Testing Correlation of Unlabeled Random Graphs

By Yihong Wu¹, Jiaming Xu²,*, and Sophie H. Yu²,†

¹Department of Statistics and Data Science, Yale University, yihong.wu@yale.edu
²The Fuqua School of Business, Duke University, *jx77@duke.edu; †haoyang.yu@duke.edu

We study the problem of detecting the edge correlation between two random graphs with n unlabeled nodes. This is formalized as a hypothesis testing problem, where under the null hypothesis, the two graphs are independently generated; under the alternative, the two graphs are edge-correlated under some latent node correspondence, but have the same marginal distributions as the null. For both Gaussian-weighted complete graphs and dense Erdős-Rényi graphs (with edge probability \(n^{-\alpha(1)}\)), we determine the sharp threshold at which the optimal testing error probability exhibits a phase transition from zero to one as \(n \to \infty\). For sparse Erdős-Rényi graphs with edge probability \(n^{-\Omega(1)}\), we determine the threshold within a constant factor.

The proof of the impossibility results is an application of the conditional second-moment method, where we bound the truncated second moment of the likelihood ratio by carefully conditioning on the typical behavior of the intersection graph (consisting of edges in both observed graphs) and taking into account the cycle structure of the induced random permutation on the edges. Notably, in the sparse regime, this is accomplished by leveraging the pseudoforest structure of subcritical Erdős-Rényi graphs and a careful enumeration of subpseudoforests that can be assembled from short orbits of the edge permutation.

CONTENTS

1 Introduction .................................................. 2
1.1 Main results .............................................. 4
1.2 Test statistic and proof techniques ....................... 6
1.3 Connection to the literature ............................. 8
1.4 Notation and paper organization ...................... 10
2 First Moment Method for Detection ................... 10
2.1 Proof of Theorem 1: positive part ..................... 12
2.2 Proof of Theorem 2: positive part ..................... 12
3 Unconditional Second Moment Method and Obstructions 13
3.1 Node permutation, edge permutation, and cycle decomposition 13
3.2 Second moment calculation ............................ 14
3.3 Obstruction from short orbits ......................... 18
4 Conditional Second Moment Method: Dense regime 19
4.1 Sharp threshold for the Gaussian model ................. 20
5 Conditional Second Moment Method: Sparse regime 24
5.1 Classification of edge orbits ............................ 30
5.2 Orbit graph and backbone graph ..................... 30
5.3 Warm-up: Generating function of orbit forests ........ 32
5.4 Proof of Theorem 4: Generating function of orbit pseudoforests 34

MSC2020 subject classifications: Primary 62H15, 05C80; secondary 05C60, 68Q87, 05C30.
Keywords and phrases: Hypothesis testing, Graph matching, Unlabeled graphs, Erdős-Rényi graphs, Conditional second moment method, Cycle decomposition.
1. **Introduction.** Understanding and quantifying the correlation between datasets are among the most fundamental tasks in statistics. In many modern applications, the observations may not be in the familiar form of vectors but rather graphs. Furthermore, the node labels may be absent or scrambled, in which case one needs to decide the similarity between these *unlabeled graphs* on the sheer basis of their topological structures. Equivalently, it amounts to determining whether there exists a node correspondence under which the (weighted) edges of the two graphs are correlated. This problem arises naturally in a wide range of fields:

- In social network analysis, one is interested in deciding whether two friendship networks on different social platforms share structural similarities, where the node labels are frequently anonymized due to privacy considerations [35, 36].
- In computer vision, 3-D shapes are commonly represented by geometric graphs, where nodes are subregions and edges encode the adjacency relationships between different regions. A key building block for pattern recognition and image processing is to determine whether two graphs correspond to the same object that undergoes different rotations or deformations (changes in pose or topology) [11, 7].
- In computational biology, an important task is to assess the correlation of two biological networks in two different species so as to enrich one dataset using the other [44, 47].
- In natural language processing, the so-called ontology alignment problem refers to uncovering the correlation between two knowledge graphs that are in either different languages [23] or different domains (e.g. Library of Congress versus Wikipedia [6]).

Inspired by the hypothesis testing model proposed by Barak et al [5], we formulate a general problem of testing network correlation as follows. Let \( G = (\{n\}, W) \) denote a weighted undirected graph on the node set \( \{n\} \triangleq \{1, \ldots, n\} \) with weighted adjacency matrix \( W \), where \( W_{ii} = 0 \) and for any \( 1 \leq i < j \leq n \), \( W_{ij} = 1 \) (or the edge weight) if \( i \) and \( j \) are adjacent and \( W_{ij} = 0 \) otherwise. Recall that two weighted graphs \( G = (\{n\}, W) \) and \( H = (\{n\}, W') \) are isomorphic and denoted by \( G \cong H \) if there exists a permutation (called a graph isomorphism) \( \pi \) on \( \{n\} \) such that \( W_{ij} = W'_{\pi(i)\pi(j)} \) for all \( i, j \). Given a weighted graph \( G \), its *isomorphism class* \( \overline{G} \) is the equivalence class \( \overline{G} = \{ H : H \cong G \} \). We refer to an isomorphism class as an unlabeled graph and \( \overline{G} \) as the unlabeled version of \( G \).

**Problem 1** (Testing correlation of unlabeled graphs). Let \( G_1 = (\{n\}, W) \) and \( G_2 = (\{n\}, W') \) be two weighted random graphs, where the edge weights \{\( W_{ij}, W'_{ij} \) : \( 1 \leq i < j \leq n \) \}
are i.i.d. pairs of random variables, and \( W_{ij} \) and \( W'_{ij} \) have the same marginal distribution. Under the null hypothesis \( \mathcal{H}_0 \), \( W_{ij} \) and \( W'_{ij} \) are independent; under the alternative hypothesis \( \mathcal{H}_1 \), \( W_{ij} \) and \( W'_{ij} \) are correlated. Given the unlabeled versions of \( G_1 \) and \( G_2 \), i.e., their isomorphism classes \( \overline{G}_1 = \{ G : G \cong G_1 \} \) and \( \overline{G}_2 = \{ G : G \cong G_2 \} \), the goal is to test \( \mathcal{H}_0 \) versus \( \mathcal{H}_1 \).

Note that were the node labels of \( G_1 \) and \( G_2 \) observed, one could stack all the edge weights as a vector and reduce the problem to simply testing the correlation of two random vectors. However, when the node labels are unobserved, the inherent correlation between \( G_1 \) and \( G_2 \) is obscured by the latent node correspondence, making the testing problem significantly more challenging. Indeed, since the observed graphs are unlabeled, the test needs to rely on graph invariants (i.e., graph properties that are invariant under graph isomorphisms), such as subgraphs counts (e.g. the number of edges and triangles) and spectral information (e.g. eigenvalues of adjacency matrices or Laplacians).

In this work, we focus on the following two special cases of particular interests:

- (Gaussian Wigner model). Suppose that under \( \mathcal{H}_1 \), each pair of edge weights \( W_{ij} \) and \( W'_{ij} \) are jointly normal with zero mean, unit variance and correlation coefficient \( \rho \in [0, 1] \); under \( \mathcal{H}_0 \), \( W_{ij} \) and \( W'_{ij} \) are independent standard normals. Note that marginally \( W, W' \) are two Gaussian Wigner random matrices under both \( \mathcal{H}_0 \) and \( \mathcal{H}_1 \). The correlated Gaussian Wigner model is proposed in [16] as a prototypical model for random graph matching and further studied in [17, 21].

- (Erdős-Rényi random graph). Let \( \mathcal{G}(n, p) \) denote the Erdős-Rényi random graph model with edge probability \( p \in [0, 1] \). Consider the edge sampling process that generates a children graph from a given parent graph by keeping each edge independently with probability \( s \in [0, 1] \). Suppose that under \( \mathcal{H}_1 \), \( G_1 \) and \( G_2 \) are independently subsampled from a common parent graph \( G \sim \mathcal{G}(n, p) \); under \( \mathcal{H}_0 \), \( G_1 \) and \( G_2 \) are independently subsampled from two independent parent graphs \( G, G' \sim \mathcal{G}(n, p) \), respectively. See Fig. 1 for an illustration.

Note that \( G_1 \) and \( G_2 \) are both instances of \( \mathcal{G}(n, ps) \) that are independent under \( \mathcal{H}_0 \) and correlated under \( \mathcal{H}_1 \). This specific model of correlated Erdős-Rényi random graphs is initially proposed by [38] and has been widely used for studying the problem of matching random graphs [12, 13, 5, 34, 15, 14, 16, 18, 22, 24].

We further focus on the following two natural types of testing guarantees.

**Definition 1 (Strong and weak detection).** Let \( \mathcal{Q} \) and \( \mathcal{P} \) denote the probability measure under \( \mathcal{H}_0 \) and \( \mathcal{H}_1 \), respectively. We say a test statistic \( T(\overline{G}_1, \overline{G}_2) \) with threshold \( \tau \) achieves

- **strong detection** if the sum of type I and type II error converges to 0 as \( n \to \infty \), that is,

\[
\lim_{n \to \infty} \left[ \mathcal{P} \left( T(\overline{G}_1, \overline{G}_2) < \tau \right) + \mathcal{Q} \left( T(\overline{G}_1, \overline{G}_2) \geq \tau \right) \right] = 0;
\]

- **weak detection**, if the sum of type I and type II error is bounded away from 1 as \( n \to \infty \), that is,

\[
\limsup_{n \to \infty} \left[ \mathcal{P} \left( T(\overline{G}_1, \overline{G}_2) < \tau \right) + \mathcal{Q} \left( T(\overline{G}_1, \overline{G}_2) \geq \tau \right) \right] < 1.
\]

Note that strong detection requires the test statistic to determine with high probability whether \( (\overline{G}_1, \overline{G}_2) \) is drawn from \( \mathcal{Q} \) or \( \mathcal{P} \), while weak detection only aims at strictly outperforming random guessing. It is well-known that the minimal sum of type I and type II error is \( 1 - TV(\mathcal{P}, \mathcal{Q}) \), achieved by the likelihood ratio test, where \( TV(\mathcal{P}, \mathcal{Q}) = \frac{1}{2} \int |d\mathcal{P} - d\mathcal{Q}| \)
(a) Two labeled graphs $G_1$ and $G_2$ are subsampled from a common parent graph according to the correlated Erdős-Rényi graph model with $n = 20$, $p = 0.1$, and $s = 0.8$ under $\mathcal{H}_1$, where blue edges are edges sampled from the parent graph, and red, dashed edges are edges deleted from the parent graph.

(b) Two observed graphs $\overline{G}_1$ and $\overline{G}_2$ are the unlabeled versions of $G_1$ and $G_2$, respectively.

Fig 1: Example of testing correlation of two Erdős-Rényi random graphs. The task is to test the underlying hypothesis ($\mathcal{H}_0$ or $\mathcal{H}_1$) based on the two unlabeled graphs in panel (b).

denotes the total variation distance between $\mathcal{P}$ and $\mathcal{Q}$. Thus strong and weak detection are equivalent to $\lim_{n \to \infty} TV(\mathcal{P}, \mathcal{Q}) = 1$ and $\lim \inf_{n \to \infty} TV(\mathcal{P}, \mathcal{Q}) > 0$, respectively.

Recent work [5] developed a polynomial-time test based on counting certain subgraphs that correctly distinguishes between $\mathcal{H}_0$ and $\mathcal{H}_1$ with probability at least $0.9$, provided that the edge subsampling probability $s = \Omega(1)$ and the average degree satisfies certain conditions; however, the fundamental limit of detection remains elusive. The main objective of this paper is to obtain tight necessary and sufficient conditions for strong and weak detection.

