X = M + W$  where  $W$  is a Wigner noise matrix. Applying Lemma 1, the second moment (where  $X$  is drawn from the null model) is

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_{v, w} e^{\frac{\lambda^2}{2n} \langle v, w \rangle^2}, \quad (28)$$

where  $v$  and  $w$  are drawn independently from the prior.

Denote the overlap  $z = |\text{supp}(v) \cap \text{supp}(w)|$  and let  $t$  be the difference between the number of indices in that intersection where  $v$  and  $w$  agree and the number of indices where they disagree. In that case,

$$\langle v, w \rangle = \frac{t}{\gamma}.$$

Then,  $z$  follows an hypergeometric distribution with parameter  $(n, \gamma n, \gamma n)$  and given  $z$ ,  $t$  is distributed as a sum of  $z$  independent Rademacher random variables. If we write

$$\eta = \lambda / \gamma, \quad (29)$$

then

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \right].$$

We know from [4, p.173] that  $z$  has the same distribution as the random variable  $\mathbb{E}[\bar{z} | \mathcal{B}_n]$  where  $\bar{z}$  is a Binomial random variable with parameters  $(\gamma n, \gamma)$  and  $\mathcal{B}_n$  some suitable  $\sigma$ -algebra. Given  $\bar{z}$ , let  $\bar{t}$  be distributed as a sum of  $\bar{z}$  independent Rademacher variables.

**Lemma 6.** *Let  $(\epsilon_i)_{i \geq 1}$  denote a sequence of independent Rademacher random variables. For any  $a > 0$ , let  $g$  be the piecewise linear function on  $[1, \infty)$  such that, for any positive integer  $z$ ,  $g(z) = \mathbb{E}_\epsilon \exp[a(\sum_{i=1}^z \epsilon_i)^2]$ . Then, the function  $g$  is convex.*

*Proof.* Since  $g$  is convex and continuously differentiable on each interval of the form  $(z, z+1)$  where  $z$  is an integer, we only have to prove that its left derivative is less or equal to its right derivative at  $z+1$ . This is equivalent to showing that  $g(z+2) + g(z) \geq 2g(z+1)$ . Define  $u = \sum_{i=1}^z \epsilon_i$ . Conditioning with respect to  $u$ , we obtain  $g(z+1) = \mathbb{E}_u [e^{au^2+a} \cosh 2au]$  and  $g(z+2) = \mathbb{E}_u [e^{au^2} [0.5e^{4a} \cosh 4au + 0.5]]$ . Hence, it suffices to prove that, for any  $u$ ,

$$e^a \cosh 2au \leq \frac{1}{4} e^{4a} \cosh 4au + \frac{3}{4}.$$

For  $x \geq 0$ , let  $h(x) = e^{ax} \cosh(2au\sqrt{x})$ . Since  $h$  is a product of two increasing convex functions,  $h$  is also convex. This implies the above inequality and concludes the proof.  $\square$

By Jensen's inequality, it follows that

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 \leq \mathbb{E}_{\bar{t}} \left[ e^{\frac{\eta^2 \bar{t}^2}{2n}} \right]. \quad (30)$$

To simplify the notation, we simply write  $z$  and  $t$  instead of  $\bar{z}$  and  $\bar{t}$  in the sequel. Note that

$$\begin{aligned} \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] &= \sum_{u=0}^z e^{\frac{\eta^2 u^2}{2n}} (\mathbb{P}_t[|t| \geq u \mid z] - \mathbb{P}_t[|t| \geq u+1 \mid z]) \\ &\leq 1 + \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{\eta^2 u^2}{2n}} \mathbb{P}_t[|t| \geq u \mid z] \end{aligned} \quad (31)$$

$$\leq 1 + 2 \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{u^2}{2} \left( \frac{\eta^2}{n} - \frac{1}{z} \right)}, \quad (32)$$

where we applied Hoeffding's inequality:  $\mathbb{P}_t(|t| \geq u \mid z) \leq 2e^{-u^2/(2z)}$  in the last line.

We consider three subcases depending on the value of  $z$ .

**Case 1:** If  $z \leq (n/\eta^2)\lambda$ ,

$$\begin{aligned} \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] &\leq 1 + 2 \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{u^2}{2} \left( \frac{\eta^2}{n} - \frac{1}{z} \right)} \leq 1 + O(1) \int_0^\infty \frac{\eta^2 u}{n} e^{-\frac{u^2}{2} \left( \frac{1}{z} - \frac{\eta^2}{n} \right)} du \\ &\leq O(1) \left[ 1 + \frac{\eta^2}{n/z - \eta^2} \right] \leq O \left( \frac{1}{1 - \lambda} \right), \end{aligned} \quad (33)$$

where we used  $z \leq \frac{n\lambda}{\eta^2}$  in the last inequality.



**Case 2:** If  $(n/\eta^2)\lambda < z \leq n/\eta^2$ , we have

$$\begin{aligned} \mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\frac{n}{\eta^2}\lambda, \frac{n}{\eta^2}]} \right] &\leq \mathbb{E}_z \left[ \left( 1 + 2 \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{u^2}{2} \left( \frac{\eta^2}{n} - \frac{1}{z} \right)} \right) \mathbf{1}_{z \in (\frac{n}{\eta^2}\lambda, \frac{n}{\eta^2}]} \right] \\ &\leq \mathbb{E}_z \left[ \left( 1 + \frac{\eta^2 (z+1)^2}{n} \right) \mathbf{1}_{z \in (\frac{n}{\eta^2}\lambda, \frac{n}{\eta^2}]} \right] \\ &\leq O(1 + n\gamma) \mathbb{P}_z \left[ z \geq \frac{n}{\eta^2} \lambda \right], \end{aligned}$$

where in the second inequality we bound  $\exp(u^2/2 (\eta^2/n - 1/z)) \leq 1$  and in the third inequality we use  $z \leq n/\eta^2$  and  $z \leq n\gamma$ . Since  $\lambda/\eta^2 = \gamma^2/\lambda > \gamma^2$  and  $z \sim \text{Bin}(\gamma n, \gamma)$ , Bernstein's inequality implies that  $\mathbb{P}_z [z \geq (n/\eta^2)\lambda]$  is exponentially small. Therefore,

$$\mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\frac{n}{\eta^2}\lambda, \frac{n}{\eta^2}]} \right] = o(1). \quad (34)$$

**Case 3:** Finally, if  $n/\eta^2 < z \leq \gamma n$ , then  $\exp(u^2/2 (\eta^2/n - 1/z))$  is exponentially large in  $u$ . Thus to show that the second moment is finite, we need to use the fact that  $\mathbb{P}_z [z \geq a]$  for  $a > n/\eta^2$  is exponentially small. When  $z > n/\eta^2$ , the bound in(32) implies that

$$\mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \leq 1 + 2e^{\frac{z^2 \eta^2}{2n} - \frac{z}{2}} \sum_{u=1}^z \frac{\eta^2 u}{n} \leq O(n) \exp \left[ \frac{z^2 \eta^2}{2n} - \frac{z}{2} \right],$$

where we applied  $z \leq \gamma n$  and the second inequality holds due to  $\lambda < 1$ . For any  $0 < p_0 < p_1 \leq 1$ , define

$$h_{p_0}(p_1) = p_1 \log\left(\frac{p_1}{p_0}\right) + (1 - p_1) \log\left(\frac{1 - p_1}{1 - p_0}\right), \quad (35)$$

the KL-divergence between Bernoulli random variables with parameters  $p_0$  and  $p_1$  respectively. Chernoff's inequality implies that for any  $a \geq \gamma^2 n$ ,

$$\mathbb{P}_z [z \geq a] \leq \exp \left[ -\gamma n h_\gamma \left( \frac{a}{\gamma n} \right) \right].$$

As a consequence,

$$\begin{aligned} \mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\frac{n}{\eta^2}, \gamma n]} \right] &\leq O(n) \sum_{z=n/\eta^2}^{\gamma n} \exp \left[ \frac{z^2 \eta^2}{2n} - \frac{z}{2} - \gamma n h_\gamma \left( \frac{z}{\gamma n} \right) \right] \\ &\leq O(n^2) \exp \left[ n \sup_{\zeta \in [1/\eta^2, \gamma]} \psi(\zeta) \right], \end{aligned}$$

where

$$\psi(\zeta) = \frac{(\eta^2 \zeta - 1)\zeta}{2} - \gamma h_\gamma(\zeta/\gamma) = \frac{(\eta^2 \zeta - 1)\zeta}{2} - \zeta \log\left(\frac{\zeta}{\gamma}\right) - (\gamma - \zeta) \log\left(\frac{\gamma - \zeta}{1 - \gamma}\right) + \gamma \log(\gamma), \quad (36)$$

Then, we need to show that

$$\psi(\zeta) < 0 \quad \text{for all } \zeta \in [\gamma^2/\lambda^2, \gamma], \quad (37)$$

Note that this property is trivial when  $\gamma/\lambda^2 > 1$  so that we may restrict our attention to  $\gamma/\lambda^2 \leq 1$ . Since  $\lambda < 1$ , it follows that  $\psi(\gamma^2/\lambda^2) = -\gamma h_\gamma(\gamma/\lambda^2) < 0$ . For  $\zeta = \gamma$ ,  $\psi(\zeta) = (\lambda^2 - \gamma)/2 - \gamma \log(1/\gamma)$ , which is negative for

$$\lambda < \sqrt{2\gamma(-\log \gamma + 1/2)}. \quad (38)$$

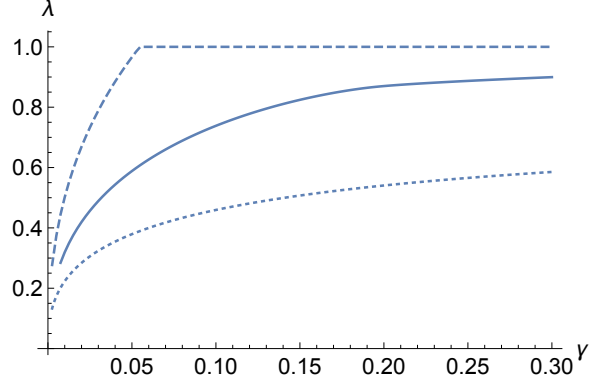


Figure 1: Upper and lower bounds on the information-theoretic detectability threshold in sparse PCA. Our upper bound (dashed) shows that the detectability threshold is strictly below the spectral threshold  $\lambda = \gamma\eta = 1$  for  $\gamma < 0.054$ . The solid line shows the lower bound given by (37), and the dotted line shows the simpler lower bound given by (40). Notice that the solid line is not touching the dashed line even in the limit  $\gamma \rightarrow 0$ ; there is a gap of  $\sqrt{2}$ .

Moreover, the second derivative of  $\psi$  has at most two roots. It follows that  $\psi(\zeta)$  can have at most three local minima or maxima occurring at the roots of

$$\psi' = \eta^2 \zeta - \frac{1}{2} - \log \left( \frac{\zeta(1-\gamma)}{\gamma(\gamma-\zeta)} \right).$$

Figure 1 shows  $\lambda$  as a function of  $\gamma$ , illustrating in particular that it rapidly approaches the spectral transition  $\lambda = 1$  as  $\gamma$  approaches 1.

We now derive an analytic bound of  $\psi$ . For  $\zeta \in (\gamma^2/\lambda^2, \gamma]$ ,

$$\begin{aligned} \psi(\zeta) &\leq \zeta \frac{\eta^2 \gamma - 1}{2} - \zeta \log \left( \frac{\zeta}{\gamma^2} \right) + \gamma(1 - \zeta/\gamma) \log \left( \frac{1-\gamma}{1-\zeta/\gamma} \right) \\ &\leq \zeta \frac{\eta^2 \gamma - 1}{2} - \zeta \log \left( \frac{\zeta}{\gamma^2} \right) + \zeta - \gamma^2 \\ &\leq \zeta \left( \frac{\lambda^2/\gamma + 1}{2} + 2 \log \lambda \right), \end{aligned}$$

where we used  $\log(1+x) \leq x$  in the second line and  $\zeta \geq \gamma^2/\lambda^2 \geq \gamma^2$  in the third line.