1.1. Main results.

**Theorem 1 (Gaussian Wigner model).** If

\[
\rho^2 \geq \frac{4 \log n}{n - 1},
\]
then \( TV(P, Q) = 1 + o(1) \). Conversely, if
\[
\rho^2 \leq \frac{(4 - \epsilon) \log n}{n}
\]
for any constant \( \epsilon > 0 \), then \( TV(P, Q) = o(1) \).

**Theorem 2 (Erdős-Rényi graphs).** If
\[
s^2 \geq \frac{2 \log n}{(n - 1)p \left( \log \frac{1}{p} - 1 + p \right)},
\]
then \( TV(P, Q) = 1 - o(1) \).

Conversely, assume that \( p \) is bounded away from 1.

* (Dense regime): If \( p = n^{-o(1)} \) and
\[
s^2 \leq \frac{(2 - \epsilon) \log n}{np \left( \log \frac{1}{p} - 1 + p \right)}
\]
for any constant \( \epsilon > 0 \), then \( TV(P, Q) = o(1) \).

* (Sparse regime): If \( p = n^{-\Omega(1)} \) and
\[
s^2 \leq \frac{1 - \omega(n^{-1/3})}{np} \wedge c_0
\]
for some universal constant \( c_0 (c_0 = 0.01 \text{ works}) \), then \( TV(P, Q) = 1 - \Omega(1) \). In addition, if (7) holds and \( s = o(1) \), then \( TV(P, Q) = o(1) \).

For the Gaussian Wigner model, Theorem 1 shows that the fundamental limit of detection in terms of the limiting value of \( \frac{np^2}{\log n} \) exhibits a sharp threshold at 4, above which strong detection is possible and below which weak detection is impossible, a phenomenon known as the “all-or-nothing” phase transition [41]. In the Erdős-Rényi model, for dense parent graphs with \( p = n^{-o(1)} \) and bounded away from 1, Theorem 2 shows that a similar sharp threshold for \( \frac{nps^2}{\log n} \) exists at 2. Curiously, the function \( p \mapsto p \left( \log \frac{1}{p} - 1 + p \right) \) is not monotone and uniquely maximized at \( p_* \approx 0.203 \), the solution to the equation \( \log \frac{1}{p} = 2(1 - p) \). This shows the counterintuitive fact that the parent graph with edge density \( p_* \) is the “easiest” for detection as it requires the lowest sampling probability \( s \); nevertheless, such non-monotonicity in the detection threshold can be anticipated by noting that in the extreme cases of \( p = 0 \) and \( p = 1 \), the observed two graphs are always independent and the two hypotheses are identical.

For sparse parent graphs with \( p = n^{-\Omega(1)} \), the picture is less clear:

* Unbounded average degree \( np = \omega(1) \): For simplicity, assume that \( p = n^{-\alpha + o(1)} \) for some constant \( \alpha \in (0, 1] \). Theorem 2 implies that strong detection is possible if \( \liminf nps^2 > \frac{2}{\alpha} \) and weak detection is impossible if \( \limsup nps^2 < 1 \); these two conditions differ by a constant factor.

* Bounded average degree \( np = \Theta(1) \): For simplicity, assume that \( p = d/n \) for some constant \( d > 0 \). Theorem 2 shows that strong detection is possible if \( s^2 > \frac{2}{d} \) and impossible if \( s^2 < c_0 \wedge \frac{1}{d} \).

For both cases, it is an open problem to determine the sharp threshold for detection (or the existence thereof).
REMARK 1 (Simple test for weak detection). In the non-trivial case of \( p = \omega(1/n^2) \) and \( p \) bounded away from 1, as long as the sampling problem \( s \) is any constant, weak detection can be achieved in linear time by simply comparing the number of edges of the two observed graphs. Intuitively, their difference behaves like a centered Gaussian with slightly different scale parameters under the two hypotheses which can then be distinguished non-trivially (see Section 7.1 for a rigorous justification). In view of the negative result for weak detection in Theorem 2, we conclude that for parent graph with bounded average degree \( np = O(1) \), weak detection is possible if and only if \( s = \Omega(1) \).

As discussed in the next subsection, the testing procedure used to achieve strong detection in both Theorem 1 and Theorem 2 involves a combinatorial optimization that is intractable in the worst case. Thus it is of interest to compare the optimal threshold to the performance of existing computationally efficient algorithms. These methods are based on subgraph counts that extend the simple idea of counting edges in Remark 1. For Erdős-Rényi graphs, the polynomial-time test in [5, Theorem 2.2] (based on counting certain probabilistically constructed subgraphs) correctly distinguishes between \( H_0 \) and \( H_1 \) with probability at least 0.9, provided that the edge subsampling probability \( s = \Omega(1) \) and \( nps \in [n^2, n^{1+\epsilon}] \cup [n^{2/3}, n^{1-\epsilon}] \) for some small constant \( \epsilon > 0 \). This performance guarantee is highly suboptimal compared to \( s^2 = \Omega(\log n / np \log(1/p)) \) given by Theorem 2. In a companion paper [31], we propose a polynomial-time algorithm based on counting trees that achieves strong detection, provided that \( np \geq n^{-o(1)} \) and \( \rho^2 \triangleq s^2(1-p)^2 / (1-ps) > \frac{1}{\beta} \) where \( \beta \triangleq \lim_{k \to \infty} t(k)^{1/k} \approx 2.956 \) and \( t(k) \) is the number of unlabeled trees with \( k \) vertices [37]. Achieving the optimal threshold with polynomial-time tests remains an open problem.

1.2. Test statistic and proof techniques. To introduce our testing procedure and the analysis, we first reformulate the testing problem given in Problem 1 in a more convenient form. Due to the exchangeability of the (i.i.d.) edge weights, observing the unlabeled version is equivalent to observing its randomly relabeled version. Indeed, let \( \pi_1 \) and \( \pi_2 \) be two independent random permutations uniformly drawn from the set \( \mathcal{S}_n \) of all permutations on \([n]\). Consider the relabeled version of \( G_1 = ([n], W) \) with weighted adjacency matrix \( A \), where \( A_{ij} = W_{\pi_i(i)\pi_j(j)} \); similarly, let \( B \) correspond to the relabeled version of \( G_2 = ([n], W') \) with \( B_{ij} = W'_{\pi_i(i)\pi_j(j)} \). It is clear that observing the unlabeled graphs \( \overline{G}_1 \) and \( \overline{G}_2 \) is equivalent to observing the labeled graphs \( A \) and \( B \). Since \( \pi_2^{-1} \circ \pi_1 \) is also a uniform random permutation, we arrive at the following formulation that is equivalent to Problem 1:

PROBLEM 2 (Reformulation of Problem 1). Let \( A \) and \( B \) denote the weighted adjacency matrices of two weighted graphs on the vertex set \([n]\), both consisting of i.i.d. edge weights. Under \( H_0 \), \( A \) and \( B \) are independent; under \( H_1 \), conditional on a latent permutation \( \pi \) drawn uniformly at random from \( \mathcal{S}_n \), \( \{(A_{ij}, B_{\pi(i)\pi(j)}^\pi) : 1 \leq i < j \leq n\} \) are i.i.d. and each pair \( A_{ij} \) and \( B_{\pi(i)\pi(j)}^\pi \) are correlated. Upon observing \( A \) and \( B \), the goal is to test \( H_0 \) versus \( H_1 \).

Note that under \( H_1 \), the latent random permutation \( \pi \) represents the hidden node correspondence under which \( A \) and \( B \) are correlated. For this reason, we refer to \( H_1 \) as the planted model and \( H_0 \) as the null model. The likelihood ratio is given by:

\[
\frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} = \frac{1}{n!} \sum_{\pi \in \mathcal{S}_n} \frac{\mathcal{P}(A, B | \pi)}{\mathcal{Q}(A, B)},
\]
which is the optimal test statistic but difficult to analyze due to the averaging over all \( n! \) permutations. Instead, we consider the \textit{generalized likelihood ratio} by replacing the average with the maximum:

\[
\max_{\pi \in S_n} \frac{P(A, B|\pi)}{Q(A, B)}.
\]

As shown later in Section 2, for both the Gaussian Wigner and the Erdős-Rényi graph model, (9) is equivalent to

\[
T(A, B) \triangleq \max_{\pi \in S_n} T_\pi, \quad \text{where } T_\pi \triangleq \sum_{i < j} A_{ij} B_{\pi(i)\pi(j)},
\]

which amounts to computing the maximal edge correlation over all possible node correspondences between \( A \) and \( B \). As desired, the test statistic \( T(A, B) \) is invariant to the relabeling of both \( A \) and \( B \) and can be applied to their unlabeled versions. The combinatorial optimization problem (10) is an instance of the \textit{quadratic assignment problem} \cite{42}, which is known to be NP-hard to solve or to approximate within a growing factor \cite{30}.

To show the test statistic \( T(A, B) \) achieves detection, first observe that in the planted model with hidden permutation \( \pi \), \( T(A, B) \) is trivially bounded from below by \( \sum_{i < j} A_{ij} B_{\pi(i)\pi(j)} \), which can be further shown to exceed some threshold \( \tau \) with high probability by concentration inequalities. For the null model, we use a simple first moment argument (union bound) to show that \( Q(T(A, B) \geq \tau) = o(1) \). Together we conclude that \( T(A, B) \) with threshold \( \tau \) achieves strong detection and \( \text{TV}(P, Q) = 1 - o(1) \).

Next we provide an overview of the impossibility proof, which constitutes the bulk of the paper. To this end, we bound the second moment of the likelihood ratio. It is well-known that\(^1\)

\[
\mathbb{E}_Q \left[ \frac{(P(A, B))}{Q(A, B)} \right]^2 = O(1) \quad \implies \quad \text{TV}(P(A, B), Q(A, B)) \leq 1 - \Omega(1)
\]

\[
\mathbb{E}_Q \left[ \frac{(P(A, B))}{Q(A, B)} \right]^2 = 1 + o(1) \quad \implies \quad \text{TV}(P(A, B), Q(A, B)) = o(1),
\]

which correspond to the impossibility of strong and weak detection, respectively.

To compute the second moment, we introduce an independent copy \( \bar{\pi} \) of the latent permutation \( \pi \) and express the squared likelihood ratio as

\[
\left( \frac{P(A, B)}{Q(A, B)} \right)^2 = \mathbb{E}_{\bar{\pi} \perp \pi} \left[ \prod_{i < j} X_{ij} \right], \quad \text{where } X_{ij} \triangleq \frac{P(A_{ij}, B_{\pi(i)\pi(j)}) P(A_{ij}, B_{\bar{\pi}(i)\bar{\pi}(j)})}{Q(A_{ij}, B_{\pi(i)\pi(j)}) Q(A_{ij}, B_{\bar{\pi}(i)\bar{\pi}(j)})},
\]

where for any \( (i, j) \in \binom{[n]}{2} \), \( Q \) denotes the joint density function of \( A_{ij} \) and \( B_{ij} \) under \( Q \), and \( P \) denotes the joint density function of \( A_{ij} \) and \( B_{\pi(i)\pi(j)} \) under \( P \) given its latent permutation \( \pi \). Fixing \( \pi \) and \( \bar{\pi} \), we then decompose this as a product over independent randomness indexed by the so-called edge orbits. Specifically, the permutation \( \sigma \triangleq \pi^{-1} \circ \bar{\pi} \) on the node set naturally induces a permutation \( \sigma^\mathcal{O} \) on the edge set of the complete graph by permuting the end points. Denoting by \( \mathcal{O} \) the collection of edge orbits (orbit in the cycle decomposition of the edge permutation \( \sigma^\mathcal{O} \)), we show that

\[
\left( \frac{P(A, B)}{Q(A, B)} \right)^2 = \mathbb{E}_{\bar{\pi} \perp \pi} \left[ \prod_{\mathcal{O} \in \mathcal{O}} X_{\mathcal{O}} \right], \quad X_{\mathcal{O}} \triangleq \prod_{(i, j) \in \mathcal{O}} X_{ij},
\]

\(^1\)Indeed, (11) follows from, e.g., \cite[Lemma 2.6 and 2.7]{45} and (12) is by Cauchy-Schwarz inequality.
Then, we take expectation $E_{(A,B) \sim Q}$ on the right-hand side and interchange the two expectations. For both the Gaussian and Erdős-Rényi models, this calculation can be explicitly carried out by evaluating the trace of certain operators. In particular, this computation shows the following dichotomy: the second moment is $1 + o(1)$ when $\rho^2 \leq \frac{(2 - \epsilon) \log n}{n}$, but unbounded when $\rho^2 \geq \frac{(2 + \epsilon) \log n}{n}$, where $\rho$ is the correlation coefficient in the Gaussian case and $\rho = s(1-p) \frac{1}{1-ps}$ in the Erdős-Rényi case. Compared with Theorems 1 and 2, we see that directly applying the second-moment method fails to capture the sharp threshold: The impossibility condition $\rho^2 \leq \frac{(2 - \epsilon) \log n}{n}$ is suboptimal by a multiplicative factor of 2 in the Gaussian case and by an unbounded factor in the Erdős-Rényi case when $p = o(1)$.