Therefore,  $\mathbb{E}_z[\mathbb{E}_t[\exp(\eta^2 t^2/2n) | z] \mathbf{1}_{z \in (n/\eta^2, \gamma n)}]$ , and hence the second moment, are bounded as long as

$$\log \lambda^2 + \frac{\lambda^2/\gamma + 1}{2} < 0. \quad (39)$$

If, for any  $y > 0$ , we use  $\mathcal{W}(y)$  to denote the root  $x$  of  $xe^x = y$ , (39) holds whenever

$$\lambda < \sqrt{2\gamma \mathcal{W} \left( \frac{1}{2\sqrt{e}\gamma} \right)}. \quad (40)$$

As  $y \rightarrow \infty$ , we have  $\mathcal{W}(y) \sim \log y$ . Thus as  $\gamma \rightarrow 0$ , this lower bound approaches

$$\lambda^{\text{lower}} \sim \sqrt{2\gamma \log \frac{1}{2\sqrt{e}\gamma}}. \quad (41)$$

Let us now turn to regime  $\gamma > 0.6$ , where we will show the second moment is bounded whenever  $\lambda < 1$ . In view of (33) and (34), it suffices to prove that

$$\mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\gamma^2 n, \gamma n]} \right] = O(1),$$

whenever  $\lambda < 1$ . From (31), we have

$$\begin{aligned} & \mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\gamma^2 n, \gamma n]} \right] \\ & \leq \mathbb{E}_z \left[ 1 + \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{\eta^2 u^2}{2n}} \mathbb{P}_t [|t| \geq u \mid z] \mathbf{1}_{z \in (\gamma^2 n, \gamma n]} \right] \\ & \stackrel{(a)}{\leq} 1 + \sum_{z=\gamma^2 n}^{\gamma n} \sum_{u=1}^z \frac{\eta^2 u}{n} e^{\frac{\eta^2 u^2}{2n}} \mathbb{P}_t [|t| \geq u \mid z] \binom{\gamma n}{z} \gamma^z (1-\gamma)^{\gamma n - z} \\ & \stackrel{(b)}{\leq} 1 + O(1) \sum_{z=\gamma^2 n}^{\gamma n} \sum_{u=1}^z \frac{\eta^2 u}{n \sqrt{(z(1-z/\gamma n)) \vee 1}} e^{-\frac{(1-\lambda^2)u^2}{2n\gamma^2}} \exp \left[ \frac{u^2}{2n\gamma^2} + zh \left( \frac{u}{2z} + \frac{1}{2} \right) - z \log(2) - \gamma n h_\gamma \left( \frac{z}{\gamma n} \right) \right], \end{aligned}$$

where we used in (a) that  $z$  follows a Binomial distribution. In step (b),  $h_\gamma$  is defined as in (35), and we have used the facts that

$$\mathbb{P}_t [|t| \geq u \mid z] = 2 \Pr \left[ \text{Bin}(z, 1/2) \geq \frac{u+z}{2} \right] \leq 2 \exp \left( -zh_{1/2} \left( \frac{u+z}{2z} \right) \right)$$

and

$$\binom{\gamma n}{z} \leq \left( \frac{1}{\sqrt{2\pi z(1-z/(\gamma n))}} \wedge 1 \right) \exp \left( \gamma n h \left( \frac{z}{\gamma n} \right) \right)$$

for  $z \leq \gamma n$ .

Expanding as Taylor series, we have

$$h(u) \leq \log(2) - 2(u-1/2)^2 - \frac{4}{3}(u-1/2)^4 \quad \text{and} \quad h_\gamma(u) \geq \frac{(u-\gamma)^2}{2\gamma(1-\gamma)}.$$

This yields

$$\begin{aligned} & \mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\gamma^2 n, \gamma n]} \right] \\ & \leq 1 + O(1) \sum_{z=\gamma^2 n}^{\gamma n} \sum_{u=1}^z \frac{\eta^2 u}{n \sqrt{(z(1-z/\gamma n)) \vee 1}} e^{-\frac{(1-\lambda^2)u^2}{2n\gamma^2}} \exp \left[ n \underbrace{\left( \frac{u^2}{2(\gamma n)^2} - \frac{u^2}{2zn} - \frac{u^4}{12z^3 n} - \frac{(z/(\gamma n) - \gamma)^2}{2(1-\gamma)} \right)}_{= (I)} \right] \end{aligned}$$

We focus on the term (I), which is maximized with respect to  $u$  by choosing

$$u^2 = \frac{1}{2} \times 12z^3 n \left( \frac{1}{2\gamma^2 n^2} - \frac{1}{2zn} \right).$$

Hence,

$$\begin{aligned}
(I) &\leq \frac{3}{4} \frac{z^3}{\gamma^2 n^3} \left( \frac{1}{\gamma} - \frac{\gamma n}{z} \right)^2 - \frac{(z/(\gamma n) - \gamma)^2}{2(1-\gamma)} \\
&\leq \left[ \frac{3z}{4\gamma^2 n} - \frac{1}{2(1-\gamma)} \right] \left( \frac{z}{\gamma n} - \gamma \right)^2 \\
&\leq \left[ \frac{3}{4\gamma} - \frac{1}{2(1-\gamma)} \right] \left( \frac{z}{\gamma n} - \gamma \right)^2,
\end{aligned}$$

since  $z \leq \gamma n$ . The above expression is negative as soon as  $\gamma > 0.6$ . For such a choice of  $\gamma$ , there exist two positive constants  $c_1$  and  $c_2$  such that

$$\mathbb{E}_z \left[ \mathbb{E}_t \left[ e^{\frac{y^2 t^2}{2n}} \mid z \right] \mathbf{1}_{z \in (\gamma^2 n, \gamma n)} \right] \leq 1 + O(1) \sum_{z=\gamma^2 n}^{\gamma n} \sum_{u=1}^z \frac{u}{n \sqrt{(z(1-z/\gamma n)) \vee 1}} e^{-c_1 \frac{u^2}{n}} e^{-c_2 \frac{(z-\gamma^2 n)^2}{n}} = O(1),$$

where the last equality holds because  $\sum_{u=1}^z (u/n) e^{-c_1 u^2/n} = O(n)$ . This completes the proof in the regime  $\gamma > 0.6$ .

The conclusion for reconstruction follows by applying (16) and Theorem 4. Furthermore, for any estimator  $\widehat{v} \in \mathcal{V}$  of  $v$ , applying Theorem 4 to the estimator  $\widehat{M} = (\lambda/\sqrt{n})\widehat{v}\widehat{v}^\dagger$  gives

$$\frac{1}{n^2} \mathbb{E} \langle v, \widehat{v} \rangle^2 = \frac{1}{n\lambda^2} \mathbb{E} \langle M, \widehat{M} \rangle = o(1).$$

Thus we can neither reconstruct the signal matrix nor the sparse vector  $v$ .

### 4.2.3 Conditional second moment lower bound for sparse PCA

Bounding the second moment is too rough to pinpoint the exact information-theoretical threshold for small  $\gamma$ . Indeed, there is asymptotically an  $\sqrt{2}$  gap between the  $\lambda^{\text{lower}}$  and  $\lambda^{\text{upper}}$ . To recover the exact constant, we shall bound some conditional second moment. Throughout this proof, we consider  $\lambda$  such that

$$\lambda^2 < 4\gamma \left[ \log \left( \frac{1}{\gamma} \right) - 2.1 \sqrt{2 \log \left( \frac{1}{\gamma} \right)} - \frac{3}{2} \log \left( \frac{3e}{1-\gamma} \right) \right] \leq 4\gamma \log \left( \frac{1}{\gamma} \right). \quad (42)$$

We shall restrict our attention to  $\gamma$  small enough that  $\log(1/\gamma) > 41 + \log(81)$ , which is equivalent to

$$9\sqrt{\gamma} < \sqrt{2\gamma \mathcal{W} \left( \frac{1}{2\sqrt{e}\gamma} \right)}. \quad (43)$$

For any set  $a \subset [n]$  and any square matrix  $X$ , let  $X_a$  refer to the matrix whose entries outside  $a \times a$  have been set to zero. Given a vector  $v$ , we define the event  $\Gamma_v$  by

$$\Gamma_v := \left\{ \left\| \left( X - \frac{\lambda}{\sqrt{n}} v v^\dagger \right)_{\text{supp}(v)} \right\|_2 \leq 2.1 \sqrt{n\gamma} \right\}. \quad (44)$$

Under  $\mathbb{P}(\cdot|v)$ , the  $\text{supp}(v) \times \text{supp}(v)$  submatrix of  $X - \frac{\lambda}{\sqrt{n}} v v^\dagger$  is distributed as a Wigner Matrix. By [7, Theorem 5.1], its spectral norm rescaled by  $\sqrt{\gamma n}$  converges almost surely to 2 when  $n \rightarrow \infty$ , and so  $\mathbb{P}(\Gamma_v|v) = 1 + o(1)$  uniformly with respect to  $v$ . The event  $\Gamma_v$  means that the noise added to the nonzero entries of  $v v^\dagger$  is not uncharacteristically large.

Next, we condition on the high probability events  $\Gamma_v$  and define the conditional probability distribution

$$\mathbb{P}'(X) = \mathbb{E}_v \left[ \mathbb{P}(X|v) \frac{\mathbf{1}_{\Gamma_v}}{\mathbb{P}(\Gamma_v|v)} \right]. \quad (45)$$

The conditional second moment decomposes as

$$\begin{aligned} \mathbb{E}_{X \sim \mathbb{Q}} \left[ \frac{\mathbb{P}'^2(X)}{\mathbb{Q}^2(X)} \right] &= \mathbb{E}_{v,w} \left[ \mathbb{E}_{X \sim \mathbb{Q}} \left[ \frac{\mathbb{P}(X|v)\mathbb{P}(X|w)}{\mathbb{Q}^2(X)} \frac{\mathbf{1}_{\Gamma_v}\mathbf{1}_{\Gamma_w}}{\mathbb{P}(\Gamma_v|v)\mathbb{P}(\Gamma_w|w)} \right] \right] \\ &\leq (1 + o(1)) \mathbb{E}_{v,w} \left[ \underbrace{\mathbb{E}_{X \sim \mathbb{Q}} \left[ e^{\frac{\lambda}{2\sqrt{n}} \langle vv^\dagger + ww^\dagger, X \rangle - \frac{\lambda^2 n}{2}} \mathbf{1}_{\Gamma_v} \right]}_{= (I)} \right], \end{aligned}$$

where we used that  $\mathbb{P}(\Gamma_v|v) = 1 + o(1)$ . Introduce the notation  $z = |\text{supp}(v) \cap \text{supp}(w)|$ ,  $t_+ = |\text{supp}(v+w)|$ ,  $t_- = |\text{supp}(v-w)|$  and  $t = t_+ - t_-$ , so that that  $z = t_+ + t_-$ . Finally, we define the function

$$g(t_+, t_-) := \frac{\lambda(t_+^2 + t_-^2)}{\gamma^2 \sqrt{n}} + 2.1 \sqrt{\frac{n}{\gamma}} (t_+ + t_-).$$

Under  $\Gamma_v$ , one has  $\langle vv^\dagger, X_{\text{supp}(v+w)} + X_{\text{supp}(v-w)} \rangle \leq g(t_+, t_-)$ . To bound (I), we first integrate with respect to entries of  $X$  outside  $\text{supp}(v+w) \times \text{supp}(v+w) \cup \text{supp}(v-w) \times \text{supp}(v-w)$ .

$$\begin{aligned} (I) &= \mathbb{E}_{X \sim \mathbb{Q}} \left[ \exp \left( \frac{\lambda}{\sqrt{n}} \langle vv^\dagger, X_{\text{supp}(v+w)} + X_{\text{supp}(v-w)} \rangle - \frac{\lambda^2 z^2}{2\gamma^2 n} \right) \mathbf{1}_{\Gamma_v} \right] \\ &\leq \mathbb{E}_{X \sim \mathbb{Q}} \left[ \exp \left( \frac{\lambda}{\sqrt{n}} \langle vv^\dagger, X_{\text{supp}(v+w)} + X_{\text{supp}(v-w)} \rangle - \frac{\lambda^2 z^2}{2\gamma^2 n} \right) \mathbf{1}_{\langle vv^\dagger, X_{\text{supp}(v+w)} + X_{\text{supp}(v-w)} \rangle \leq g(t_+, t_-)} \right] \\ &\stackrel{(a)}{\leq} \exp \left[ \frac{\lambda^2 t^2}{2\gamma^2 n} - \frac{1}{2} \left( \frac{\lambda \sqrt{2(t_+^2 + t_-^2)}}{\gamma \sqrt{n}} - \frac{g(t_+, t_-) \gamma}{\sqrt{2(t_+^2 + t_-^2)}} \right)_+^2 \right] \\ &\leq \exp \left[ \frac{\eta^2 t^2}{2n} - \frac{1}{2} \left( \frac{\eta \sqrt{z^2 + t^2}}{2\sqrt{n}} - 2.1 \sqrt{n\gamma} \right)_+^2 \right], \end{aligned}$$

where we used

$$\mathbb{E}_{Y \sim \mathcal{N}(0,1)} [e^{aY} \mathbf{1}_{Y \leq b}] \leq e^{a^2/2 - (a-b)_+^2/2}$$

and the fact that  $\langle vv^\dagger, X_{\text{supp}(v+w)} + X_{\text{supp}(v-w)} \rangle \sim \mathcal{N}(0, 2(t_+^2 + t_-^2)/\gamma^2)$  in (a) and  $\eta = \lambda/\gamma$  in the last line. When  $v$  and  $w$  are sampled independently according to the sparse PCA model, then  $z$  follows a hypergeometric distribution with parameters  $(n, \gamma n, \gamma n)$ . Conditioned on  $z$ ,  $t$  is distributed as a sum of  $z$  independent Rademacher random variables. Returning to the second moment, we arrive at

$$\mathbb{E}_{X \sim \mathbb{Q}} \left[ \frac{\mathbb{P}'^2(X)}{\mathbb{Q}^2(X)} \right] \leq (1 + o(1)) \mathbb{E}_{z,t} \left[ \exp \left[ \frac{\eta^2 t^2}{2n} - \frac{1}{2} \left( \frac{\eta \sqrt{z^2 + t^2}}{2\sqrt{n}} - 2.1 \sqrt{n\gamma} \right)_+^2 \right] \right]. \quad (46)$$