It turns out that the second moment is mostly influenced by those short edge orbits of length $k = O(\log n)$ for which $\prod_{|O| = k} X_O$ has a large expectation (see Section 3.3 for a detailed explanation). Fortunately, the atypically large magnitude of $\prod_{|O| = k} X_O$ can be attributed to certain rare events associated with the intersection graph (edges that are included in both $A$ and $B^{\pi} = (B^{\pi(i)} \pi(j))$), which is distributed as $G(n, ps^2)$ under the planted model $P$. This observation prompts us to apply the conditional second moment method, which truncates the squared likelihood ratio on appropriately chosen global event that has high probability under $P$. Specifically,

- In the dense case (including Gaussian model and dense Erdős-Rényi graphs), the dominating contribution comes from fixed points ($k = 1$) which can be regulated by conditioning on the edge density of large induced subgraphs of the intersection graph. Note that for Erdős-Rényi graphs, even though the density of small induced subgraphs (e.g., induced by $\Theta(\log n)$ vertices) can deviate significantly from their expectations [3], fortunately we only need to consider sufficiently large subgraphs here.
- For sparse Erdős-Rényi graphs, the argument is much more involved and combinatorial, as one need to control the contribution of not only fixed points, but all edge orbits of length $O(\log n)$. Crucially, the major contribution is due to those edge orbits that are subgraphs of the intersection graph. Under the impossibility condition of Theorem 2, the intersection graph $G(n, ps^2)$ is subcritical and a pseudoforest (each component having at most one cycle) with high probability. This global structure significantly limits the co-occurrence of edge orbits in the intersection graph. We thus truncate the squared likelihood ratio on the global event that the intersection graph is a pseudoforest. To compute the conditional second moment, we first study the graph structure of edge orbits, then reduce the problem to enumerating pseudoforests that are disjoint union of edge orbits and bounding their generating functions, and finally average over the cycle lengths of the random permutation $\sigma$. This is the most challenging part of the paper.

1.3. Connection to the literature. This work joins an emerging line of research which examines inference problems on networks from statistical and computational perspectives. We discuss some particularly relevant work below.

Random graph matching. Given a pair of graphs, the problem of graph matching (or network alignment) refers to finding a node correspondence that maximizes the edge correlation [9, 29], which amounts to solving the QAP in (10). Due to the worst-case intractability of the QAP, there is a recent surge of interests in the average-case analysis of matching two correlated random graphs [12, 13, 5, 34, 15, 14, 16, 18, 22, 24], where the goal is to reconstruct the hidden node correspondence between the two graphs accurately with high probability. To this end, the correlated Erdős-Rényi graph model (the alternative hypothesis $H_1$ in Problem 2) has been used as a popular model, for which the solution to the QAP (10) is the maximal
likelihood estimator. It is shown in [13] that exact recovery of the hidden node correspondence with high probability is information-theoretically possible if \( np^2 - \log n \to +\infty \) and \( p = O((\log^{-3}(n))) \), and impossible if \( np^2 - \log n = O(1) \). In contrast, the state of the art of polynomial-time algorithms achieve the exact recovery only when \( np = \text{poly}(\log n) \) and \( 1 - s = 1/\text{poly}(\log n) \) [16, 17, 18].

Recent work [14] initiated the study of almost exact recovery, that is, to obtain a matching (possibly imperfect) of size \( n - o(n) \) that is contained in the true matching with high probability. It shows that the almost exact recovery is information-theoretically possible if \( np^2 = \omega(1) \) and \( p \leq n^{-\Omega(1)} \), and impossible if \( np^2 = O(1) \). Another work [22] considers a weaker objective of partial recovery, that is, to output a matching that contains \( \Theta(1) \) correctly matched vertex pairs with high probability. It is shown that the partial recovery can be attained in polynomial time by a neighborhood tree matching algorithm in the sparse graph regime where \( np^2 \in [1, \lambda_0] \) for some constant \( \lambda_0 \) close to 1 and \( s \in (s_0, 1] \) for some constant \( s_0 \) close to 1. More recently, the partial recovery is shown to be information-theoretically impossible if \( np^2 \log \frac{1}{p} = o(1) \) when \( p = o(1) \) [24]. For ease of comparison, we summarize the different thresholds under various performance metrics in Table 1 in the Erdős-Rényi model.

<table>
<thead>
<tr>
<th>Performance metric</th>
<th>Positive result</th>
<th>Negative result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exact recovery</td>
<td>( np^2 \geq \log n + \omega(1) ) &amp; ( p = O((\log^{-3}(n))) ) [13]</td>
<td>( np^2 \leq \log n - \omega(1) ) [12]</td>
</tr>
<tr>
<td>Almost exact recovery</td>
<td>( np^2 = \omega(1) ) &amp; ( p \leq n^{-\Omega(1)} ) [14]</td>
<td>( np^2 = O(1) ) [14]</td>
</tr>
<tr>
<td>Partial recovery</td>
<td>( np^2 \in [1, \lambda_0] ) &amp; ( s \in (s_0, 1] ) [22]</td>
<td>( np^2 \log \frac{1}{p} = o(1) ) [24]</td>
</tr>
<tr>
<td>Detection (This paper)</td>
<td>( np^2 \log \frac{1}{p} \geq (2 + \epsilon) \log n )</td>
<td>( p = n^{-o(1)} ) &amp; ( np^2 \log \frac{1}{p} \leq (2 - \epsilon) \log n ), or ( p = n^{-\Omega(1)} ) &amp; ( np^2 \in [1, \lambda_0] ) &amp; ( s^2 \leq \frac{1 - \omega(n^{-1/3})}{np} ) ( \wedge 0.01 )</td>
</tr>
</tbody>
</table>

**Table 1**

Thresholds for various recovery criteria in the correlated Erdős-Rényi graph model when \( p = o(1) \).

In contrast to the aforementioned work focusing on recovering the latent matching, this work studies the hypothesis testing aspect of graph matching, which, nevertheless, has direct consequences on the recovery problem. As an application of the truncated second moment calculation, in a companion paper [48] we resolve the sharp threshold of recovery by characterizing the asymptotic mutual information \( I(A, B; \pi) \). In particular, we show that in the dense regime with \( p = n^{-o(1)} \), the sharp threshold of recovery exactly matches the detection threshold above which almost exact recovery is possible and below which partial recovery is impossible, thereby closing the gap in Table 1. In the sparse regime with \( p = n^{-\Omega(1)} \), we show that the information-theoretic threshold for partial recovery is at \( np^2 \asymp 1 \), which coincides with the detection threshold up to a constant factor.

**Detection problems in networks.** There is a recent flurry of work using the first and second-moment methods to study hypothesis testing problems on networks with latent structures such as community detection under stochastic block models [33, 1, 46, 4]. Notably, a conditional second moment argument was applied by Arias-Castro and Verzelen in [1] and [46] to study the problem of detecting the presence of a planted community in dense and sparse Erdős-Rényi graphs, respectively. Similar to our work, for dense graphs, they condition on the edge density of induced subgraphs (see also the earlier work [8] for the Gaussian model);
for sparse graphs, they condition on the planted community being a forest and bound the truncated second-moment by enumerating subforests using Cayley’s formula. However, the crucial difference is that in our setting simply enumerating the pseudoforests is inadequate for proving Theorem 2. Instead, we need to take into account the cycle structure of permutations and enumerate orbit pseudoforests, i.e., pseudoforests assembled from edge orbits (see the discussion before Theorem 4 in Section 5 for details). By separately accounting for orbits of different lengths and their graph properties, we are able to obtain a much finer control on the generating function of orbit pseudoforests that allows the conditional second moment to be bounded after averaging over the random permutation. This proof technique is of particular interest, and likely to be useful for other detection problems regarding permutations.

Finally, we mention that the recent work [40] studied a related correlation detection problem, where the observed two graphs are either independent, or correlated randomly growing graphs (which grow together until time $t_*$ and grow independently afterwards according to either uniform and preferential attachment models). Sufficient conditions are obtained for both weak detection and strong detection as $t_* \to \infty$. However, the problem setup, main results, and proof techniques are very different from the current paper.

1.4. Notation and paper organization. For any $n \in \mathbb{N}$, let $[n] = \{1, 2, \cdots, n\}$ and $S_n$ denote the set of all permutations on $[n]$. For a given graph $G$, let $V(G)$ denote its vertex set and $E(G)$ its edge set. For two graphs on $[n]$ with (weighted) adjacency matrices $A$ and $B$, their intersection graph is a graph on $[n]$ with (weighted) adjacency matrix $A \land B$, where

$$
(A \land B)_{ij} \triangleq A_{ij} B_{\pi(i)\pi(j)};
$$

in the unweighted case, the edge set of $A \land B$ is the intersection of those of $A$ and $B$. Given a permutation $\pi \in S_n$, let $B^\pi = (B_{\pi(i)\pi(j)})$ denote the relabeled version of $B$ according to $\pi$. For any $S \subset [n]$, define $e_A(S) \triangleq \sum_{i<j \in S} A_{ij}$ as the total edge weights in the subgraph induced by $S$.

For any $a, b \in \mathbb{R}$, let $a \land b = \min\{a, b\}$ and $a \lor b = \max\{a, b\}$. Given any $n, m \in \mathbb{N}$, let $\text{lcm}(n, m)$ denote the least common multiple of $n$ and $m$. Given any $n, m \in \mathbb{N}$, and some nonnegative integers $\{k_i\}_{i=1}^m$ such that $\sum_{i=1}^m k_i = n$, let $(k_1, k_2, \cdots, k_m) = \frac{n!}{\prod_{i=1}^m k_i!}$ be a multinomial coefficient. We use standard asymptotic notation: for two positive sequences $\{a_n\}$ and $\{b_n\}$, we write $a_n = O(b_n)$ or $a_n \lesssim b_n$, if $a_n \leq C b_n$ for some an absolute constant $C$ and for all $n$; $a_n = \Omega(b_n)$ or $a_n \gtrsim b_n$, if $b_n = O(a_n)$; $a_n = \Theta(b_n)$ or $a_n \asymp b_n$, if $a_n = O(b_n)$ and $a_n = \Omega(b_n)$; $a_n = o(b_n)$ or $b_n = \omega(a_n)$, if $a_n/b_n \to 0$ as $n \to \infty$.