In comparison to the second moment bound for the original distribution  $\mathbb{P}(X)$ , the bound for  $\mathbb{P}'(X)$  involves a correction factor  $(\lambda \sqrt{z^2 + t^2}/2\gamma \sqrt{n} - 2.1 \sqrt{n\gamma})_+$ , which is most effective when  $z$  is large. If instead  $z \leq n/(2\eta^2)$ , we make use of the bound (33) proved for second moment bound:

$$\mathbb{E}_t \left[ e^{\frac{\eta^2 t^2}{2n}} |z \right] \leq O \left( 1 + \frac{\eta^2}{n/z - \eta^2} \right) = O(1). \quad (47)$$

For larger values of  $z$ , we rely on the fact that the hypergeometric distribution with parameters  $(n, \gamma n, \gamma n)$  is stochastically dominated by the Binomial distribution with parameters  $(\gamma n, \gamma/(1-\gamma))$ . It follows from Chernoff's bound that

$$\begin{aligned}
\mathbb{E}_{z,t} \left[ e^{\frac{\eta^2 t^2}{2n}} \mathbf{1}_{z \in (\frac{z}{2\eta^2}, \gamma n/3)} \right] &\stackrel{(a)}{\leq} \sum_{z=n/(2\eta^2)}^{\gamma n/3} \exp\left(\frac{\eta^2 z^2}{2n} - \gamma n h_{\gamma/(1-\gamma)}\left(\frac{z}{\gamma n}\right)\right) \\
&\stackrel{(b)}{\leq} \sum_{z=n/(2\eta^2)}^{\gamma n/3} \exp\left(z \left(\frac{\eta^2 z}{2n} - \log\left(\frac{z(1-\gamma)}{e\gamma^2 n}\right)\right)\right) \\
&\stackrel{(c)}{\leq} \sum_{z=n/(2\eta^2)}^{\gamma n/3} \exp\left(z \left(\left(\frac{\lambda^2}{6\gamma} - \log\frac{1-\gamma}{3e\gamma}\right) \vee \left(\frac{1}{4} + \log\frac{2e\lambda^2}{1-\gamma}\right)\right)\right) \\
&\stackrel{(d)}{\leq} \sum_{z=n/(2\eta^2)}^{\gamma n/3} \exp\left(z \left(\left(\frac{\lambda^2}{6\gamma} - \log\frac{1-\gamma}{3e\gamma}\right) \vee \left(\log\frac{8e^{5/4}\gamma \log(1/\gamma)}{1-\gamma}\right)\right)\right) \\
&\leq \sum_{z=n/(2\eta^2)}^{\gamma n/3} \exp(-z\epsilon) = o(1), \tag{48}
\end{aligned}$$

where the last line holds for some constant  $\epsilon > 0$  in view of (42) and of the condition  $\gamma < 1/(81e^{41})$ . We used in (a) that  $t \leq z$ , in (b) that  $h_{p_0}(p_1) \geq p_1 \log(p_1/(ep_0))$  in (c) that the function  $x \mapsto \eta^2 x/(2n) - \log(x)$  is decreasing on  $(0, 2n/\eta^2]$  and increasing on  $[2n/\eta^2, \infty)$ . and in (d) that  $\lambda^2 \leq -4\gamma \log \gamma$ .

Finally, we turn to the case  $z \in [\gamma n/3, \gamma n]$ , for which we will rely on the correcting term in (46). Assume that  $\lambda \geq 9\sqrt{\gamma}$  without loss of generality, because otherwise by (43), the second moment is bounded without any conditioning. For  $z$  larger than  $\gamma n/3$ ,

$$\frac{\lambda z}{\sqrt{2\gamma\sqrt{n}}} \geq 2.1\sqrt{n\gamma},$$

and we can once again apply Chernoff's bound to obtain

$$\begin{aligned}
&\mathbb{E}_{z,t} \left[ \exp\left(\frac{\eta^2 t^2}{2n} - \frac{1}{2} \left(\frac{\eta\sqrt{z^2+t^2}}{2\sqrt{n}} - 2.1\sqrt{n\gamma}\right)_+^2\right) \mathbf{1}_{z \in (\gamma n/3, \gamma n)} \right] \\
&\leq \mathbb{E}_{z,t} \left[ \exp\left(\frac{\eta^2 z^2}{2n} - \frac{1}{2} \left(\frac{\eta z}{\sqrt{2n}} - 2.1\sqrt{n\gamma}\right)_+^2\right) \mathbf{1}_{z \in (\gamma n/3, \gamma n)} \right] \\
&\leq \sum_{z=\gamma n/3}^{\gamma n} \exp\left(\frac{\eta^2 z^2}{4n} + \frac{2.1}{\sqrt{2}} \eta z \sqrt{\gamma} - \gamma n h_{\gamma/(1-\gamma)}\left(\frac{z}{\gamma n}\right)\right) \\
&\stackrel{(a)}{\leq} \sum_{z=\gamma n/3}^{\gamma n} \exp\left(\frac{\eta^2 z^2}{4n} + \frac{2.1}{\sqrt{2}} \eta z \sqrt{\gamma} - z \log\left(\frac{z(1-\gamma)}{e\gamma^2 n}\right)\right) \\
&\leq \sum_{z=\gamma n/3}^{\gamma n} \exp\left(z \left(\frac{\eta^2 \gamma}{4} - \log\left(\frac{1}{\gamma}\right) + \frac{2.1\eta\sqrt{\gamma}}{\sqrt{2}} + \log\left(\frac{3e}{1-\gamma}\right)\right)\right) \\
&\leq \sum_{z=\gamma n/3}^{\gamma n} e^{-z\epsilon} = o(1),
\end{aligned}$$

where we used  $t \leq z$  and the fact that the whole exponent is monotone increasing in  $t^2$  in the first line. The last inequality holds for some constant  $\epsilon > 0$ , because of condition (42) on  $\lambda$  together with the inequality

$\lambda \leq 2\sqrt{\gamma \log(1/\gamma)}$ . In (a), we applied  $h_{p_0}(p_1) \geq p_1 \log(p_1/(ep_0))$ . Together with (46), (47), and (48), we conclude that  $\mathbb{E}_{X \sim \mathbb{Q}} \left[ \frac{\mathbb{P}^{\prime 2}(X)}{\mathbb{Q}^2(X)} \right] = O(1)$ .

**Conditional second moment bound for reconstruction** In view of (16) and a bounded conditional second moment, we have  $D_{\text{KL}}(\mathbb{P}'\|\mathbb{Q}) = O(1)$ . Also, we have  $\|M\|_* = \|M\|_2 = \frac{\lambda}{\sqrt{n}} \|v\|_2^2 = \lambda\sqrt{n}$ . Therefore, the conclusion for reconstruction follows by applying Theorem 4 together with Theorem 5.

### 4.3 Submatrix Localization

In this section we prove Theorem 2. Recall that  $X = (\mu/\sqrt{n})(Y - \mathbb{J}/k) + W$ , where  $\sigma_0 : [n] \rightarrow [k]$  is a balanced partition,  $Y_{i,j} = \mathbf{1}_{\sigma_0(i)=\sigma_0(j)}$ , and  $W$  is Wigner.

#### 4.3.1 First moment upper bound for submatrix localization

It follows from (14) that the conditional log likelihood ratio reads

$$\log \frac{\mathbb{P}(X|\sigma)}{\mathbb{Q}(X)} = \frac{\mu}{2\sqrt{n}} \langle Y - \mathbb{J}/k, X \rangle - \frac{\mu^2}{4n} \|Y - \mathbb{J}/k\|_F^2.$$

Therefore, maximizing  $\log \mathbb{P}(X|\sigma)/\mathbb{Q}(X)$  over  $\sigma$  is equivalent to computing

$$\max_{\sigma} \mathcal{T}(\sigma) := \max_{\sigma} \sum_{i < j} X_{i,j} (Y_{i,j} - 1/k).$$

In both the planted model and the null model,  $\mathcal{T}(\sigma)$  is the sum of independent, Gaussian random variables and is therefore itself Gaussian. Under  $\mathbb{Q}$ ,

$$\mathcal{T}(\sigma) \sim \mathcal{N}\left(0, \frac{n^2(k-1)}{2k^2} + O(n)\right).$$

Under  $\mathbb{P}$ , denoting by  $\sigma_0$  the planted partition,

$$\begin{aligned} \mathcal{T}(\sigma) &= \frac{\mu}{\sqrt{n}} \sum_{i < j} (\mathbf{1}_{\sigma_0(i)=\sigma_0(j)} - 1/k) (\mathbf{1}_{\sigma(i)=\sigma(j)} - 1/k) + \sum_{i < j} W_{i,j} (\mathbf{1}_{\sigma(i)=\sigma(j)} - 1/k) \\ &= \frac{\mu}{\sqrt{n}} \sum_{i < j} \mathbf{1}_{\sigma_0(i)=\sigma_0(j), \sigma(i)=\sigma(j)} + \sum_{i < j} W_{i,j} (\mathbf{1}_{\sigma(i)=\sigma(j)} - 1/k) - \frac{n^2}{2k^2} + O(n). \end{aligned}$$

Hence the distribution of  $\mathcal{T}(\sigma)$  depends on the overlap matrix  $\omega$  between  $\sigma$  and the planted partition  $\sigma_0$ . For a given  $\omega$ , among all  $\binom{n}{2}$  pairs  $i, j$  with  $i < j$ , there are  $\|\omega\|_F^2 n^2/2k^2 + O(n)$  pairs such that  $\sigma_0(i) = \sigma_0(j)$  and  $\sigma(i) = \sigma(j)$ . Therefore,

$$\mathcal{T}(\sigma) \sim \mathcal{N}\left(\frac{\mu n^2 (\|\omega\|_F^2 - 1)}{2k^2 \sqrt{n}} + O(n), \frac{n^2(k-1)}{2k^2} + O(n)\right).$$

To prove that detection is possible, notice that in the planted model,  $\max_{\sigma} \mathcal{T}(\sigma) \geq \mathcal{T}(\sigma_0)$ . Setting  $\omega = \mathbb{I}$ , Gaussian tail bounds tell us that

$$\mathbb{P}\left[\mathcal{T}(\sigma_0) > \frac{n^2 \mu (k-1)}{2k^2 \sqrt{n}} - O(n\sqrt{\log n})\right] \leq n^{-\Omega(1)}.$$

In the null model, taking the union bound over the  $n^k$  ways to choose  $\sigma$ , we can bound the probability that *any* partition is as good, according to  $\mathcal{T}$ , as the planted one, by

$$\mathbb{Q}\left[\max_{\sigma} \mathcal{T}(\sigma) > \frac{n^2 \mu (k-1)}{2k^2 \sqrt{n}} - O(n\sqrt{\log n})\right] \leq \exp\left(n \left(\log k - \frac{\mu^2 (k-1)}{4k^2} + O(\sqrt{\log n/n})\right)\right).$$

Thus the probability of this event is  $e^{-\Omega(n)}$  whenever

$$\mu^2 > \frac{4k^2 \log k}{k-1},$$

meaning that above this threshold we can distinguish the null and planted models with generalized likelihood testing.

To prove that reconstruction is possible, we compute in the planted model the probability that  $\mathcal{T}(\sigma) > \mathcal{T}(\sigma_0)$  given that  $\sigma$  has  $L_2$  overlap  $z$  with the planted partition, and argue that this probability tends to zero whenever the overlap is small enough. Taking the union bound over every  $\sigma$  with  $L_2$  overlap at most  $z$  gives

$$\mathbb{P} \left[ \max_{\|\omega(\sigma, \sigma_0)\|_F^2 \leq z} \mathcal{T}(\sigma) \geq \frac{n^2 \mu(k-1)}{2k^2 \sqrt{n}} - O(n\sqrt{\log n}) \right] \leq \exp \left( n \left( \log k - \frac{\mu^2(k-z)^2}{k^2(k-1)} + O(\sqrt{\log n/n}) \right) \right).$$

By the assumption that  $\mu^2 > 4k^2 \log k / (k-1)$ , it follows that there exists a fixed constant  $\epsilon > 0$  such that  $\mu^2(1-\epsilon)^2 > 4k^2 \log k / (k-1)$ . Hence, setting  $z = 1 + (k-1)\epsilon$  in the last displayed equation, it yields that with probability at least  $1 - e^{-\Omega(n)}$ ,

$$\max_{\|\omega(\sigma, \sigma_0)\|_F^2 \leq z} \mathcal{T}(\sigma) < \frac{n^2 \mu(k-1)}{2k^2 \sqrt{n}} - O(n\sqrt{\log n}),$$

and consequently  $\|w(\widehat{\sigma}_{\text{ML}}, \sigma_0)\|_F^2 \geq 1 + (k-1)\epsilon$ . By Lemma 2, this further implies that the trace overlap satisfies  $T(\widehat{\sigma}_{\text{ML}}, \sigma_0) \geq 1 + (k-1)\epsilon$ . Moreover, construct an  $n \times n$  matrix  $\widehat{M}$  so that  $\widehat{M}_{ij} = (\mu/\sqrt{n}) \mathbf{1}_{\widehat{\sigma}_{\text{ML}}(i) = \widehat{\sigma}_{\text{ML}}(j)}$ . Then  $\|\widehat{M}\|_F^2 = O(n)$ , and

$$\langle \widehat{M}, M \rangle = \frac{n\mu^2}{k^2} (\|w(\widehat{\sigma}_{\text{ML}}, \sigma_0)\|_F^2 - 1) + O(1),$$

which is at least  $n\mu^2(k-1)\epsilon/k^2 + O(1)$  with high probability. Thus, we can reconstruct the signal matrix  $M$  and the planted partition  $\sigma_0$  better than chance.