The rest of the paper is organized as follows. In Section 2 we prove the positive result of strong detection for both Gaussian Wigner model and Erdős-Rényi random graphs. To lay the groundwork for the conditional second moment method, in Section 3 we present the unconditional second moment calculation and discuss the key reasons for its looseness. Section 4 presents the conditional second-moment proof for weak detection in the dense regime. Due to their similarity, the proof for the Gaussian Wigner model is given in Section 4.1 and the (more technical) proof for dense Erdős-Rényi graphs is postponed till Section 7.3. Section 5 provides the impossibility proofs of both strong and weak detection for sparse Erdős-Rényi random graphs. Several other technical proofs are also relegated to supplementary materials in Section 7 and Section 8. Some useful concentration inequalities and facts about random permutations are collected in supplementary materials for readers’ convenience.

2. First Moment Method for Detection. In this section we prove the positive parts of Theorems 1 and 2 by analyzing the test statistic (9). Recall from Section 1.2 the reformulated Problem 2 with observations $A$ and $B$, whose distributions are specified as follows:
• Gaussian Wigner model.

\( \mathcal{H}_0 : (A_{ij}, B_{ij}) \overset{i.i.d.}{\sim} \mathcal{N}\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}\right) \), conditional on \( \pi \sim \text{Uniform}(S_n) \).

(14) \quad \mathcal{H}_1 : \left(A_{ij}, B_{\pi(i)\pi(j)}\right) \overset{i.i.d.}{\sim} \mathcal{N}\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}\right)

• Erdős-Rényi random graph

(16) \quad \mathcal{H}_0 : (A_{ij}, B_{ij}) \overset{i.i.d.}{\sim} \text{Bern}(ps) \otimes \text{Bern}(ps),

\mathcal{H}_1 : \left(A_{ij}, B_{\pi(i)\pi(j)}\right) \overset{i.i.d.}{\sim} \text{pair of correlated Bern}(ps) \text{ conditional on } \pi \sim \text{Uniform}(S_n),

(17) \quad A_{ij} \sim \text{Bern}(ps) \text{ and } B_{\pi(i)\pi(j)} \sim \begin{cases} \text{Bern}(s) & \text{if } A_{ij} = 1 \\ \text{Bern}\left(ps(1-s) \over 1-ps \right) & \text{if } A_{ij} = 0 \end{cases}

Then we get

(18) \quad \frac{P(A, B|\pi)}{Q(A, B)} = \prod_{1 \leq i < j \leq n} L(A_{ij}, B_{\pi(i)\pi(j)}),

where

(19) \quad L(A_{ij}, B_{\pi(i)\pi(j)}) \triangleq \frac{P(A_{ij}, B_{\pi(i)\pi(j)})}{Q(A_{ij}, B_{\pi(i)\pi(j)})}.

For the Gaussian Wigner model, we have

(20) \quad L(a, b) = \frac{1}{\sqrt{1-\rho^2}} \exp\left(\frac{-\rho^2 (b^2 + a^2) + 2 \rho ab}{2 (1-\rho^2)}\right).

For the Erdős-Rényi graph model, we have

(21) \quad L(a, b) = \begin{cases} \frac{1}{p} & a = 1, b = 1 \\ \frac{1-s}{1-ps} & a = 1, b = 0 \text{ or } a = 0, b = 1 \\ \frac{1-2ps+ps^2}{(1-ps)^2} & a = 0, b = 0 \end{cases}

Then, it yields that the generalized likelihood ratio test (9) is equivalent to

(22) \quad \max_{\pi \in S_n} \frac{P(A, B|\pi)}{Q(A, B)} \iff \max_{\pi \in S_n} \sum_{i<j} A_{ij} B_{\pi(i)\pi(j)}

for both Gaussian Wigner model and Erdős-Rényi random graphs. In particular, for the Erdős-Rényi graphs model, this follows from

\[ L(A_{ij}, B_{\pi(i)\pi(j)}) = \left(\begin{array}{c} L(1,1) & L(0,0) \\ L(0,1) & L(1,0) \end{array}\right) A_{ij} B_{\pi(i)\pi(j)} \left(\begin{array}{c} L(1,0) \\ L(0,0) \end{array}\right) A_{ij} B_{\pi(i)\pi(j)} L(0,0), \]

and the fact that \( \frac{L(1,1) L(0,0)}{L(0,1) L(1,0)} \geq 1 \).
2.1. Proof of Theorem 1: positive part. Throughout the proof, denote $m = \binom{n}{2}$ for brevity. Without loss of generality, we assume that (3) holds with equality, i.e., $\rho^2 = \frac{2n \log n}{m}$; otherwise, one can apply the test to $(A', B')$ where $A' = \cos(\theta)A + \sin(\theta)Z, B' = \cos(\theta)B + \sin(\theta)Z$ with an appropriately chosen $\theta$, and $Z$ is standard normal and independent of $(A, B)$. Define

\begin{equation}
\tau = m \rho - a_n
\end{equation}

where $a_n$ is some sequence to be chosen satisfying $a_n = \omega(n)$ and $a_n = O(n^{3/2})$.

We first analyze the error event under the alternative hypothesis (15). Let $\pi$ denote the latent permutation such that $(A_{ij}, B_{\pi(i)\pi(j)})$ are iid pairs of standard normals with correlation coefficient $\rho$. Applying the Hanson-Wright inequality (see Lemma 10 in Appendix 9) with $M = I_m$ to $T_\pi = \sum_{1 \leq i < j \leq n} A_{ij}B_{\pi(i)\pi(j)}$, we get that

\[ P(T_\pi \leq \tau) = P(T_\pi \leq m \rho - a_n) \leq e^{-\alpha n} + e^{-\alpha^2 n^2 / m}, \]

for some universal constant $\alpha$. Since by definition $T \geq T_\pi$, it follows that $P(T \leq \tau) = o(1)$.

To analyze the error event under the null hypothesis (14), in which case for each $\pi \in S_n$, $(A_{ij}, B_{\pi(i)\pi(j)})$ are iid pairs of independent standard normals. Note that for $X, Y \sim \mathcal{N}(0, 1)$ and any $\lambda \in (-1, 1)$, we have

\begin{equation}
\mathbb{E}[\exp(\lambda XY)] = \mathbb{E}\left[\exp\left(\frac{\lambda^2 Y^2}{2}\right)\right] = \frac{1}{\sqrt{1 - \lambda^2}}
\end{equation}

Then by the Chernoff bound, for any $\lambda \in (0, 1)$,

\[ Q(T_\pi \geq \tau) = Q(\exp(\lambda T_\pi) \geq \exp(\lambda \tau)) \leq \exp\left\{-\frac{m}{2} \log(1 - \lambda^2) - \lambda \tau\right\}. \]

Choosing $\lambda = \frac{\tau}{m}$, which satisfies $0 < \lambda = o(1)$ in view of (3) and (23), we have $Q(T_\pi \geq \tau) \leq e^{-\frac{\tau^2}{2m} + O(\tau^4 / m^3)}$. Finally by the union bound and Stirling approximation that $n! \leq e^{n \log n} e^{-n}$, $Q(T \geq \tau) \leq n! e^{-\frac{\tau^2}{2m} + O(\tau^4 / m^3)} = o(1)$, provided that $\frac{\rho^2 m}{2n \log n} - \rho a_n - O(p^4 m) - n \log \frac{n}{\tau} - \frac{\log n}{2} \rightarrow +\infty$. This is ensured by the assumption that $\rho^2 = \frac{2n \log n}{m}$ and the choice of $a_n = n.1.1$.

2.2. Proof of Theorem 2: positive part. Throughout the proof, denote $m = \binom{n}{2}$ for brevity. Without loss of generality, we assume that (5) holds with equality, i.e.,

\begin{equation}
mps^2 \left(\log \frac{1}{p} - 1 + p\right) = n \log n;
\end{equation}

otherwise, one can apply the test to $(A', B')$ where $A' (B')$ are edge-subsampled from $A (B)$ with an appropriately chosen subsampling probability $s'$. It follows from (25) that $p \leq 1/n$ and $mps^2 = \Omega(n)$. Define

\begin{equation}
\tau = mps^2 (1 - \delta_n)
\end{equation}

where $0 < \delta_n < 1$ is some sequence to be chosen satisfying $\delta_n = \omega\left(1/\sqrt{mps^2}\right)$.

We first analyze the error event under the alternative hypothesis (17). Let $\pi$ denote the latent permutation such that $(A_{ij}, B_{\pi(i)\pi(j)}) \sim \text{Bern}(ps^2)$. Then $T_\pi \sim \text{Binom}(m, ps^2)$. By applying the Chernoff bound (118): $P(T_\pi \leq \tau) \leq \exp\left(-\frac{\delta_n^2 mps^2}{2}\right) = o(1)$. Since by definition $T \geq T_\pi$, it follow that $P(T \leq \tau) = o(1)$. 


Next, we analyze the error event under the null hypothesis (16), in which case for each \( \pi \in S_n \), \((A_{ij} B_{\pi(i)\pi(j)})^{i,j} \sim \text{Bern}(p^2 s^2)\) and thus \( T_\pi \sim \text{Binom}(m, p^2 s^2) \). Using the multiplicative Chernoff bound for Binomial distributions (117), we obtain that

\[
Q(T_\pi \geq \tau) \leq \exp \left( -\tau \log \frac{\tau}{e\mu} - \mu \right)
\]

\[
= \exp \left( -mps^2 (1 - \delta_n) \log \frac{1 - \delta_n}{ep} - mp^2 s^2 \right)
\]

\[
\leq \exp \left( -mps^2 \left( \log \frac{1}{p} - 1 + p \right) + mp^2 s \log \frac{1}{p} \right),
\]

where \( \mu = mp^2 s^2 \), and the last inequality holds due to \((1 - \delta_n) \log \frac{1 - \delta_n}{ep} \geq -1\).

Then by applying union bound and Stirling approximation that \( n! \leq e n^{n+\frac{1}{2}} e^{-n} \), we have that

\[
Q(T \geq \tau) \leq e \exp \left( -mps^2 \left( \log \frac{1}{p} - 1 + p \right) + mp^2 s \log \frac{1}{p} + n \log \frac{n}{e} + \frac{1}{2} \log n \right)
\]

\[
= e \exp \left( (mps^2)^{0.6} \log \frac{1}{p} - n + \frac{1}{2} \log n \right) = o(1),
\]

where the first equality holds by the assumption \( mps^2 \left( \log \frac{1}{p} - 1 + p \right) = n \log n \) and choosing \( \delta_n = 1/(mps^2)^{0.4} \); the last equality holds by the claim that \( (mps^2)^{0.6} \log \frac{1}{p} = o(n) \). To finish the proof, it suffices to verify the claim, which is done separately in the following two cases.

Suppose \( 1 - p = \Omega(1) \). Thus, in view of assumption (25), we get that \( mps^2 = O(n \log n / \log(1/p)) \). It follows that \( (mps^2)^{0.6} \log(1/p) \leq O \left( (n \log n)^{0.6} \log^{0.4}(1/p) \right) = o(n) \), where the last equality holds due to \( p \geq 1/n \).

Suppose \( 1 - p = o(1) \). As \( \log(1/p) - 1 + p \geq (1 - p)^2/2 \), it follows from assumption (25) that \( (1 - p)^2 = \Omega(\log n/n) \). Furthermore, \( \log(1/p) \leq \frac{1-p}{p} \). Thus by assumption (25), \( (mps^2)^{0.6} \log \frac{1}{p} \leq O \left( (n \log n)^{0.6} (1 - p)^{-0.2} \right) = O \left( n^{0.7} \log^{0.5} n \right) = o(n) \).

3. Unconditional Second Moment Method and Obstructions. In this section, we apply the unconditional second moment method to derive impossibility conditions for detection. As mentioned in Section 1.2 (and described in details in Section 3.3), these conditions do not match the positive results in Section 2, due to the obstructions presented by the short edge orbits. To overcome these difficulties, in Sections 4 and 5, we apply the conditional second moment method by building upon the second moment computation in this section. We start by introducing some preliminary definitions associated with permutations.

3.1. Node permutation, edge permutation, and cycle decomposition. Let \( \sigma \in S_n \) be a permutation on \([n]\). For each element \( a \in [n] \), its orbit is a cycle \((a_0, \ldots, a_{k-1})\) for some \( k \leq n \), where \( a_i = \sigma^i(a) \), \( i = 0, \ldots, k-1 \) and \( \sigma(a_{k-1}) = a \). Each permutation can be decomposed as disjoint orbits. For example, consider the permutation \( \sigma \in S_5 \) that swaps 1 with 2, swaps 3 with 4, and cyclically shifts 5678. Then \( \sigma \) consists of three orbits represented in canonical notation as \( \sigma = (12)(34)(5678) \).

Consider the complete graph \( K_n \) with vertex set \([n]\). Each permutation \( \sigma \in S_n \) naturally induces a permutation \( \sigma^E \) on the edge set of \( K_n \), the set \( \binom{[n]}{2} \) of all unordered pairs, according to

\[
\sigma^E((i, j)) \triangleq (\sigma(i), \sigma(j)).
\]
We refer to $\sigma$ and $\sigma^E$ as node permutation and edge permutation, whose orbits are referred to as node orbits and edge orbits, respectively. For each edge $(i,j)$, let $O_{ij}$ denotes its orbit under $\sigma^E$. As a concrete example, consider again the permutation $\sigma = (12)(34)(5678)$. Then $O_{12} = \{(1,2)\}$ and $O_{34} = \{(3,4)\}$ are 1-edge orbits (fixed point of $\sigma^E$) and $O_{56} = \{(5,6), (6,7), (7,8), (8,5)\}$ is a 4-edge orbit. (See Table 2 in Section 5.1 for more examples.)

The cycle structure of the edge permutation is determined by that of the node permutation. Let $n_k$ (resp. $N_k$) denote the number of $k$-node (resp. $k$-edge) orbits in $\sigma$ (resp. $\sigma^E$). For example,

$$N_1 = \binom{n_1}{2} + n_2, \quad N_2 = \binom{n_2}{2} \times 2 + n_1 n_2 + n_4.$$  

This is due to the following reasoning.

- Consider a 1-edge orbit given by $\{(i,j)\}$. Since $(i,j)$ is unordered, it follows that either both $i$ and $j$ are fixed points of $\sigma$ or $i,j$ form a 2-node orbit of $\sigma$. Thus, $N_1 = \binom{n_1}{2} + n_2$.
- Consider a 2-edge orbit given by $\{(i,j), (\sigma(i), \sigma(j))\}$. Then there are three cases: (a) $i,j$ belong to two different 2-node orbits; (b) $i$ is a fixed point and $j$ lies in a 2-node orbit; (c) $i,j$ belong to a common 4-node orbit of the form $(i * j * )$. Thus, $N_2 = \binom{n_2}{2} \times 2 + n_1 n_2 + n_4$.

3.2. Second moment calculation. Recall the second-moment method described in Section 1.2. When $P$ is a mixture distribution, the calculation of the second moment can proceed as follows. Note that the likelihood ratio is $P_{(A,B)} / Q_{(A,B)} = \mathbb{E}_\pi [ P_{(A,B|\pi)} / Q_{(A,B|\pi)} ]$, where $\pi$ is a random permutation uniformly distributed over $S_n$. Introducing an independent copy $\bar{\pi}$ of $\pi$ and noting that $B$ has the same marginal distribution under both $P$ and $Q$, the squared likelihood ratio can be expressed as

$$\left( \frac{P_{(A,B)}}{Q_{(A,B)}} \right)^2 = \mathbb{E}_{\bar{\pi}, \pi} \left[ \frac{P_{(A,B|\pi)} P_{(A,B|\bar{\pi})}}{Q_{(A,B)} Q_{(A,B)}} \right] = \mathbb{E}_{\bar{\pi}, \pi} \left[ \prod_{i<j} X_{ij} \right],$$

where $\pi \perp \bar{\pi}$ denotes that $\pi$ and $\bar{\pi}$ are independent, and

$$X_{ij} \triangleq L \left( A_{ij}, B_{\pi(i)\pi(j)} \right) L \left( A_{ij}, B_{\bar{\pi}(i)\bar{\pi}(j)} \right).$$

Interchanging the expectations yields

$$\mathbb{E}_Q \left[ \left( \frac{P_{(A,B)}}{Q_{(A,B)}} \right)^2 \right] = \mathbb{E}_{\bar{\pi}, \pi} \mathbb{E}_{(A,B) \sim Q} \left[ \prod_{i<j} X_{ij} \right].$$

Fixing $\pi$ and $\bar{\pi}$, we first compute the inner expectation in (31). Observe that $X_{ij}$ may not be independent across different pairs of $(i,j)$. For example, suppose $(i_1,j_1) \neq (i_2,j_2)$ and $(\pi(i_1), \pi(j_1)) = (\bar{\pi}(i_2), \bar{\pi}(j_2))$, then $B_{\pi(i_1)\pi(j_1)} = B_{\bar{\pi}(i_2)\bar{\pi}(j_2)}$ and $X_{i_1j_1}$ is not independent of $X_{i_2j_2}$. In order to decompose $\prod_{i<j} X_{ij}$ as a product over independent randomness, we use the notion of cycle decomposition introduced in Section 3.1. Define

$$\sigma \triangleq \pi^{-1} \circ \bar{\pi},$$

which is also uniformly distributed on $S_n$. Let $\sigma^E$ denote the edge permutation induced by $\sigma$ as in (27), i.e., $\sigma^E(i,j) = (\sigma(i), \sigma(j))$. For each edge orbit $O$ of $\sigma^E$, define

$$X_{O} \triangleq \prod_{(i,j) \in O} X_{ij} = \prod_{(i,j) \in O} L \left( A_{ij}, B_{\pi(i)\pi(j)} \right) L \left( A_{ij}, B_{\bar{\pi}(i)\bar{\pi}(j)} \right).$$
Importantly, observe that $X_O$ is a function of $(A_{ij}, B_{\pi(i)\pi(j)})_{(i,j) \in O}$. Indeed, since $(\pi(i), \pi(j)) = (\sigma(i), \sigma(j))$, or equivalently in terms of edge permutation, $\pi^E = \pi^E \circ \sigma^E$, and $O$ is an orbit of $\sigma^E$, we have $\{B_{\pi(i)\pi(j)})_{(i,j) \in O} = \{B_{\pi(i)\pi(j)})_{(i,j) \in O}$.

Let $O$ denote the collection of all edge orbits of $\sigma$. Since edge orbits are disjoint, we have

$$
\prod_{i<j} X_{ij} = \prod_{O \in O} X_O.
$$

Since $\{A_{ij}\}_{i<j}$ and $\{B_{ij}\}_{i<j}$ are i.i.d. under $Q$, we conclude $\{X_O\}_{0 \in O}$ are mutually independent under $Q$. Therefore, by (31),

$$
\mathbb{E}_Q \left[ \left( \mathcal{P}(A, B) \right)^2 \right] = \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \prod_{O \in O} \mathbb{E}_{(A, B) \sim Q} [X_O] \right].
$$

Recall that, for the Gaussian Wigner model, $\rho$ denotes the correlation coefficient of edge weights in the planted model $\mathcal{P}$. For Erdős-Rényi graph model, the correlation parameter in the planted model $\mathcal{P}$ is defined as:

$$
\rho \triangleq \frac{\text{Cov}(A_{ij}, B_{\pi(i)\pi(j)})}{\sqrt{\text{Var}(A_{ij})} \sqrt{\text{Var}(B_{\pi(i)\pi(j)})}} = \frac{s(1-p)}{1-ps}.
$$

**PROPOSITION 1.** Fixing $\pi$ and $\bar{\pi}$, for any edge orbit $O$ of $\sigma = \pi^{-1} \circ \bar{\pi}$, we have

- for Gaussian Wigner models,
  
  $$
  \mathbb{E}_{(A, B) \sim Q} [X_O] = \frac{1}{1 - \rho^{2|O|}},
  $$

- for Erdős-Rényi random graphs,
  
  $$
  \mathbb{E}_{(A, B) \sim Q} [X_O] = 1 + \rho^{2|O|}.
  $$

**PROOF.** Recall from (19) that $L(x, y) = \frac{P(x, y)}{Q(x, y)} = \frac{P(x, y)}{Q(x)Q(y)}$. This kernel defines an operator as follows: for any square-integrable function $f$ under $Q$,

$$
(Lf)(x) \triangleq \mathbb{E}_{Y \sim Q} [L(x, Y) f(Y)] = \mathbb{E}_{(X, Y) \sim P} [f(Y) \mid X = x].
$$

In addition, $L^2 = L \circ L$ is given by $L^2(x, y) = \mathbb{E}_{Z \sim Q} [L(x, Z) L(Z, y)]$ and $L^k$ is similarly defined. For both Gaussian and Bernoulli model, we have $L(x, y) = L(y, x)$ and hence $L$ is self-adjoint. Furthermore, since $\int \int L(x, y)^2 Q(dx)Q(dy) < \infty$, $L$ is Hilbert-Schmidt. Thus $L$ is diagonalizable with eigenvalues $\lambda_i$’s and the trace of $L$ is given by $\text{tr}(L) = \mathbb{E}_{Y \sim Q} [L(Y, Y)] = \sum \lambda_i$.

Let $k = |O|$. To simplify the notation, let $a_i$’s and $b_i$’s be independent sequences of i.i.d. random variables drawn from $Q$. Since $O$ is an edge orbit of $\sigma^E$, we have $\{B_{\pi(i)\pi(j)})_{(i,j) \in O} = \{B_{\pi(i)\pi(j)})_{(i,j) \in O}$ and $(\pi(i), \pi(j)) = (\sigma(i), \sigma(j))$. By (33),

$$
\mathbb{E}_{A, B \sim Q} [X_O] = \mathbb{E}_{A, B \sim Q} \left[ \prod_{(i,j) \in O} L(A_{ij}, B_{\pi(i)\pi(j)}) \right] 
= \mathbb{E} \left[ \prod_{\ell=1}^k L(a_\ell, b_\ell) L(a_\ell, b_{(\ell+1) \mod k}) \right]
$$
\[ = \mathbb{E} \left[ \prod_{\ell=1}^{k} L^2 \left( b_{\ell}, b_{(\ell+1) \mod k} \right) \right] \]
\[ = \text{tr} \left( L^{2k} \right) = \sum \lambda_i^{2k}. \]

For Gaussian Wigner model, \( L(x, y) \) given in (20) is known as Mehler’s kernel and can be diagonalized by Hermite polynomials as
\[ L(x, y) = \sum_{i=0}^{\infty} \frac{\rho^i}{i!} H_i(x) H_i(y), \]
where \( \mathbb{E}_{Y \sim N(0, 1)} [H_i(Y) H_j(Y)] = i! \mathbf{1}_{(i=j)} \) [28]. It follows that the eigenvalues of operator \( L \) are given by \( \lambda_i = \rho^i \) for \( i \geq 0 \) and thus \( \text{tr} \left( L^{2k} \right) = \sum_{i=0}^{\infty} \rho^{2ki} = \frac{1}{1-\rho^{2k}}. \)

For Erdős-Rényi graphs, by (35) and (38), we get
\[ (L f)(x) = \sum_{y \in \{0,1\}} \frac{P(x, y)}{Q(x)Q(y)} f(y)Q(y) = \frac{1}{Q(x)} \sum_{y \in \{0,1\}} P(x, y) f(y). \]