### 4.3.2 Second moment lower bound for submatrix localization

We first prove that when

$$\mu^2 < \begin{cases} k^2 & k = 2 \\ \frac{2k^2 \log(k-1)}{k-1} & k \geq 3, \end{cases} \quad (49)$$

then the second moment is bounded. Applying Lemma 1,

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_{\sigma, \tau} \exp \left( \frac{\mu^2}{2n} \langle Y - \mathbb{J}/k, Y' - \mathbb{J}/k \rangle \right),$$

where  $Y_{ij} = \mathbf{1}_{\sigma(i) = \sigma(j)}$  and  $Y'_{ij} = \mathbf{1}_{\tau(i) = \tau(j)}$ . Recall that  $\omega$  denotes the overlap matrix between partitions  $\sigma$  and  $\tau$ . Then  $\langle Y, Y' \rangle = n^2 \|\omega\|_F^2 / k^2$  and  $\langle Y, \mathbb{J} \rangle = \langle Y', \mathbb{J} \rangle = n^2 / k$ . It follows from the last displayed equation that

$$\mathbb{E}_{X \sim \mathbb{Q}} \left( \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right)^2 = \mathbb{E}_{\sigma, \tau} \exp \left( \frac{\mu^2 n}{2k^2} (\|\omega\|_F^2 - 1) \right), \quad (50)$$

Lemmata 3, 4 and 5 assure us that this expression is bounded by a constant so long as (49) holds.

For reconstruction, in view of (16) and a bounded second moment,  $D_{\text{KL}}(\mathbb{P} \| \mathbb{Q}) = O(1)$ . Apply Theorem 4 so that for any estimator  $\widehat{M}$  with  $\|\widehat{M}\|_F^2 = O(n)$ , we have  $\mathbb{E}[\langle M, \widehat{M} \rangle] = o(n)$ . Recall that  $\sigma_0$  is the planted partition and  $M = (\mu/\sqrt{n})(Y - \mathbb{J}/k) = (\mu/\sqrt{n})UU^\dagger$ , where  $U \in \mathbb{R}^{n \times k}$  with  $U_{is} = \mathbf{1}_{\sigma_0(i) = s} - 1/k$ . Then for



any estimator  $\widehat{\sigma}$  of  $\sigma_0$ , by defining  $\widehat{U}$  such that  $\widehat{U}_{is} = \mathbf{1}_{\widehat{\sigma}(i)=s} - 1/k$  and letting  $\widehat{M} = (\mu/\sqrt{n})\widehat{U}\widehat{U}^\dagger$ , it follows that

$$\frac{1}{n^2} \mathbb{E} \|U^\dagger \widehat{U}\|_F^2 = \frac{1}{\mu^2 n} \mathbb{E} \langle M, \widehat{M} \rangle = o(1).$$

Finally, notice that by letting  $\omega = \omega(\widehat{\sigma}, \sigma_0)$ ,

$$\|U^\dagger \widehat{U}\|_F^2 = \frac{n^2}{k^2} \sum_{\ell, s} (\omega_{\ell, s} - 1/k)^2 = \frac{n^2}{k^2} (\|\omega\|_F^2 - 1);$$

thus  $\mathbb{E} \|\omega\|_F^2 = 1 + o(1)$ . Hence, we can neither reconstruct the signal matrix  $M$  nor the planted partition  $\sigma_0$ .

### 4.3.3 Conditional second moment lower bound for submatrix localization

Notice that in the large  $k$  asymptotic, the right hand side of (49) converges to  $2k \log k$ , while the first moment upper bound gives  $4k \log k$ . To match the first moment upper bound in the larger  $k$  asymptotic, we apply a conditional second moment method. In the sequel we assume that

$$\mu^2 \leq 4k \log k - 44k \log^{3/4}(k). \quad (51)$$

If  $\log k < 11^4$ , then  $4k \log k - 44k \log^{3/4} k$  is negative. Hence, we focus on the setting  $\log k \geq 11^4$ .

For any partition  $\sigma : [n] \rightarrow k$ , let  $M = \frac{\mu}{\sqrt{n}}(Y_\sigma - \mathbb{J}/k)$  and define the event  $\Gamma_\sigma$  by

$$\Gamma_\sigma := \left\{ \sup_{1 \leq \ell \leq k} \left\| [X - M]_{\sigma^{-1}(\ell)} \right\|_2 \leq 3\sqrt{n/k} \right\},$$

where  $[X - M]_{\sigma^{-1}(\ell)}$  denotes the  $\sigma^{-1}(\ell) \times \sigma^{-1}(\ell)$  submatrix of  $X - M$ . In other words, on  $\Gamma_\sigma$ , the spectral norms of submatrices  $[X - M]_{\sigma^{-1}(\ell)}$  for every  $1 \leq \ell \leq k$  are all upper bounded by  $3\sqrt{n/k}$ . Since  $[X - M]_{\sigma^{-1}(\ell)}$  is distributed as a Wigner Matrix under  $\mathbb{P}(\cdot|\sigma)$ , by Gaussian concentration theorem and Slepian's inequality we have

$$\mathbb{P} \left[ \left\| [X - M]_{\sigma^{-1}(\ell)} \right\|_2 \geq 2\sqrt{n/k} + t \mid \sigma \right] \leq e^{-t^2/4}, \forall 1 \leq \ell \leq k.$$

Since  $k = o(n/\log(n))$ , we have  $\mathbb{P}(\Gamma_\sigma|\sigma) = 1 + o(1)$  uniformly with respect to  $\sigma$ .

Next, we condition on the high probability events  $\Gamma_\sigma$  by defining

$$\mathbb{P}'(X) = \mathbb{E}_\sigma \left[ \mathbb{P}(X|\sigma) \frac{\mathbf{1}_{\Gamma_\sigma}}{\mathbb{P}(\Gamma_\sigma|\sigma)} \right],$$

It follows that the conditional second moment satisfies

$$\begin{aligned} \mathbb{E}_{X \sim \mathbb{Q}} \left[ \left( \frac{\mathbb{P}'(X)}{\mathbb{Q}(X)} \right)^2 \right] &= \mathbb{E}_{\sigma, \tau} \left[ \mathbb{E}_{X \sim \mathbb{Q}} \left[ \frac{\mathbb{P}(X|\sigma)\mathbb{P}(X|\tau)}{\mathbb{Q}^2(X)} \frac{\mathbf{1}_{\Gamma_\sigma}\mathbf{1}_{\Gamma_\tau}}{\mathbb{P}(\Gamma_\sigma|\sigma)\mathbb{P}(\Gamma_\tau|\tau)} \right] \right] \\ &= (1 + o(1)) \mathbb{E}_{\sigma, \tau} \left[ \underbrace{\mathbb{E}_{X \sim \mathbb{Q}} \left[ e^{\frac{\mu}{2\sqrt{n}} \langle X, Y_\sigma + Y_\tau - 2\mathbb{J}/k \rangle - \frac{\mu^2}{2n} \|Y_\sigma - \mathbb{J}/k\|_F^2} \mathbf{1}_{\Gamma_\sigma} \right]}_{= (I)} \right], \end{aligned}$$

where we used that  $\mathbb{P}(\Gamma_v|v) = 1 + o(1)$ . Given  $\sigma$  and  $\tau$ , define  $\mathcal{A}_{\ell\ell'} = \sigma^{-1}(\ell) \cap \tau^{-1}(\ell')$  and the event

$$\bar{\Gamma}_{\ell\ell'} = \left\{ \sum_{i, j \in \mathcal{A}_{\ell\ell'}} X_{ij} \leq \frac{\mu}{\sqrt{n}} \left( 1 - \frac{1}{k} \right) |\mathcal{A}_{\ell\ell'}|^2 + 3|\mathcal{A}_{\ell\ell'}| \sqrt{n/k} \right\}$$

Obviously,  $\bar{\Gamma}_{\ell\ell'} \subset \Gamma_\sigma$  for all  $\ell, \ell' \in [k]$ . Equipped with this notation, we bound (I) by the exponential moment of  $k^2 + 1$  thresholded normal random variables:

$$\begin{aligned} (I) &\leq \mathbb{E}_{X \sim \mathbb{Q}} \left[ \exp \left( \frac{\mu}{2\sqrt{n}} \langle X, Y_\sigma + Y_\tau - 2\mathbb{J}/k \rangle - \frac{\mu^2}{2n} \|Y_\sigma - \mathbb{J}/k\|_F^2 \right) \prod_{\ell, \ell'=1}^k \mathbf{1}_{\bar{\Gamma}_{\ell\ell'}} \right] \\ &\leq \exp \left( \frac{\mu^2}{2n} \langle Y_\sigma - \mathbb{J}/k, Y_\tau - \mathbb{J}/k \rangle \right) \prod_{\ell, \ell'=1}^k \exp \left( -\frac{1}{2} \left[ \mu \left( 1 - \frac{1}{k} \right) \frac{|\mathcal{A}_{\ell\ell'}|}{\sqrt{2n}} - 3\sqrt{\frac{n}{2k}} \right]_+^2 \right) \end{aligned}$$

where we used

$$\mathbb{E}_{Z \sim \mathcal{N}(0,1)} [e^{aZ} \mathbf{1}_{Z \leq b}] \leq e^{a^2/2 - (a-b)_+^2/2}.$$

Recall that  $\omega$  denotes the overlap matrix between  $\sigma$  and  $\tau$ . Then  $\langle Y_\sigma, Y_\tau \rangle = n\|\omega\|_F^2/k^2$ ,  $\langle Y_\sigma, \mathbb{J} \rangle = \langle Y_\sigma, \mathbb{J} \rangle = n^2/k$  and  $|\mathcal{A}_{\ell\ell'}| = n\omega_{\ell\ell'}/k$ . Define

$$\begin{aligned} a_k &:= 3 \log^{1/4}(k) \\ b_k &:= 2/k + 6/a_k. \end{aligned}$$

It follows from the last displayed equation that

$$\begin{aligned} \frac{\log(I)}{n} &\leq \frac{\mu^2}{2k^2} (\|\omega\|_F^2 - 1) - \frac{\mu^2}{4k^2} \sum_{\ell, \ell'} \omega_{\ell\ell'}^2 \left( 1 - \frac{1}{k} - 3 \frac{\sqrt{k}}{\mu\omega_{\ell\ell'}} \right)_+^2 \\ &\leq \frac{\mu^2}{4k^2} (1 + b_k) (\|\omega\|_F^2 - 1) + \frac{\mu^2}{4k^2} \sum_{\ell, \ell'} \left( \omega_{\ell\ell'}^2 - \frac{1}{k^2} \right) \mathbf{1}_{\omega_{\ell\ell'} \leq \sqrt{k}a_k/\mu}, \end{aligned} \quad (52)$$

where we used  $(1-x)_+^2 \geq \max((1-2x), 0)$  and  $b_k \leq 1$  since  $\log k \geq 11^4$  in the second line. Unfortunately, the expression

$$\exp \left( \sum_{\ell, \ell'} \left( \omega_{\ell\ell'}^2 - \frac{1}{k^2} \right) \mathbf{1}_{\omega_{\ell\ell'} \leq \sqrt{k}a_k/\mu} \right)$$

is not easy to integrate over  $\omega$ . This is why we shall bound it by a combination of the entropy of  $\omega$  and a second degree polynomial.

**Lemma 7.** *Let  $t \in (0, 1)$  be such that  $t \leq 0.4$  and  $t \geq \frac{3}{k} \vee \left(\frac{e}{k}\right)^{1/5} \vee \frac{1-1/k}{2\lceil \log k - 1 \rceil} \vee \frac{2 \log k}{5(k-2 \log k + 1)}$ . Upon defining  $c_t := \frac{5t}{\log k - 1} - \frac{2+5t}{k\lceil \log k - 1 \rceil} > 0$ , we have for any  $x \in [0, 1]$ ,*

$$\left(x^2 - \frac{1}{k^2}\right) \mathbf{1}_{x < t} \leq 5t\left(x - \frac{1}{k}\right)(1-x) + c_t \left[ x \log(x) + \frac{\log k}{k} \right]. \quad (53)$$

*Proof.* Indeed, let  $g$  be defined by  $g(x) = 5t\left(x - \frac{1}{k}\right)(1-x) + c_t \left[ x \log(x) + \frac{\log k}{k} \right] - \left(x^2 - \frac{1}{k^2}\right) \mathbf{1}_{x < t}$ . For any  $x \neq t$ ,  $g'(x) = 5t(-2x + 1 + 1/k) + c_t \log(xe) - 2x \mathbf{1}_{x < t}$  and  $g''(x) = \frac{c_t}{x} - 10t - 2 \cdot \mathbf{1}_{x < t}$ . Since  $c_t \leq 10t^2$ ,  $g'$  is increasing on  $(0, c_t/[2 + 10t])$  and decreasing on  $(c_t/[2 + 10t], t)$  and  $(t, 1]$ . Besides,  $c_t/[2 + 10t] \geq 1/k$  as this inequality reduces to  $t \geq \frac{2 \log k}{5(k-2 \log k + 1)}$ . Since  $c_t$  has been chosen in such a way that  $g'(1/k) = 0$ , the minimum of  $g$  is either achieved at  $1/k$ ,  $t_-$ , or 1. We have  $g(1/k) = 0$  and  $g(1) = c_t \log k/k > 0$ , and

$$g(t_-) \geq 5t(t - 1/k)(1-t) - c_t t \log(1/t) - t^2 \geq t^2 - \frac{5t^2 \log(1/t)}{\log k - 1} \geq 0,$$

where we used  $(t - 1/k)(1-t) \geq 2t/5$  and  $t \geq (e/k)^{1/5}$ . We have proved (53).  $\square$

Since  $\mu \leq 2\sqrt{k \log k}$ , we have  $\sqrt{k}a_k/\mu \geq \frac{3}{2} \log^{-1/4}(k)$ . Assuming that  $\mu \geq 2.5\sqrt{k}a_k$  and since  $\log k \geq 11^4$ , the assumptions of (53) are satisfied for  $t = \sqrt{k}a_k/\mu$ . Writing  $c_k$  for  $c_{\sqrt{k}a_k/\mu}$ , it follows from (52) and (53) that

$$\begin{aligned} \frac{\log(I)}{n} &\leq \frac{\mu^2}{4k^2}(1+b_k)(\|\omega\|_F^2 - 1) + \frac{5\mu a_k}{4k^{3/2}} \sum_{\ell, \ell'} \left( \omega_{\ell\ell'} - \frac{1}{k} \right) (1 - \omega_{\ell\ell'}) + \frac{\mu^2 c_k}{4k^2} \sum_{\ell, \ell'} \left[ \omega_{\ell\ell'} \log(\omega_{\ell\ell'}) + \frac{\log k}{k} \right] \\ &\stackrel{(a)}{\leq} \frac{\mu^2}{4k^2}(1+b_k)(\|\omega\|_F^2 - 1) - \frac{\mu^2 c_k}{4k} [H(\omega) - \log k] \\ &\leq \frac{\mu^2}{4k^2}(1+b_k)(\|\omega\|_F^2 - 1) - \frac{5\mu a_k}{4\sqrt{k}(\log k - 1)} [H(\omega) - \log k] \\ &\leq \frac{\mu^2}{4k^2}(1+b_k)(\|\omega\|_F^2 - 1) - \frac{15}{2} \log^{-1/4}(k) [H(\omega) - \log k] , \end{aligned}$$

where (a) follows because  $\omega$  is doubly stochastic so that  $\sum_{\ell, \ell'} (\omega_{\ell\ell'} - \frac{1}{k})(1 - \omega_{\ell\ell'}) = 1 - \|\omega\|_F^2 \leq 0$ ; the last inequality holds due to  $\mu \leq 2\sqrt{k \log k}$ . If  $\mu \leq 2.5\sqrt{k}a_k$ , we simply come back to (52) to ensure that  $\log(I) \leq n \frac{\mu^2}{2k^2} (\|\omega\|_F^2 - 1)$ . We arrive at

$$\mathbb{E}_{X \sim \mathbb{Q}} \left[ \left( \frac{\mathbb{P}'(X)}{\mathbb{Q}(X)} \right)^2 \right] \leq (1 + o(1)) \mathbb{E}_{\sigma, \tau} \exp \left[ n (t_1 (\|\omega\|_F^2 - 1) - t_2 (H(\omega) - \log k)) \right] \quad (54)$$

with  $t_1 = \frac{\mu^2}{2k^2}$  and  $t_2 = 0$  when  $\mu < 2.5\sqrt{k}a_k$  and  $t_1 = \frac{\mu^2}{4k^2}(1+b_k)$  and  $t_2 = 8 \log^{-1/4}(k)$  when  $\mu \geq 2.5\sqrt{k}a_k$ .

Hence, to prove the conditional second moment is bounded, it reduces to verifying the right hand side of (54) is bounded. By assumption (51) and  $\log k \geq 11^4$ , it holds that

$$\mu^2 \leq \frac{4k^2}{(k-1)(1+b_k)} \left( \log(k-1) - 8 \log(k-1) \log^{-1/4}(k) - 1 \right) .$$

This further implies that

$$\frac{t_1}{1-t_2} \leq \frac{\log(k-1) - 1/(1-t_2)}{k-1} .$$

Therefore, by Lemma 4, we have that for all  $\omega$ ,

$$(H(\omega) - \log k) (1 - t_2) + t_1 (\|\omega\|_F^2 - 1) \leq -\frac{1}{k-1} (\|\omega\|_F^2 - 1) .$$

Hence, assumptions in Lemma 3 are satisfied with  $\varphi(\omega) = t_1 (\|\omega\|_F^2 - 1) - t_2 [H(\omega) - \log k]$  and  $\delta = 1/(k-1)$ , and it follows from Lemma 3 that the right hand side of (54) is bounded.

**Conditional second moment bound for reconstruction** In view of (16) and a bounded conditional second moment, we have  $D_{\text{KL}}(\mathbb{P}'\|Q) = O(1)$ . Also, we have that

$$\|M\|_2 = \frac{\mu}{\sqrt{n}} \|Y - \mathbb{J}/k\|_2 \leq \frac{\mu}{\sqrt{n}} (\|Y\|_2 + \|\mathbb{J}\|_2/k) = 2\mu\sqrt{n}/k$$

and since  $M$  is of rank  $k$ ,  $\|M\|_* \leq k\|M\|_2 \leq 2\mu\sqrt{n}$ . Therefore, the conclusion for reconstruction follows by applying Theorem 4 together with Theorem 5.

#### 4.4 Gaussian Mixture Clustering

Finally, we turn to the Gaussian Mixture Clustering problem, where  $\sigma : [n] \rightarrow [k]$  is a balanced partition chosen uniformly at random,  $v_1, \dots, v_k \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(0, k/(k-1)\mathbb{I}_{n,n})$ , and we observe the matrix

$$X = \sqrt{\frac{\rho}{n}} \left( S - \frac{1}{k} \mathbb{J}_{m,k} \right) V^\dagger + W, \quad (55)$$

where  $W$  has independent standard normal entries,  $S$  is an  $m \times k$  matrix with  $S_{i,t} = \mathbf{1}_{\sigma(i)=t}$ , and  $V = [v_1, \dots, v_k]$ .

#### 4.4.1 First moment upper bound for Gaussian mixture clustering

In this section, we derive an upper bound on the detection and reconstruction threshold via the first moment method. The testing procedure is again based on the generalized likelihood ratio  $\sup_{v,\sigma} \log \mathbb{P}(X|v,\sigma)/\mathbb{Q}(X)$ , which from (14) we write as

$$\begin{aligned} \log \frac{\mathbb{P}(X | v, \sigma)}{\mathbb{Q}(X)} &= \sqrt{\frac{\rho}{n}} \langle X, (S - \mathbb{J}_{m,k}/k)V^\dagger \rangle - \frac{\rho}{2n} \|(S - \mathbb{J}_{m,k}/k)V^\dagger\|_F^2 \\ &= \sqrt{\frac{\rho}{n}} \sum_{s=1}^k \langle \sum_{i:\sigma(i)=s} x_i, v_s - \bar{v} \rangle - \frac{\rho m}{2nk} \sum_{s=1}^k \|v_s - \bar{v}\|_2^2. \end{aligned}$$

When  $\sigma$  is fixed, we can optimize in  $v$  by setting the  $s$ th cluster center to

$$v_s - \bar{v} = \frac{k\sqrt{n}}{m\sqrt{\rho}} \sum_{i:\sigma(i)=s} x_i,$$

the rescaled center of the data points  $x_i$  which have been assigned to cluster  $s$  according to  $\sigma$ . Up to multiplicative constants, then, the generalized likelihood ratio test is equivalent to the test based on the statistic

$$\max_{\sigma} \mathcal{T}(\sigma) := \max_{\sigma} \frac{k}{m} \sum_s \left\| \sum_{\sigma(i)=s} x_i \right\|^2. \quad (56)$$

In the null model, for any fixed  $\sigma$ ,

$$\mathcal{T}(\sigma) \sim \chi_{nk}^2,$$

where  $\chi_{nk}^2$  is the central chi-squared distribution with  $nk$  degrees of freedom.

In the planted model, let  $v^0$  and  $\sigma_0$  denote the planted vectors and partition respectively, and for an arbitrary partition  $\sigma$ , let  $\omega$  once again be the overlap matrix between  $\sigma$  and  $\sigma_0$ . For any  $1 \leq \ell \leq k$ ,

$$\sum_{\sigma(i)=s} x_i \sim \mathcal{N} \left( \frac{m\sqrt{\rho}}{k\sqrt{n}} \sum_t \omega_{s,t} (v_t^0 - \bar{v}^0), \frac{m}{k} \mathbb{I} \right).$$

For  $y \sim \mathcal{N}(\mu, \mathbb{I}_d)$ , let  $\chi_d^2(\|\mu\|^2)$  denote the distribution of  $\|y\|^2$ , which is known as non-central chi-square distribution with  $d$  degrees of freedom and non-centrality  $\|\mu\|^2$ . In this notation,  $\mathcal{T}(\sigma)$  is distributed in  $\mathbb{P}$  as a non-central chi-squared random variable with  $nk$  degrees of freedom and noncentrality

$$\begin{aligned} \frac{\alpha\rho}{k} \sum_{\ell=1}^k \left\| \sum_s \omega_{\ell,s} (v_s^0 - \bar{v}^0) \right\|^2 &= \frac{\alpha\rho}{k} \sum_{\ell=1}^k \sum_{s,t} \omega_{\ell,s} \omega_{\ell,t} \langle v_s^0 - \bar{v}^0, v_t^0 - \bar{v}^0 \rangle \\ &= \frac{n\alpha\rho}{k-1} \left( \|\omega\|_F^2 - 1 \right) + O(\sqrt{n \log n}). \end{aligned} \quad (57)$$

To obtain the last line, note that the  $v_\ell^0$  are Gaussian with zero mean and variance  $k/(k-1)$  in each coordinate, making  $\langle v_s^0 - \bar{v}^0, v_t^0 - \bar{v}^0 \rangle = -n/(k-1) + O(\sqrt{n \log n})$  for  $s \neq t$  and  $\|v_s^0 - \bar{v}^0\|^2 = n + O(\sqrt{n \log n})$  with high probability.

We will need the following tail bounds for non-central chi-squared distributions [13, Lemma 8.1]: for  $t > 0$ ,

$$\Pr \left[ \chi_d^2 \left( \|\mu\|^2 \right) < d + \|\mu\|^2 - 2\sqrt{\left( d + 2\|\mu\|^2 \right) t} \right] < e^{-t} \quad (58)$$

$$\Pr \left[ \chi_d^2 \left( \|\mu\|^2 \right) > d + \|\mu\|^2 + 2\sqrt{\left( d + 2\|\mu\|^2 \right) t + 2t} \right] < e^{-t} \quad (59)$$

Notice that we can obtain central chi-square tail bounds by setting  $\|\mu\|^2 = 0$ .

To derive the first moment bound for detectability, notice that in the planted model, when  $\sigma = \sigma_0$  up to a permutation of cluster indices,  $\|\omega\|_F^2 = k$  and

$$\mathcal{T}(\sigma_0) \sim \chi_{nk}^2 \left( \alpha n \rho + O(\sqrt{n \log n}) \right).$$

Setting  $t = \log n$  in (58), we know that with high probability  $\mathcal{T}(\sigma_0) > nk + n\alpha\rho - O(\sqrt{n \log n})$ .