Thus the eigenvalues of \( L \) are given by the eigenvalues of the following \( 2 \times 2 \) row-stochastic matrix \( M \) with rows and columns indexed by \( \{0,1\} \) and \( M(x, y) = \frac{P(x, y)}{Q(x)} \). Explicitly, by (21) we have
\[ M = \begin{pmatrix} \frac{1-ps(2-s)}{1-ps} & \frac{ps(1-s)}{1-ps} \\ \frac{1}{1-s} & \frac{s}{1-s} \end{pmatrix}. \]
The eigenvalues of \( M \) are 1 and \( \rho = \frac{s(1-p)}{1-ps} \), so \( \text{tr} \left( L^{2k} \right) = 1 + \rho^{2k}. \)

In view of Propositions 1, \( \mathbb{E}_{(A,B) \sim Q} [X_O] \) decreases when the orbit length \( |O| \) increases. Let \( n_k \) denote the total number of \( k \)-node orbits in the cycle decomposition of node permutation \( \sigma \), and let \( N_k \) denote the total number of \( k \)-edge orbits in the cycle decomposition of edge permutation \( \sigma^E \), for \( k \in \mathbb{N} \). For the Gaussian Wigner model, by (35) and (37), we get
\[ \mathbb{E}_{Q} \left[ \left( \frac{P(A,B)}{Q(A,B)} \right)^2 \right] = \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \prod_{O \in \mathcal{O}} \left( \frac{1}{1-\rho^{2|O|}} \right) \right] = \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \prod_{k=1}^{\binom{n}{2}} \left( \frac{1}{1-\rho^{2k}} \right)^{N_k} \right]. \]
For the Erdős-Rényi graphs, by (35) and (38), we get
\[ \mathbb{E}_{Q} \left[ \left( \frac{P(A,B)}{Q(A,B)} \right)^2 \right] = \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \prod_{O \in \mathcal{O}} \left( 1 + \rho^{2|O|} \right) \right] = \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \prod_{k=1}^{\binom{n}{2}} \left( 1 + \rho^{2k} \right)^{N_k} \right]. \]

Let us assume
\[ n^2 \rho^6 = o(1), \]
which is ensured by (4) for Gaussian model in Theorem 1 or (6) for dense Erdős-Rényi model with \( p = n^{-o(1)} \) in Theorem 2.

For the Gaussian model, consider the orbits of length \( k \geq 3 \). Since \( \sum_{k=3}^{\binom{n}{2}} N_k \leq \binom{n}{2} \), we have
\[ \prod_{k=3}^{\binom{n}{2}} \left( \frac{1}{1-\rho^{2k}} \right)^{N_k} \leq \left( \frac{1}{1-\rho^6} \right)^{\binom{n}{2}} = \left( 1 + \frac{\rho^6}{1-\rho^6} \right)^{\binom{n}{2}} \leq \exp \left( \frac{n^2 \rho^6}{2(1-\rho^6)} \right) = 1 + o(1), \]
where the last equality holds due to (42). Moreover, for 1-orbits and 2-orbits,

\[
\left( \frac{1}{1 - \rho^2} \right)^{N_1} \left( \frac{1}{1 - \rho^4} \right)^{N_2} \leq \left( 1 + \frac{\rho^2}{1 - \rho^2} \right)^{N_1} \left( 1 + \left( \frac{\rho^2}{1 - \rho^2} \right)^2 \right)^{N_2} \leq \exp \left( \frac{\rho^2}{1 - \rho^2} N_1 + \left( \frac{\rho^2}{1 - \rho^2} \right)^2 N_2 \right).
\]

Therefore,

\[
\mathbb{E}_Q \left[ \left( \frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] \leq (1 + o(1)) \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \exp \left( \frac{\rho^2}{1 - \rho^2} N_1 + \left( \frac{\rho^2}{1 - \rho^2} \right)^2 N_2 \right) \right].
\]

For Erdős-Rényi graphs, analogously, for the orbits of length \( k \geq 3 \),

\[
\prod_{k=3}^{(\gamma)} \left( 1 + \rho^{2k} \right)^{N_k} \leq \left( 1 + \rho^6 \right)^{(\gamma)} \leq \exp \left( \frac{n^2 \rho^6}{2} \right) = 1 + o(1),
\]

where the last equality holds due to (42). For 1-orbits and 2-orbits, \( (1 + \rho^2)^{N_1} (1 + \rho^4)^{N_2} \leq \exp \left( \rho^2 N_1 + \rho^4 N_2 \right) \). Therefore,

\[
\mathbb{E}_Q \left[ \left( \frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] \leq (1 + o(1)) \mathbb{E}_{\pi \perp \bar{\pi}} \left[ \exp \left( \rho^2 N_1 + \rho^4 N_2 \right) \right].
\]

Next, we bound the contribution of \( N_1 \) and \( N_2 \) to the second moment for both models using the following proposition. The proof, based on Poisson approximation, is deferred till Section 7.2.

**PROPOSITION 2.** Assume \( \mu, \nu, \tau \geq 0 \) such that \( \tau^2 = o \left( \frac{1}{n} \right) \), and \( \mu b + \nu + 2 - \log b \leq 0 \) for some \( 1 \leq b \leq n \) such that \( b = \Omega(1) \).

1. If \( \alpha = \Omega(1) \) and \( \nu \leq \log(\alpha) - 3 \),

\[
\mathbb{E}_{\pi \perp \bar{\pi}} \left[ \exp \left( \mu n_1^2 + \nu n_1 + \tau n_2 + \tau^2 N_2 \right) \right] = o(1).
\]

2. If \( \alpha = 0 \) and \( \nu = o(1) \),

\[
\mathbb{E}_{\pi \perp \bar{\pi}} \left[ \exp \left( \mu n_1^2 + \nu n_1 + \tau n_2 + \tau^2 N_2 \right) \right] \leq 1 + o(1).
\]

In particular, if \( 0 \leq \tau \leq \frac{2(\log n - 2)}{n} \), then

\[
\mathbb{E}_{\pi \perp \bar{\pi}} \left[ \exp \left( \tau N_1 + \tau^2 N_2 \right) \right] = 1 + o(1).
\]

Finally, we arrive at a sufficient condition for bounded second moment, which turns out to be essentially necessary as we will see shortly in Section 3.3.

**THEOREM 3** (Impossibility condition by unconditional second moment method). Fix any constant \( \epsilon > 0 \). If

\[
\rho^2 \leq \frac{(2 - \epsilon) \log n}{n},
\]

then for both Gaussian Wigner and Erdős-Rényi graphs, \( \mathbb{E}_Q \left[ \left( \frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] = 1 + o(1) \), which further implies that \( TV(\mathcal{P}, \mathcal{Q}) = o(1) \), the impossibility of weak detection.

**PROOF.** Note that (50) implies (42). Thus, by combining (44) or (46) with (49) in Proposition 2, we get \( \mathbb{E}_Q \left[ \left( \frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] = 1 + o(1) \), which yields \( TV(\mathcal{P}, \mathcal{Q}) = o(1) \) in view of (12). \( \square \)
3.3. **Obstruction from short orbits.** The impossibility condition in Theorem 3 is not optimal. In the Gaussian case, (50) differs by a factor of 2 from the positive result of \( \rho^2 \geq \frac{(4+\epsilon)\log n}{n} \) in Theorem 1. For Erdős-Rényi graphs the suboptimality is more severe: Theorem 2 shows that if \( nps^2 \left( \log \frac{1}{p} - 1 + p \right) \geq (2 + \epsilon) \log n \), then strong detection is possible. In the regime of \( p = o(1) \), since \( \rho = (1 + o(1))s \), this translates to the condition \( \rho^2 \geq \frac{(2+\epsilon)\log n}{np\log p} \), which differs from (50) by an unbounded factor. This is the limitation of the second moment method, as the condition \( \rho^2 \leq \frac{(2-\epsilon)\log n}{n} \) is actually tight for the second moment to be bounded. When \( \rho^2 \geq \frac{(2+\epsilon)\log n}{np\log p} \), the second moment diverges because of certain rare events associated with short orbits in \( \sigma = \pi^{-1} \circ \bar{\pi} \). Below we describe the lower bound on the second moment due to short orbits, which motivates the conditional second moment arguments in Sections 4 and 5 that eventually overcome these obstructions.

Specifically, in view of (29) and (34), for both Gaussian and Erdős-Rényi models, the squared likelihood ratio factorizes into products over the edge orbits of \( \sigma \):

\[
\left( \frac{P(A,B)}{Q(A,B)} \right)^2 = \mathbb{E}_{\pi,\bar{\pi}} \left[ \prod_{O \in \mathcal{O}} X_O \right],
\]

where \( X_O \) is defined in (33). Since both \( \pi \) and \( \bar{\pi} \) are uniform random permutations, so is \( \sigma = \pi^{-1} \circ \bar{\pi} \). For each divisor \( k \) of \( n \), consider the rare event that \( \sigma \) decomposes into \( (n/k) \)-node orbits (i.e. \( n_k = n/k \) and all the other \( n_j \)'s are zero), which occurs with probability \( \frac{1}{(n/k)!^2} \geq n^{-n/k} \). These short node orbits create an abundance of short edge orbits, as each pair of distinct \( k \)-node orbits can form \( k \) different \( k \)-edge orbits.\(^2\) Thus, the following lower bound on the second moment ensues

\[
\mathbb{E}_{(A,B) \sim \mathcal{Q}} \left[ \left( \frac{P(A,B)}{Q(A,B)} \right)^2 \right] = \mathbb{E}_{\pi,\bar{\pi}} \left[ \prod_{O \in \mathcal{O}} \mathbb{E}_\mathcal{Q} [X_O] \right] \\
\geq \mathbb{E} \left[ \left( 1 + \rho^{2k} \right)^{\binom{n}{k}^2} \right] \geq n^{-n/k} \left( 1 + \rho^{2k} \right)^{\binom{n}{k}^2} \\
= \exp \left( \frac{n}{k} \log n + \binom{n/k}{2} k \log \left( 1 + \rho^{2k} \right) \right),
\]

(51)

where \(^{(a)}\) holds because \( \mathbb{E}_\mathcal{Q} [X_O] = 1 + \rho^{2k} \) for each \( k \)-edge orbit \( O \) in both Gaussian ((37)) and Erdős-Rényi models ((38)).

Consequently, for any \( k = o(n) \),

\[
\rho^{2k} \geq \frac{(2 + \epsilon) \log n}{n} \implies \mathbb{E}_\mathcal{Q} \left[ \left( \frac{P(A,B)}{Q(A,B)} \right)^2 \right] \to \infty.
\]

In particular, the strongest obstruction comes from \( k = 1 \) (fixed points):

\[
\rho^2 \geq \frac{(2 + \epsilon) \log n}{n} \implies \mathbb{E}_\mathcal{Q} \left[ \left( \frac{P(A,B)}{Q(A,B)} \right)^2 \right] \to \infty.
\]

In this case, the culprit is the rare event of \( \pi \) “colliding” with \( \bar{\pi} \) (\( \sigma = \text{id} \)), which holds with probability \( 1/n! \) but has an excessive contribution of \( (1 + \rho^2)^{\binom{n}{2}} \) to the second moment.