In the null model, by the union bound and (59), letting  $t = (1 + \epsilon)m \log k$  for an arbitrarily small constant  $\epsilon > 0$ ,

$$\mathbb{Q} \left[ \max_{\sigma} \mathcal{T}(\sigma) > nk + 2\sqrt{nk t} + 2t \right] = k^m \Pr \left[ \chi_{nk}^2 > nk + 2\sqrt{nk t} + 2t \right] = e^{-\Omega(m)},$$

Hence, with high probability, in the null model,

$$\max_{\sigma} \mathcal{T}(\sigma) \leq nk + 2\sqrt{(1 + \epsilon)mnk \log k} + 2(1 + \epsilon)m \log k.$$

By the assumption that  $\rho > \rho^{\text{upper}}$ , i.e.,  $\rho\sqrt{\alpha} > 2\sqrt{k \log k} + 2\sqrt{\alpha} \log k$ , it follows that for sufficiently large  $n$ ,

$$n\alpha\rho - O(\sqrt{n \log n}) \geq 2(1 + \epsilon) \left( \sqrt{mnk \log k} + m \log k \right),$$

and consequently, with high probability,  $\max_{\sigma} \mathcal{T}(\sigma) > nk + n\alpha\rho - O(\sqrt{n \log n})$  under  $\mathbb{P}$ , and  $\max_{\sigma} \mathcal{T}(\sigma) < nk + n\alpha\rho - O(\sqrt{n \log n})$  under  $\mathbb{Q}$ .

To show reconstruction is possible above this bound, let  $\sigma$  have overlap matrix  $\omega$  with  $\sigma_0$  and set  $\|\omega\|_F^2 = \theta$ . We will show that, when  $\theta$  is sufficiently small, there are with high probability no such partition with likelihood as high as the planted one. In the planted model,

$$\mathcal{T}(\sigma) \sim \chi_{nk}^2 \left( n\alpha\rho \frac{\theta - 1}{k - 1} + O(\sqrt{n \log n}) \right).$$

Taking the union bound over all partitions  $\sigma$  which have  $L_2$  overlap at most  $1 + (k - 1)\epsilon$  with the planted one—of which there are no more than  $k^m$ —and invoking (59) with  $t = (1 + \epsilon)m \log k$ , we know that with high probability,

$$\begin{aligned} \max_{\sigma: \|\omega(\sigma, \sigma_0)\|_F^2 \leq 1 + (k-1)\epsilon} \mathcal{T}(\sigma) &\leq nk + n\alpha\rho\epsilon + 2\sqrt{(1 + \epsilon)(nk + 2n\alpha\rho\epsilon)m \log k} \\ &\quad + 2(1 + \epsilon)m \log k + O(\sqrt{n \log n}), \end{aligned}$$

By the assumption that  $\rho\sqrt{\alpha} > 2\sqrt{k \log k} + 2\sqrt{\alpha} \log k$ , it follows that for sufficiently large  $n$ ,

$$n\alpha\rho(1 - \epsilon) - O(\sqrt{n \log n}) \geq 2(1 + \epsilon) \left( \sqrt{(nk + 2n\alpha\rho\epsilon)m \log k} + m \log k \right),$$

and consequently, with high probability,

$$\max_{\sigma: \|\omega(\sigma, \sigma_0)\|_F^2 \leq 1 + (k-1)\epsilon} \mathcal{T}(\sigma) < \mathcal{T}(\sigma_0).$$

Let  $\hat{\sigma}_{\text{ML}} = \arg \max \mathcal{T}(\sigma)$  denote the maximum likelihood estimator of  $\sigma_0$ . Then with high probability,  $\|\omega(\hat{\sigma}_{\text{ML}}, \sigma_0)\|_F^2 \geq 1 + (k-1)\epsilon$ , which further implies that the trace overlap satisfies  $T(\hat{\sigma}_{\text{ML}}, \sigma_0) \geq 1 + (k-1)\epsilon$  in view of Lemma 2.

Finally, we argue that above the first moment bound, one can construct an estimator  $\widehat{M}$  of  $M$  such that  $\mathbb{E}[\|\widehat{M}\|_F^2] = O(n^2)$  and  $\mathbb{E}[\langle M, \widehat{M} \rangle] = \Omega(n)$ . Intuitively, if we can estimate the planted partition better than chance, then we should be able to construct an estimator of the signal matrix which out-performs the trivial one. Our proof uses the sample splitting method. Thinking of the rows of  $X$  as noisy observations of the cluster centers contained in the rows of  $M$ , we will project each observation into two orthogonal subspaces, use the first of these projections to build an estimator  $\hat{\sigma}$  of the planted partition  $\sigma_0$ , and finally combine  $\hat{\sigma}$  with the *second* projection to estimate the cluster centers. This technique gains us a subtle and important independence property: the partition we estimate based on the first projection is independent of the noise in the second.

Let us proceed. For  $\delta \in (0, 1)$  to be optimized later, let  $n_1 = (1-\delta)n \in \mathbb{N}$  and denote by  $X_1 \in \mathbb{R}^{m \times n_1}$  and  $X_2 \in \mathbb{R}^{m \times (n-n_1)}$  the restrictions of the data matrix  $X$  to its first  $n_1$  and final  $n-n_1$  columns respectively; define  $M_1$  and  $M_2$  analogously. We first reconstruct  $M_1$  from  $X_1$  with parameters  $\rho' = (\rho/n)n_1 = (1-\delta)\rho$  and  $\alpha' = m/n_1 = \alpha/(1-\delta)$ . Notice that our assumption  $\rho\sqrt{\alpha} > 2\sqrt{k}\log k + 2\sqrt{\alpha}\log k$  means that we can choose  $\delta$  sufficiently small to ensure  $\rho'\sqrt{\alpha'} > 2\sqrt{k}\log k + 2\sqrt{\alpha'}\log k$ . Let  $\hat{\sigma}$  denote the ML estimator of the planted partition based only on the data  $X_1$ . We have already shown that  $\|\omega(\hat{\sigma}, \sigma_0)\|_F^2 \geq 1 + (k-1)\epsilon$  with high probability.

Now we use  $\hat{\sigma}$  to construct an estimator of  $M_2$ . Specifically, let  $\widehat{S}$  be the  $m \times k$  indicator matrix for  $\hat{\sigma}$ ,  $\widehat{S}_{is} = \mathbf{1}_{\hat{\sigma}(i)=s}$ , and define  $\widehat{M}_2 = (k/m)\widehat{S}\widehat{S}^\dagger X_2$ . Then

$$\mathbb{E}\langle M_2, \widehat{M}_2 \rangle = \frac{k}{m}\mathbb{E}\langle M_2, \widehat{S}\widehat{S}^\dagger(M_2 + W_2) \rangle \stackrel{(a)}{=} \frac{k}{m}\mathbb{E}\langle M_2, \widehat{S}\widehat{S}^\dagger M_2 \rangle = \frac{k}{m}\mathbb{E}\|\widehat{S}^\dagger M_2\|_F^2,$$

where (a) follows because the noise  $W_2$  is independent of  $M_2$  and  $\widehat{S}$  and  $\mathbb{E}W_2 = 0$ . Furthermore,

$$\frac{k}{m}\mathbb{E}\|\widehat{S}^\dagger M_2\|_F^2 = \frac{k}{m}\frac{m^2}{k^2}\frac{\rho}{n}\sum_{\ell=1}^k\left\|\sum_s\omega_{\ell,s}(u_s^0 - \bar{u}^0)\right\|^2,$$

where  $u_s^0$  is the restriction of  $v_s^0$  to the last  $\delta n$  coordinates,  $\bar{u}^0$  is the restriction of  $\bar{v}^0$  to the last  $\delta n$  coordinates, and  $\omega_{\ell,s} = \omega(\hat{\sigma}, \sigma_0)$ . In view of (57), it follows from the last two displayed equations that  $\mathbb{E}\langle M_2, \widehat{M}_2 \rangle = \Omega(n)$ . One can additionally verify that  $\mathbb{E}\|\widehat{M}_2\|_F^2 = O(n^2)$ . Finally letting  $\widehat{M} = [\mathbf{0}_{m,n_1}, \widehat{M}_2]$  be the estimator, i.e., concatenating  $\widehat{M}_2$  on the left with  $n_1$  zero columns, we have shown that  $\mathbb{E}\|\widehat{M}\|_F^2 = O(n^2)$  and  $\mathbb{E}\langle M, \widehat{M} \rangle = \Omega(n)$ .

#### 4.4.2 Second moment lower bound for Gaussian mixture clustering

We first show that if  $\rho < \rho^{\text{lower}}$ , i.e.,  $\alpha\rho^2 < 2(k-1)\log(k-1)$ , then the second moment is bounded. Recall that  $S$  is the  $m \times k$  indicator matrix for a partition  $\sigma$  with  $S_{i,t} = \mathbf{1}_{\sigma(i)=t}$ , and  $V = [v_1, \dots, v_k]$ . Let  $\tau$  be an independent copy of  $\sigma$ , with indicator matrix  $T_{i,t} = \mathbf{1}_{\tau(i)=t}$  and  $U = [u_1, \dots, u_k]$  be an independent copy of  $V$ . Applying Lemma 1,

$$\begin{aligned}\mathbb{E}_{X \sim Q}\left(\frac{\mathbb{P}(X)}{\mathbb{Q}(X)}\right)^2 &= \mathbb{E}_{\sigma, \tau}\mathbb{E}_{v, u}\exp\left(\frac{\rho}{n}\langle (S - \mathbb{J}_{m,k}/k)V^\dagger, (T - \mathbb{J}_{m,k}/k)U^\dagger \rangle\right) \\ &= \mathbb{E}_{\sigma, \tau}\mathbb{E}_{v, u}\exp\left(\frac{\alpha\rho}{k}\langle U, V(\omega - \mathbb{J}/k) \rangle\right),\end{aligned}$$

where  $\omega$  is the overlap matrix between  $\sigma$  and  $\tau$ . The last equality follows from  $S^\dagger T = (m/k)\omega$  and  $S^\dagger \mathbb{J}_{m,k} = (m/k)\mathbb{J}_{k,k} = \mathbb{J}_{m,k}^\dagger T$ . Let  $\widetilde{V} = \sqrt{(k-1)/k}V$  and define  $\widetilde{U}$  analogously, so that these two matrices now contain i.i.d standard Gaussian entries. Evaluating the moment generating function for the Gaussian random

matrix  $\tilde{U}$  and invoking the standard linear algebra result that  $\|AB\|_F \leq \|A\|_2 \|B\|_F$ , it follows that

$$\begin{aligned} \mathbb{E}_{v,u} \exp\left(\frac{\alpha\rho}{k} \langle U, V(\omega - \mathbf{J}/k) \rangle\right) &= \mathbb{E}_{v,u} \exp\left(\frac{\alpha\rho}{k-1} \langle \tilde{U}, \tilde{V}(\omega - \mathbf{J}/k) \rangle\right) \\ &= \mathbb{E}_v \exp\left(\frac{\alpha^2 \rho^2}{2(k-1)^2} \left\| \tilde{V}(\omega - \mathbf{J}/k) \right\|_F^2\right) \\ &\leq \mathbb{E}_v \exp\left(\frac{\alpha^2 \rho^2}{2(k-1)^2} \|\tilde{V}\|_2^2 \|\omega - \mathbf{J}/k\|_F^2\right). \end{aligned}$$

In view of [48, Corollary 5.35],  $\tilde{V}$  is a ‘tall’ Gaussian random matrix with spectral norm tightly concentrated:

$$\Pr \left[ \|\tilde{V}\|_2 \leq \sqrt{n} + \sqrt{k} + \epsilon \right] \leq e^{-\epsilon^2/2}.$$

Since  $k$  is assumed to be fixed constant, with high probability  $\|\tilde{V}\|_2 \leq \sqrt{(1+\epsilon)n}$  for an arbitrarily small constant  $\epsilon > 0$ . Notice that if this event does not hold, the second moment becomes unbounded. We therefore will compute the second moment conditioned on the high probability event that  $\|\tilde{V}\|$  is not abnormally large. As we discussed in §3.2, we define the event

$$\mathcal{F} = \{V : \|\tilde{V}\|_2 \leq \sqrt{(1+\epsilon)n}\},$$

and conditional distributions  $\mathbb{P}'(v, \sigma) = \mathbb{P}(v, \sigma) \mathbf{1}_{\mathcal{F}} / \mathbb{P}(\mathcal{F})$  and  $\mathbb{P}'(X) = \mathbb{E}_{v, \sigma \sim \mathbb{P}'}[\mathbb{P}(X|v, \sigma)]$ . Notice that  $\mathbb{P}\{\mathcal{F}\} \rightarrow 1$ . Then the conditional second moment satisfies

$$\begin{aligned} \mathbb{E}_{X \sim Q} \left( \frac{\mathbb{P}'(X)}{Q(X)} \right)^2 &\leq \frac{1}{\mathbb{P}^2(\mathcal{F})} \mathbb{E}_{\sigma, \tau} \mathbb{E}_{v,u} \exp\left(\frac{\alpha\rho}{k} \langle U, V(\omega - \mathbf{J}/k) \rangle\right) \mathbf{1}_{U \in \mathcal{F}} \mathbf{1}_{V \in \mathcal{F}} \\ &\leq \frac{1}{\mathbb{P}^2(\mathcal{F})} \mathbb{E}_{\sigma, \tau} \mathbb{E}_{v,u} \exp\left(\frac{\alpha\rho}{k} \langle U, V(\omega - \mathbf{J}/k) \rangle\right) \mathbf{1}_{V \in \mathcal{F}} \\ &\leq \frac{1}{\mathbb{P}^2(\mathcal{F})} \mathbb{E}_{\sigma, \tau} \mathbb{E}_v \exp\left(\frac{\alpha^2 \rho^2}{2(k-1)^2} \|\tilde{V}\|_2^2 \|\omega - \mathbf{J}/k\|_F^2\right) \mathbf{1}_{V \in \mathcal{F}} \\ &\leq \frac{1}{\mathbb{P}^2(\mathcal{F})} \mathbb{E}_{\sigma, \tau} \exp\left((1+\epsilon) \frac{\alpha^2 \rho^2 n}{2(k-1)^2} \|\omega - \mathbf{J}/k\|_F^2\right). \end{aligned}$$

As in the submatrix localization problem, it remains to show that

$$\mathbb{E}_{\sigma, \tau} \exp\left((1+\epsilon) \frac{\alpha^2 \rho^2 n}{2(k-1)^2} \|\omega - \mathbf{J}/k\|_F^2\right) \quad (60)$$

is bounded by a constant for a sufficiently small  $\epsilon$ . This is guaranteed if  $\alpha\rho^2 < 1$  for  $k = 2$  and  $\alpha\rho^2 < 2(k-1) \log(k-1)$  for  $k > 2$ , in view of Lemmata 3, 4 and 5.