\(^2\)For example, (12) and (34) can form two edge orbits \( O_{13} \) and \( O_{14} \) of length 2; these edge orbits will be referred to as Type-M; see Section 5.1 for a full classification of edge orbits.
In conclusion, the second moment is susceptible to the influence of short edge orbits, for which \( \prod_{|O|=k} X_{O} \) for small \( k \) has a large expectation. Fortunately, it turns out that the atypically large magnitude of \( \prod_{|O|=k} X_{O} \) can be attributed to certain rare events associated with the intersection graph \( A \land B^{\pi} \) under the planted model \( \mathcal{P} \). This motivates us to condition on some appropriate high-probability event under \( \mathcal{P} \), so that the excessively large magnitude of \( \prod_{|O|=k} X_{O} \) is truncated. As we will see in Section 4, in the dense regime (including Gaussian Wigner model and dense Erdős-Rényi graphs), it suffices to consider \( k = 1 \) and regulate \( \prod_{|O|=1} X_{O} \) by conditioning on the edge density for all sufficiently large induced subgraphs of \( A \land B^{\pi} \) under \( \mathcal{P} \). In contrast, in the sparse regime, we need to consider all edge orbits up to length \( k = \Theta(\log n) \) for which more sophisticated techniques are called for, as we will see in Section 5.

4. Conditional Second Moment Method: Dense regime. In this section, we improve Theorem 3 by applying the conditional second moment method. The proof of the sharp threshold for the Gaussian model is given in full details in Section 4.1. The proof for dense Erdős-Rényi graphs uses similar ideas but is technically more involved and hence deferred to Section 7.3. We start by describing the general program of conditional second moment method. Note that sometimes certain rare events under \( \mathcal{P} \) can cause the second moment to explode, while \( \text{TV}(\mathcal{P}, \mathcal{Q}) \) remains bounded away from one. To circumvent such catastrophic events, we can compute the second moment conditioned on events that are typical under \( \mathcal{P} \). More precisely, given an event \( \mathcal{E} \) such that \( \mathcal{P}(\mathcal{E}) = 1 + o(1) \), define the planted model conditioned on \( \mathcal{E} \):

\[
\mathcal{P}'(A, B, \pi) \triangleq \frac{\mathcal{P}(A, B, \pi) 1_{\{A, B, \pi \} \in \mathcal{E}}}{\mathcal{P}(\mathcal{E})} = (1 + o(1)) \mathcal{P}(A, B, \pi) 1_{\{A, B, \pi \} \in \mathcal{E}},
\]

the last equality holds because \( \mathcal{P}(\mathcal{E}) = 1 + o(1) \). Then the likelihood ratio between the conditioned planted model \( \mathcal{P}' \) and the null model \( \mathcal{Q} \) is given by

\[
\frac{\mathcal{P}'(A, B)}{\mathcal{Q}(A, B)} = \int \frac{\mathcal{P}'(A, B, \pi) d\pi}{\mathcal{Q}(A, B)} = (1 + o(1)) \int \frac{\mathcal{P}(\pi) \mathcal{P}(A, B | \pi) 1_{\{A, B, \pi \} \in \mathcal{E}}}{\mathcal{Q}(A, B)} d\pi = (1 + o(1)) \mathbb{E}_{\pi} \left[ \frac{\mathcal{P}(A, B | \pi)}{\mathcal{Q}(A, B)} 1_{\{A, B, \pi \} \in \mathcal{E}} \right].
\]

By the same reasoning that led to (35), the conditional second moment is given by

\[
\mathbb{E}_{\mathcal{Q}} \left[ \left( \frac{\mathcal{P}'(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] = (1 + o(1)) \mathbb{E}_{\pi \perp \tilde{\pi}} \left[ \mathbb{E}_{\mathcal{Q}} \left[ \frac{\mathcal{P}(A, B | \pi)}{\mathcal{Q}(A, \tilde{B})} \mathcal{P}(A, B | \tilde{\pi}) 1_{\{A, B, \pi \} \in \mathcal{E}} 1_{\{A, B, \tilde{\pi} \} \in \mathcal{E}} \right] \right]
\]

\[
= (1 + o(1)) \mathbb{E}_{\pi \perp \tilde{\pi}} \left[ \mathbb{E}_{\mathcal{Q}} \left[ \prod_{O \in \mathcal{O}} X_{O} 1_{\{A, B, \pi \} \in \mathcal{E}} 1_{\{A, B, \tilde{\pi} \} \in \mathcal{E}} \right] \right],
\]

where the last equality follows from the decomposition (34) over edge orbits \( O \in \mathcal{O} \) of \( \sigma = \pi^{-1} \circ \tilde{\pi} \). Compared to the unconditional second moment in (29), the extra indicators in (52) will be useful for ruling out those rare events causing the second moment to blow up.

We caution the reader that, crucially, the conditioning event \( \mathcal{E} \) must be measurable with respect to the observed and the latent variables \( (A, B, \pi) \). Thus we cannot rule out the rare event that \( \pi \) is close to its independent copy \( \tilde{\pi} \) so that \( \sigma = \pi^{-1} \circ \tilde{\pi} \) induces a proliferation of short edge orbits. Instead, as we will see, by truncating certain rare events associated with the intersection graph \( A \land B^{\pi} \), the excessively large magnitude of \( \prod_{|O|=k} X_{O} \) can be regulated for small \( k \).
By the data processing inequality of total variation, we have
\[ TV(\mathcal{P}(A, B), \mathcal{P}'(A, B)) \leq TV(\mathcal{P}(A, B, \pi), \mathcal{P}'(A, B, \pi)) = \mathcal{P}((A, B, \pi) \not\in \mathcal{E}) = o(1). \]

Combining this with the second moment bound (11)–(12) and applying the triangle inequality, we arrive at the following conditions for non-detection:
\[ \mathbb{E}_Q \left[ \left( \frac{\mathcal{P}'(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] = O(1) \implies TV(\mathcal{P}(A, B), \mathcal{Q}(A, B)) \leq 1 - \Omega(1) \]
\[ \mathbb{E}_Q \left[ \left( \frac{\mathcal{P}'(A, B)}{\mathcal{Q}(A, B)} \right)^2 \right] = 1 + o(1) \implies TV(\mathcal{P}(A, B), \mathcal{Q}(A, B)) = o(1). \]

4.1. Sharp threshold for the Gaussian model. In this section, we improve over the impossibility condition \( \rho^2 \leq \left(\frac{2-\epsilon}{\epsilon}\right)\log \frac{n}{\epsilon} \) established in Theorem 3, showing that if \( \rho^2 \leq \left(\frac{4-\epsilon}{\epsilon}\right)\log \frac{n}{\epsilon} \), then weak detection is impossible. This completes the impossibility proof of Theorem 2 for the Gaussian model.

Before the rigorous analysis, we first explain the main intuition. Let \( F \) denotes the set of fixed points of \( \sigma = \pi^{-1} \circ \tilde{\pi} \), so that \( |F| = n_1 \). Let
\[ O_1 = \left( \begin{array}{c} F \\ 2 \end{array} \right), \]
which is a subset of fixed points of the edge permutation (cf. (28)). As argued in Section 3.3, the unconditional second moment blows up when \( \rho^2 \geq \left(\frac{2+\epsilon}{\epsilon}\right)\log \frac{n}{\epsilon} \) due to the obstruction of fixed points of \( \sigma \), or more precisely, an atypically large magnitude of \( \prod_{O \in O_1} X_O \). By (20) and (30),
\[ \prod_{O \in O_1} X_O = \prod_{i<j \in F} X_{ij} \]
\[ = (1 - \rho^2)^{-\binom{n}{2}} \exp \left\{ \frac{1}{1 - \rho^2} \left( -\rho^2 \sum_{i<j \in F} \left( A_{ij}^2 + B_{\pi(i)\pi(j)}^2 \right) + 2\rho \sum_{i<j \in F} A_{ij}B_{\pi(i)\pi(j)} \right) \right\}. \]

Recall that for any \( S \subset [n] \), \( e_{A \wedge B^*}(S) = \sum_{i<j \in F} A_{ij}B_{\pi(i)\pi(j)} \) as defined in (13). To truncate \( \prod_{i<j \in F} X_{ij} \), one natural idea is to condition on the typical value of \( e_{A \wedge B^*}(F) \) under the planted model \( \mathcal{P} \) when \( |F| = n_1 \) is large. More specifically, for each \( S \subset [n] \), define
\[ \mathcal{E}_S \triangleq \left\{ (A, B, \pi) : \sum_{i<j \in S} A_{ij}^2 \geq \frac{|S|^2}{2} - Cn^{3/2}, \sum_{i<j \in S} B_{\pi(i)\pi(j)}^2 \geq \frac{|S|^2}{2} - Cn^{3/2} \right\}, \]
\[ e_{A \wedge B^*}(S) \leq \rho \left( \frac{|S|}{2} \right) + Cn^{3/2}, \]
where \( C \) is an absolute constant. We will condition on the event
\[ \mathcal{E} \triangleq \bigcap_{S \subset [n]: |S| \geq n/2} \mathcal{E}_S, \]
which will be shown to hold with high probability under the planted model \( \mathcal{P} \). Note that here in order to truncate \( \prod_{i<j \in F} X_{ij} \), \( \mathcal{E} \) is defined as the intersection of \( \mathcal{E}_S \) over all subsets \( S \) with \( |S| \geq n/2 \), so that it implies \( \mathcal{E}_F \) when \( |F| \geq n/2 \). The reason that we cannot condition on \( \mathcal{E}_F \)
directly is because the set of fixed points \( F \) depends on \( \sigma = \pi^{-1} \circ \pi \) rather than \( \pi \) alone, and thus is not measurable with respect to \((A, B, \pi)\).

Let

\[
\zeta = \rho \left( \frac{n_1}{2} \right) + Cn^{3/2}
\]

(57)

When \( n_1 \geq n/2 \), we have \( \zeta = \rho \left( \frac{n_1}{2} \right) (1 + o(1)) \). Furthermore, on the event \( \mathcal{E} \), it follows from (55) and \( \rho = o(1) \) that

\[
\mathbb{E}_Q \left[ \prod_{i<j \in F} X_{ij} \mathbf{1}_{\mathcal{E}} \right] \leq \exp \left\{ -(1 + o(1))\rho^2 \left( \frac{n_1}{2} \right) \right\} \mathbb{E}_Q \left[ \exp \left\{ \frac{2\rho}{1 - \rho^2} e_{A \wedge B^\pi} (F) \right\} \mathbf{1}_{\{e_{A \wedge B^\pi} (F) \leq \zeta \}} \right]\]

\[
\leq \exp \left\{ \frac{1 + o(1)}{2} \rho^2 \left( \frac{n_1}{2} \right) \right\},
\]

where the last inequality is by evaluating the truncated MGF of \( e_{A \wedge B^\pi} (F) \) (see (59) below). Note that without the truncation \( e_{A \wedge B^\pi} (F) \leq \zeta \), we recover the unconditional bound

\[
\mathbb{E}_Q \left[ \prod_{i<j \in F} X_{ij} \right] = \exp \left\{ (1 + o(1))\rho^2 \left( \frac{n_1}{2} \right) \right\}.
\]

Thus, the conditional bound improves over the unconditional one by a multiplicative factor of 2 in the exponent.

Finally, to ensure the second moment after conditioning is \( 1 + o(1) \), analogous to (51), in the extreme case of \( n_1 = n \), we need to ensure

\[
\frac{1}{n!} \exp \left\{ \frac{1 + o(1)}{2} \rho^2 \left( \frac{n}{2} \right) \right\} = \exp \left\{ -(1 + o(1))n \log n + \frac{1 + o(1)}{4} \rho^2 n^2 \right\} = o(1),
\]

which corresponds precisely to the desired condition \( \rho^2 \leq \frac{(4 - \epsilon) \log n}{n} \).

Next, we proceed to the rigorous proof. As the impossibility of weak detection when \( \rho^2 \leq \frac{\log n}{n} \) has already been shown in Theorem 3, henceforth we only need to focus on

\[
\frac{\log n}{n} \leq \rho^2 \leq \frac{(4 - \epsilon) \log n}{n}.
\]

The following lemma proves that \( \mathcal{E} \) holds with high probability under the planted model \( \mathcal{P} \).