For reconstruction, notice that the conditioned planted model  $\mathbb{P}'$  is still an additive Gaussian model. Let  $\mathbb{P}'(M|X)$  denote the posterior distribution of  $M$  given  $X$  under  $\mathbb{P}'$ , i.e.,  $\mathbb{P}'(M|X) = \mathbb{P}(X|M)\mathbb{P}'(M)/\mathbb{P}'(X)$ . Let  $E'(X) = \mathbb{E}_{M \sim \mathbb{P}'(M|X)}[M]$  denote the posterior mean under  $\mathbb{P}'$ . Applying Theorem 4 with  $\mathbb{P}'$  and  $Q$ , we obtain

$$\lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M, X \sim \mathbb{P}'} \|M - E'(X)\|_F^2 = \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M \sim \mathbb{P}'} \|M\|_F^2 = \lim_{n \rightarrow \infty} \frac{1}{n \mathbb{P}(\mathcal{F})} \mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^2 \mathbf{1}_{\mathcal{F}} \right],$$

where the last equality follows from the definition of  $\mathbb{P}'$ . Let  $E(X) = \mathbb{E}_{M \sim \mathbb{P}(M|X)}[M]$  denote the posterior mean under  $\mathbb{P}$ . Then

$$\begin{aligned} \mathbb{E}_{M, X \sim \mathbb{P}'} \|M - E'(X)\|_F^2 &\leq \mathbb{E}_{M, X \sim \mathbb{P}'} \|M - E(X)\|_F^2 \\ &= \frac{1}{\mathbb{P}(\mathcal{F})} \mathbb{E}_{M, X \sim \mathbb{P}} \left[ \|M - E(X)\|_F^2 \mathbf{1}_{\mathcal{F}} \right] \\ &\leq \frac{1}{\mathbb{P}(\mathcal{F})} \mathbb{E}_{M, X \sim \mathbb{P}} \|M - E(X)\|_F^2, \end{aligned}$$

where the first inequality holds because  $E'(X)$  minimizes the mean squared error under  $\mathbb{P}'$ ; the second equality holds by the definition of  $\mathbb{P}'$ . Combining the last two displayed equations yields that

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M, X \sim \mathbb{P}} \|M - E(X)\|_F^2 \geq \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^2 \mathbf{1}_{\mathcal{F}} \right]. \quad (61)$$

Since

$$\|M\|_F = \frac{\rho}{n} \|(S - \mathbb{J}_{m,k}/k)V\|_F \leq \frac{\rho}{n} \|S - \mathbb{J}_{m,k}\|_F \|V\|_F = O(\|V\|_F),$$

it follows that

$$\mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^4 \right] = O(\mathbb{E}_V[\|V\|_F^4]) = O(n^2).$$

Hence,

$$\mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^2 \mathbf{1}_{\mathcal{F}^c} \right] \leq \sqrt{\mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^4 \right]} \mathbb{P}(\mathcal{F}^c) = o\left(\sqrt{\mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^4 \right]}\right) = o(n).$$

Combing the last displayed equation with (61) gives that

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M, X \sim \mathbb{P}} \|M - E(X)\|_F^2 \geq \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^2 \right].$$

Since  $E(X)$  minimizes the mean squared error under  $\mathbb{P}$ ,  $\mathbb{E}_{M, X \sim \mathbb{P}} \|M - E(X)\|_F^2 \leq \mathbb{E}_{M \sim \mathbb{P}} \|M\|_F^2$ , it follows that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M, X \sim \mathbb{P}} \|M - E(X)\|_F^2 = \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{M \sim \mathbb{P}} \left[ \|M\|_F^2 \right],$$

and thus  $\lim_{n \rightarrow \infty} (1/n) \mathbb{E}_{X \sim \mathbb{P}} \|E(X)\|_F^2 = 0$ . By (21) in Theorem 4, we conclude that for any estimator  $\widehat{M}$  with  $\|\widehat{M}\|_F^2 = O(n)$ ,  $\mathbb{E}[\langle M, \widehat{M} \rangle] = o(n)$ .

## 4.5 Proof of Theorem 4

We give the proof for i.i.d. Gaussian noise, using a type of interpolation argument where we vary the signal to noise ratio; the proof for Wigner noise is identical. Assume that  $X(\beta) = \sqrt{\beta}M + W$  in the planted model and  $X = W$  in the null model, where  $\beta \in [0, 1]$  is a signal-to-noise ratio parameter (analogous to an inverse temperature) and  $W_{ij} \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(0, 1)$  for all  $i, j$ .

First recall that the Bayes-optimal estimator minimizing the mean squared error is the expectation of the posterior distribution,

$$\widehat{M}_{\text{MMSE}}(X) = \mathbb{E}[M|X],$$

so that the (rescaled) minimum mean squared error is given by

$$\text{MMSE}(\beta) = \frac{1}{n} \mathbb{E} \|M - \mathbb{E}[M|X]\|_F^2. \quad (62)$$

We will start by proving that, for all  $\beta \in [0, 1]$ , the MMSE tends to that of the trivial estimator  $\widehat{M} = 0$ ,

$$\limsup_{n \rightarrow \infty} \text{MMSE}(\beta) = \beta \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|M\|_F^2. \quad (63)$$

Let us compute the mutual information  $I(\beta)$  between  $M$  and  $X$ :

$$\begin{aligned} I(\beta) &= \mathbb{E}_{M, X} \log \frac{\mathbb{P}(X|M)}{\mathbb{P}(X)} \\ &= \mathbb{E}_X \log \frac{\mathbb{Q}(X)}{\mathbb{P}(X)} + \mathbb{E}_{M, X} \log \frac{\mathbb{P}(X|M)}{\mathbb{Q}(X)} \\ &= -D_{\text{KL}}(\mathbb{P} \parallel \mathbb{Q}) + \mathbb{E}_{M, X} \left[ \sqrt{\beta} \langle M, X \rangle - \frac{\beta \|M\|_F^2}{2} \right] \\ &= -D_{\text{KL}}(\mathbb{P} \parallel \mathbb{Q}) + \frac{\beta}{2} \mathbb{E}_M \|M\|_F^2. \end{aligned} \quad (64)$$



By assumption, we have  $D_{\text{KL}}(\mathbb{P}||\mathbb{Q}) = o(n)$ . This holds for  $\beta = 1$ ; by the data processing inequality for KL divergence [45, Theorem 2.2], this holds for all  $\beta < 1$  as well. Thus (64) becomes

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\beta) = \frac{\beta}{2} \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|M\|_F^2. \quad (65)$$

Next we compute the MMSE. Recall the I-MMSE formula [22],

$$\frac{dI(\beta)}{d\beta} = \frac{n}{2} \text{MMSE}(\beta), \quad (66)$$

which can also be viewed as a classic formula in thermodynamics. Note that the MMSE is by definition bounded above by the squared error of the trivial estimator  $\widehat{M} = 0$ , so that for all  $\beta$  we have

$$\text{MMSE}(\beta) \leq \frac{1}{n} \mathbb{E} \|M\|_F^2. \quad (67)$$

Combining these we have

$$\begin{aligned} \frac{1}{2} \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} [\|M\|_F^2] &\stackrel{(a)}{=} \lim_{n \rightarrow \infty} \frac{1}{n} I(1) \\ &\stackrel{(b)}{=} \frac{1}{2} \lim_{n \rightarrow \infty} \int_0^1 \text{MMSE}(\beta) d\beta \\ &\stackrel{(c)}{\leq} \frac{1}{2} \int_0^1 \limsup_{n \rightarrow \infty} \text{MMSE}(\beta) d\beta \\ &\stackrel{(d)}{\leq} \frac{1}{2} \int_0^1 \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|M\|_F^2 dt \\ &= \frac{1}{2} \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|M\|_F^2, \end{aligned}$$

where (a) and (b) hold due to (65) and (66), (c) follows from the Fatou lemma, and (d) follows from (67). Since we began and ended with the same expression, these inequalities must all be equalities. In particular, since (c) holds with equality, we have

$$\limsup_{n \rightarrow \infty} \text{MMSE}(\beta) = \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|M\|_F^2 \quad (68)$$

for almost all  $\beta \in [0, 1]$ . Since  $\text{MMSE}(\beta)$  is a non-increasing function of  $\beta$ , its limit  $\limsup_{n \rightarrow \infty} \text{MMSE}(\beta)$  is also non-increasing in  $\beta$ . Therefore, (68) holds for all  $\beta \in [0, 1]$ . This completes the proof of our claim that the optimal estimator has the same asymptotic MMSE as the trivial one.

To show that the optimal estimator actually converges to the trivial one, we expand the definition of  $\text{MMSE}(\beta)$  in (62) and subtract (68) from it. This gives

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} [-2\langle M, \mathbb{E}[M|X] \rangle + \|\mathbb{E}[M|X]\|_F^2] = 0. \quad (69)$$

Note that  $\mathbb{E} \langle M, \mathbb{E}[M|X] \rangle$  is the expected inner product between the ground truth and a draw from the posterior. By the Nishimori identity [25] or the tower property of conditional expectation, this is equal to the expected inner product between two independent draws from the posterior. By linearity of the inner product, this gives

$$\mathbb{E} \langle M, \mathbb{E}[M|X] \rangle = \mathbb{E} \langle \mathbb{E}[M|X], \mathbb{E}[M|X] \rangle = \mathbb{E} \|\mathbb{E}[M|X]\|_F^2,$$

and combining this with (69) gives (where  $\limsup$  becomes  $\liminf$  because of a sign change)

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \|\mathbb{E}[M|X]\|_F^2 = 0. \quad (70)$$

Furthermore, for any estimator  $\widehat{M} = \widehat{M}(X)$  such that  $\mathbb{E}_X \|\widehat{M}\|_F^2 = O(n)$ ,

$$\mathbb{E}_{M,X} \langle M, \widehat{M} \rangle = \mathbb{E}_X \langle \mathbb{E}[M|X], \widehat{M} \rangle \leq \mathbb{E}_X \left[ \|\mathbb{E}[M|X]\|_F \|\widehat{M}\|_F \right] \leq \sqrt{\mathbb{E}_X [\|\mathbb{E}[M|X]\|_F^2] \mathbb{E}_X [\|\widehat{M}\|_F^2]}$$

and thus the desired (21) holds.

Finally, we note that if  $M$  is of the form  $(1/\sqrt{n})UV^\dagger$  where the rows of  $U$  and  $V$  are independently and identically distributed according to some priors, then  $\lim_{n \rightarrow \infty} \text{MMSE}(\beta)$  exists by [20, Proposition III.2], and the  $\liminf$  in (20) and (21) can be replaced by  $\lim$ . Then the MMSE estimator  $\widehat{M}_{\text{MMSE}} = \mathbb{E}[M|X]$  tends to the trivial estimator  $\widehat{M} = 0$  as claimed.

## 4.6 Proof of Theorem 5

We give the proof of i.i.d. Gaussian noise; the proof for Wigner noise is identical. Let

$$Z(X) := \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} = \mathbb{E}_M \left[ e^{\langle M, X \rangle - \|M\|_F^2/2} \right].$$

By the definition of KL divergence,

$$\begin{aligned} & D_{\text{KL}}(\mathbb{P}' \|\mathbb{Q}) - D_{\text{KL}}(\mathbb{P} \|\mathbb{Q}) \\ &= \mathbb{E}_{X \sim \mathbb{P}'} \left[ \log \frac{\mathbb{P}'(X)}{\mathbb{Q}(X)} \right] - \mathbb{E}_{X \sim \mathbb{P}} \left[ \log \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right] \\ &= \mathbb{E}_{X \sim \mathbb{P}'} \left[ \log \frac{\mathbb{P}'(X)}{\mathbb{P}(X)} \right] + \mathbb{E}_{X \sim \mathbb{P}'} \left[ \log \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right] - \mathbb{E}_{X \sim \mathbb{P}} \left[ \log \frac{\mathbb{P}(X)}{\mathbb{Q}(X)} \right] \\ &\geq \mathbb{E}_{X \sim \mathbb{P}'} [\log Z(X)] - \mathbb{E}_{X \sim \mathbb{P}} [\log Z(X)], \end{aligned}$$

where the last inequality follows because  $D_{\text{KL}}(\mathbb{P}' \|\mathbb{P}) = \mathbb{E}_{X \sim \mathbb{P}'} [\log(\mathbb{P}'(X)/\mathbb{P}(X))] \geq 0$ . Furthermore,

$$\begin{aligned} & \mathbb{E}_{X \sim \mathbb{P}'} [\log Z(X)] - \mathbb{E}_{X \sim \mathbb{P}} [\log Z(X)] \\ &= \mathbb{E}_{\mathbb{P}_M} \frac{1}{\mathbb{P}(F_M|M)} \mathbb{E}_{\mathbb{P}(X|M)} [(\mathbf{1}_{F_M} - \mathbb{P}(F_M|M)) \log Z(X)] \\ &\geq -\mathbb{E}_{\mathbb{P}_M} \frac{1}{\mathbb{P}(F_M|M)} \sqrt{\mathbb{P}(F_M|M) (1 - \mathbb{P}(F_M|M))} \mathbb{E}_{\mathbb{P}(X|M)} [\log^2 Z(X)] \\ &= -o(1) \times \mathbb{E}_{\mathbb{P}_M} \sqrt{\mathbb{E}_{\mathbb{P}(X|M)} [\log^2 Z(X)]}, \end{aligned}$$

where we use the Cauchy-Schwarz inequality in the third line, and the assumption that  $\mathbb{P}(F_M|M) = 1 + o(1)$  uniformly over  $M$  in the last line.

By the assumptions that  $\|M\|_2 = O(\sqrt{n})$  and  $\|M\|_* = O(\sqrt{n})$  uniformly over all  $M$ , and in view of  $\langle M, X \rangle \leq \|M\|_* \|X\|_2$  and  $\|M\|_F^2 \leq \|M\|_* \|M\|_2$ , we have that  $|\log Z(X)| \leq O(\sqrt{n} \|X\|_2) + O(n)$ . Therefore,

$$\mathbb{E}_{\mathbb{P}(X|M)} [\log^2 Z(X)] = O(n^2) + O(n) \times \mathbb{E}_{\mathbb{P}(X|M)} [\|X\|_2^2] = O(n^2) + O(n) \times \mathbb{E}_W [\|M + W\|_2^2] = O(n^2),$$

where the last inequality holds because  $\mathbb{E}_W [\|M + W\|_2^2] \leq 2\|M\|_2^2 + 2\mathbb{E}_W [\|W\|_2^2]$  and  $\mathbb{E}_W [\|W\|_2^2] = O(n)$ . Combining the last three displayed equations together yields that

$$D_{\text{KL}}(\mathbb{P}' \|\mathbb{Q}) - D_{\text{KL}}(\mathbb{P} \|\mathbb{Q}) \geq \mathbb{E}_{X \sim \mathbb{P}'} [\log Z(X)] - \mathbb{E}_{X \sim \mathbb{P}} [\log Z(X)] \geq -o(n).$$

## Acknowledgments

We thank Yihong Wu, Lenka Zdeborová, Florent Krzakala, Thibault Lesieur, Caterina de Bacco, Alex Russell, Andrea Montanari, and Cosma Shalizi for helpful discussions. C. Moore and J. Banks are supported

by the John Templeton Foundation and the ARO under contract W911NF-12-R-0012. J. Xu is supported by Simons-Berkeley Research Fellowship. R. Vershynin is supported by NSF Grant DMS 1265782 and U.S. Air Force Grant FA9550-14-1-0009. Much of this work was done while the authors were visiting the Simons Institute for the Theory of Computing.

## References

- [1] E. Abbe and C. Sandon. Detection in the stochastic block model with multiple clusters: proof of the achievability conjectures, acyclic bp, and the information-computation gap. arXiv 1512.09080, Dec 2015.
- [2] D. Achlioptas and F. McSherry. On spectral learning of mixtures of distributions. In *Learning Theory*, pages 458–469. Springer, 2005.
- [3] D. Achlioptas and A. Naor. The two possible values of the chromatic number of a random graph. *Annals of Mathematics*, 162:1335–1351, 2005.
- [4] D. J. Aldous. Exchangeability and related topics. In *École d’été de probabilités de Saint-Flour, XIII—1983*, volume 1117 of *Lecture Notes in Math.*, pages 1–198. Springer, Berlin, 1985.
- [5] A. A. Amini and M. J. Wainwright. High-dimensional analysis of semidefinite relaxations for sparse principal components. *Ann. Statist.*, 37(5B):2877–2921, 10 2009.
- [6] E. Arias-Castro and N. Verzelen. Community detection in dense random networks. *Ann. Statist.*, 42(3):940–969, 06 2014.
- [7] Z. Bai and J. W. Silverstein. *Spectral analysis of large dimensional random matrices*. Springer Series in Statistics. Springer, New York, second edition, 2010.
- [8] J. Baik, G. Ben Arous, and S. Péché. Phase transition of the largest eigenvalue for nonnull complex sample covariance matrices. *Annals of Probability*, pages 1643–1697, 2005.
- [9] J. Banks, C. Moore, J. Neeman, and P. Netrapalli. Information-theoretic thresholds for community detection in sparse networks. In *Proceedings of the 29th Conference on Learning Theory, COLT 2016, New York, NY, June 23-26 2016*, pages 383–416, 2016.
- [10] J. Banks, C. Moore, R. Vershynin, and J. Xu. Information-theoretic bounds and phase transitions in clustering, sparse PCA, and submatrix localization. *arXiv:1607.05222*, 2016.
- [11] F. Benaych-Georges and R. R. Nadakuditi. The eigenvalues and eigenvectors of finite, low rank perturbations of large random matrices. *Advances in Mathematics*, 227(1):494–521, 2011.
- [12] Q. Berthet, P. Rigollet, et al. Optimal detection of sparse principal components in high dimension. *The Annals of Statistics*, 41(4):1780–1815, 2013.
- [13] L. Birgé. An alternative point of view on Lepski’s method. *State of the art in probability and statistics*, pages 113–133, 2001.
- [14] C. Bordenave, M. Lelarge, and L. Massoulié. Non-backtracking spectrum of random graphs: Community detection and non-regular ramanujan graphs. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS*, pages 1347–1357, 2015.
- [15] C. Butucea and Y. I. Ingster. Detection of a sparse submatrix of a high-dimensional noisy matrix. *Bernoulli*, 19(5B):2652–2688, 11 2013.
- [16] T. Cai, Z. Ma, and Y. Wu. Optimal estimation and rank detection for sparse spiked covariance matrices. *Probability Theory and Related Fields*, 161(3):781–815, 2015.

- [17] Y. Chen and J. Xu. Statistical-computational tradeoffs in planted problems and submatrix localization with a growing number of clusters and submatrices. In *Proceedings of ICML 2014 (Also arXiv:1402.1267)*, Feb 2014.
- [18] 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, 2011.
- [19] A. Decelle, F. Krzakala, C. Moore, and L. Zdeborová. Inference and phase transitions in the detection of modules in sparse networks. *Physical Review Letters*, 107(6):065701, 2011.
- [20] Y. Deshpande and A. Montanari. Information-theoretically optimal sparse PCA. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 2197–2201, June 2014.
- [21] Y. Deshpande and A. Montanari. Sparse PCA via covariance thresholding. In *Advances in Neural Information Processing Systems*, pages 334–342, 2014.
- [22] D. Guo, S. Shamai, and S. Verdú. Mutual information and minimum mean-square error in gaussian channels. *IEEE Trans. on Information Theory*, 51, 2005.
- [23] B. Hajek, Y. Wu, and J. Xu. Information limits for recovering a hidden community. arXiv 1509.07859, September 2015.
- [24] B. Hajek, Y. Wu, and J. Xu. Submatrix localization via message passing. arXiv 1510.09219, October 2015.
- [25] Y. Iba. The nishimori line and bayesian statistics. *Journal of Physics A: Mathematical and General*, 32(21):3875, 1999.
- [26] Y. I. Ingster and I. A. Suslina. *Nonparametric goodness-of-fit testing under Gaussian models*. Springer, New York, NY, 2003.
- [27] E. S. P. J. Neyman. On the problem of the most efficient tests of statistical hypotheses. *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, 231:289–337, 1933.
- [28] I. M. Johnstone and A. Y. Lu. On consistency and sparsity for principal components analysis in high dimensions. *Journal of the American Statistical Association*, 104(486):682–693, June 2009.
- [29] R. Kannan, H. Salmasian, and S. Vempala. The spectral method for general mixture models. *SIAM Journal on Computing*, 38(3):1141–1156, 2008.
- [30] R. Kannan and S. Vempala. Spectral algorithms. <http://www.cc.gatech.edu/~vempala/spectralbook.pdf>, 2009.
- [31] M. Kolar, S. Balakrishnan, A. Rinaldo, and A. Singh. Minimax localization of structural information in large noisy matrices. In *Advances in Neural Information Processing Systems*, 2011.
- [32] R. Krauthgamer, B. Nadler, and D. Vilenchik. Do semidefinite relaxations solve sparse PCA up to the information limit? *The Annals of Statistics*, 43(3):1300–1322, June 2015.
- [33] F. Krzakala, C. Moore, E. Mossel, J. Neeman, A. Sly, L. Zdeborová, and P. Zhang. Spectral redemption in clustering sparse networks. *Proceedings of the National Academy of Sciences*, 110(52):20935–20940, 2013.
- [34] F. Krzakala, J. Xu, and L. Zdeborová. Mutual information in rank-one matrix estimation. arXiv 1603.08447, March 2016.

- [35] M. Lelarge and L. Miolane. Fundamental limits of symmetric low-rank matrix estimation. arXiv:1611.03888, Nov. 2016.
- [36] T. Lesieur, C. D. Bacco, J. Banks, F. Krzakala, C. Moore, and L. Zdeborová. Phase transitions and optimal algorithms in high-dimensional gaussian mixture clustering. *Arxiv preprint arxiv:1610.02918*, 2016.
- [37] T. Lesieur, F. Krzakala, and L. Zdeborová. MMSE of probabilistic low-rank matrix estimation: Universality with respect to the output channel. In *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 680–687, Sept 2015.
- [38] T. Lesieur, F. Krzakala, and L. Zdeborová. Phase transitions in sparse PCA. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 1635–1639. IEEE, 2015.
- [39] E. Mossel, J. Neeman, and A. Sly. Belief propagation, robust reconstruction and optimal recovery of block models. In *Proceedings of The 27th Conference on Learning Theory, COLT 2014, Barcelona, Spain, June 13-15, 2014*, pages 356–370, 2014.
- [40] E. Mossel, J. Neeman, and A. Sly. Reconstruction and estimation in the planted partition model. *Probability Theory and Related Fields*, 162(3-4):431–461, 2015.
- [41] D. Paul. Asymptotics of sample eigenstructure for a large dimensional spiked covariance model. *Statistica Sinica*, 17(4):1617–1642, 2007.
- [42] S. Péché. The largest eigenvalue of small rank perturbations of hermitian random matrices. *Probability Theory and Related Fields*, 134(1):127–173, 2006.
- [43] A. Perry, A. S. Wein, and A. S. Bandeira. Statistical limits of spiked tensor models. arXiv:1612.07728, Dec. 2016.
- [44] A. Perry, A. S. Wein, A. S. Bandeira, and A. Moitra. Optimality and sub-optimality of PCA for spiked random matrices and synchronization. arXiv:1609.05573, Sept. 2016.
- [45] Y. Polyanskiy and Y. Wu. Lecture Notes on Information Theory. Feb 2015. <http://www.ifp.illinois.edu/~yihongwu/teaching/itlectures.pdf>.
- [46] N. Srebro, G. Shakhnarovich, and S. Roweis. An investigation of computational and informational limits in gaussian mixture clustering. In *Proceedings of the 23rd International Conference on Machine Learning, ICML '06*, pages 865–872, New York, NY, USA, 2006. ACM.
- [47] S. Vempala and G. Wang. A spectral algorithm for learning mixture models. *J. Comput. Syst. Sci.*, 68(4):841–860, June 2004.
- [48] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. *Arxiv preprint arxiv:1011.3027*, 2010.
- [49] N. Verzelen and E. Arias-Castro. Community detection in sparse random networks. *arXiv preprint arXiv:1308.2955*, 2013.