**Lemma 1.** It holds that \( \mathcal{P}((A, B, \pi) \in \mathcal{E}) \geq 1 - e^{-\Omega(n)} \).

**Proof.** Fix an integer \( n/2 \leq k \leq n \) and let \( m = \binom{k}{2} \). Let \( t = c \left( \sqrt{m \log(1/\delta)} + \log(1/\delta) \right) \), for a universal constant \( c \) and a parameter \( \delta \) to be specified later.

Fix a subset \( S \subset [n] \) with \( |S| = k \). Using the Hanson-Wright inequality given in Lemma 10, with probability at least \( 1 - 3\delta \),

\[
\sum_{i<j \in S} A_{ij}^2 \geq m - t, \quad \sum_{i<j \in S} B_{\pi(i) \pi(j)}^2 \geq m - t, \quad e_{A \wedge B^\pi} (S) = \sum_{i<j \in S} A_{ij} B_{\pi(i) \pi(j)} \leq \rho m + t.
\]

(58)

Now, there are \( \binom{n}{k} \) different choices of \( S \subset [n] \) with \( |S| = k \). Thus by choosing \( 1/\delta = 2^k (\binom{n}{k}) \) and applying the union bound, we get that with probability at least \( 1 - 3 \sum_{k=n/2}^{n} 2^{-k} = 1 - e^{-\Omega(n)} \), (58) holds uniformly for all \( S \subset [n] \) with \( |S| = k \) and all \( n/2 \leq k \leq n \). By definition and the fact that \( k \geq n/2, 1/\delta \leq 2^k \left( \frac{c}{2} \right)^k \leq (4e)^k \), and thus

\[
t \leq c \left( \sqrt{mk \log(4e)} + k \log(4e) \right) = O \left( n^{3/2} \right).
\]

\[ \Box \]
Now, let us compute the conditional second moment. By Lemma 1, it follows from (52) that
\[
\mathbb{E}_Q \left[ \left( \frac{\mathbb{P}'(A, B)}{Q(A, B)} \right)^2 \right] = (1 + o(1)) \mathbb{E}_{\pi \perp \tilde{\pi}} \left[ \prod_{O \in \mathcal{O}} X_O \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}\}} \mathbf{1}_{\{(A, B, \tilde{\pi}) \in \mathcal{E}\}} \right].
\]

To proceed further, we fix \(\pi, \tilde{\pi}\) and separately consider the following two cases.

**Case 1**: \(n_1 \leq n/2\). In this case, we simply drop the indicators and use the unconditional second moment:
\[
\mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}\}} \mathbf{1}_{\{(A, B, \tilde{\pi}) \in \mathcal{E}\}} \right] \leq \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O \right] = \prod_{O \in \mathcal{O}} \frac{1}{1 - \rho^{2|O|}},
\]
where the last equality follows from (37).

**Case 2**: \(n_1 > n/2\). In this case,
\[
\mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}\}} \mathbf{1}_{\{(A, B, \tilde{\pi}) \in \mathcal{E}\}} \right] \overset{(a)}{=} \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}_1} X_O \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}_F\}} \right] \prod_{O \notin \mathcal{O}_1} \mathbb{E}_Q \left[ X_O \right] \overset{(b)}{=} \mathbb{E}_Q \left[ \prod_{i < j \in F} X_{ij} \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}_F\}} \right] \prod_{O \notin \mathcal{O}_1} \frac{1}{1 - \rho^{2|O|}},
\]
where \((a)\) is due to the definition (56), \(\mathcal{E} \subset \mathcal{E}_F\) when \(n_1 \geq n/2\); \((b)\) holds because \(X_O\) is a function of \((A_{ij}, B_{\pi(i), \pi(j)})\) that are independent across different \(O \in \mathcal{O}\), and \(\mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}_F\}}\) only depends on \(\{(A_{ij}, B_{\pi(i), \pi(j)}) \mid (i, j) \in O : O \in \mathcal{O}_1\}\); \((c)\) follows from (37).

On the event \(\mathcal{E}_F\), we have
\[
\sum_{i < j \in F} A_{ij}^2 \geq (1 + o(1)) \left( \frac{n_1}{2} \right), \quad \sum_{i < j \in F} B_{\pi(i), \pi(j)}^2 \geq (1 + o(1)) \left( \frac{n_1}{2} \right), \quad e_{A \wedge B*}(F) \leq (1 + o(1)) \rho^{\left( \frac{n_1}{2} \right)},
\]
where we used the fact that \(n^{3/2} = o(\sqrt{n^2})\) in view of assumption \(\rho^2 \geq \log \frac{n}{n_1}\) and \(n_1 > n/2\).

It follows from (55) that
\[
\mathbb{E}_Q \left[ \prod_{i < j \in F} X_{ij} \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}_F\}} \right] = (1 - \rho^2) \left( \frac{n_1}{2} \right) \mathbb{E}_Q \left[ \exp \left\{ \frac{1}{1 - \rho^2} \left( \sum_{i < j \in F} \left( A_{ij}^2 + B_{\pi(i), \pi(j)}^2 \right) + 2\rho e_{A \wedge B*}(F) \right) \right\} \mathbf{1}_{\{(A, B, \pi) \in \mathcal{E}_F\}} \right] \leq (1 - \rho^2) \left( \frac{n_1}{2} \right) \mathbb{E}_Q \left[ \exp \left\{ \frac{2\rho e_{A \wedge B*}(F)}{1 - \rho^2} \right\} \mathbf{1}_{\{e_{A \wedge B*}(F) \leq \zeta\}} \right],
\]
where \(e_{A \wedge B*}(F) = \sum_{i < j \in F} A_{ij} B_{\pi(i), \pi(j)}\) and \(\zeta = \rho^{\left( \frac{n_1}{2} \right)} (1 + o(1))\).
Let $\beta = \frac{2\rho}{1-\rho^2}$. Then for any $\lambda \in [0, 1]$,

$$E_Q \left[ \exp \left\{ \frac{2\lambda e_{A,B^*}(F)}{1-\rho^2} \right\} 1_{\{ e_{A,B^*}(F) \leq \zeta \}} \right] \leq E_Q \left[ \exp \left\{ \beta \left( \lambda e_{A,B^*}(F) + (1-\lambda)\zeta \right) \right\} \right]$$

(59)

$$= \exp \left\{ \beta(1-\lambda)\zeta - \frac{1}{2} \binom{n_1}{2} \log(1-\beta^2\lambda^2) \right\},$$

where the equality uses the MGF expression in (24). Choosing $\lambda = (1-\rho^2)/2$ in (59), we obtain

$$\exp \left\{ \beta(1-\lambda)\zeta - \frac{1}{2} \binom{n_1}{2} \log(1-\beta^2\lambda^2) \right\} = \exp \left\{ (\beta - \rho)\zeta - \frac{1}{2} \binom{n_1}{2} \log(1-\rho^2) \right\}. $$

Combining the last three displayed equations yields that

$$E_Q \left[ \prod_{i<j \in F} X_{ij} 1_{\{(A,B,\pi) \in \mathcal{E}_F\}} \right] \leq \exp \left\{ \frac{-2\rho^2(1+o(1))}{1-\rho^2} \binom{n_1}{2} + (\beta - \rho)\zeta - \frac{3}{2} \binom{n_1}{2} \log(1-\rho^2) \right\}

= \exp \left\{ \frac{(1+o(1))\rho^2}{2} \binom{n_1}{2} \right\} \leq \exp \left\{ \frac{(1+o(1))\rho^2 n_1^2}{4} \right\},$$

where the equality holds under the assumption that $\rho = o(1)$ so that $\log(1-\rho^2) = -(1+o(1))\rho^2$.

Combining the two cases yields that

$$E_Q \left[ \left( \frac{P'(A,B)}{Q(A,B)} \right)^2 \right] \leq (1+o(1))E \left[ \prod_{O \in \mathcal{O}} \frac{1}{1-\rho^2|O|} 1_{\{n_1 \leq n/2\}} \right]

+ (1+o(1))E \left[ \prod_{O \notin \mathcal{O}_1} \frac{1}{1-\rho^2|O|} \exp \left\{ \frac{(1+o(1))\rho^2 n_1^2}{4} \right\} 1_{\{n_1 > n/2\}} \right].$$

Let $\tau = \frac{\rho^2}{1-\rho^2}$. Note that

$$\prod_{O \notin \mathcal{O}_1} \frac{1}{1-\rho^2|O|} = \left( \frac{1}{1-\rho^2} \right)^{n_2} \prod_{k \geq 2} \left( \frac{1}{1-\rho^2} \right)^{N_k} = (1+o(1)) \left( \frac{1}{1-\rho^2} \right)^{n_2} \left( \frac{1}{1-\rho^2} \right)^{N_2},$$

$$\leq (1+o(1)) \exp \left( \tau n_2 + \tau^2 N_2 \right),$$

where the first equality follows from (28), the second equality holds by (43) under the assumption $\rho^2 \leq (4-\epsilon)\log n/n$, and the last inequality holds because $\frac{1}{1-\rho^2} = 1+\tau \leq \exp(\tau)$ and $\frac{1}{1-\rho^2} \leq 1+\tau^2 \leq \exp(\tau^2)$. Similarly,\n
$$\prod_{O \in \mathcal{O}_1} \frac{1}{1-\rho^2|O|} = \left( \frac{1}{1-\rho^2} \right)^{\binom{n_1}{2}} \leq \exp \left( \tau n_1^2/2 \right).$$

---

This choice is motivated by choosing $\lambda$ to minimize $-\beta \lambda \zeta + \frac{1}{2} \binom{n_1}{2} \beta^2 \lambda^2$, the first-order approximation of the exponent in (59), leading to $\lambda^* = \zeta/\left( \binom{n_1}{2} \beta \right) = (1+o(1))(1-\rho^2)/2$.\n
Hence,
\[
\mathbb{E}_Q \left[ \left( \frac{P'(A,B)}{Q(A,B)} \right)^2 \right] \leq (1 + o(1)) \mathbb{E} \left[ \exp \left( \tau \left( n_1^2/2 + n_2 \right) + \tau^2 N_2 \right) 1_{\{n_1 \leq \frac{n}{2}\}} \right] \\
+ (1 + o(1)) \mathbb{E} \left[ \exp \left( \tau n_2 + \tau^2 N_2 \right) \exp \left\{ \frac{(1 + o(1))\rho^2 n_1^2}{4} \right\} 1_{\{n_2 > \frac{n}{2}\}} \right].
\]

We upper bound the two terms separately. To bound the first term, we apply (48) in Proposition 2 with $\mu = \tau/2$, $\nu = 0$, $a = 0$, and $b = n/2$. Recall that $\tau = \frac{\rho^2}{1 - \rho^2}$. By assumption $\rho^2 \leq (4 - \epsilon) \log n/n$, we have $\tau^2 = o\left(\frac{1}{n}\right)$ and $\mu b + 2 - \log b = \frac{\rho^2}{4(1 - \rho^2)} + 2 - \log(n/2) \leq 0$ for all sufficiently large $n$. Thus it follows from (48) in Proposition 2 that
\[
\mathbb{E} \left[ \exp \left( \tau \left( n_1^2/2 + n_2 \right) + \tau^2 N_2 \right) 1_{\{n_1 \leq \frac{n}{2}\}} \right] \leq 1 + o(1).
\]

To bound the second term, we apply (47) in Proposition 2 with $\mu = \frac{(1+o(1))\rho^2}{4}$, $\nu = 0$, $a = \frac{n}{2}$, and $b = n$. Recall that $\tau = \frac{\rho^2}{1 - \rho^2}$. By assumption $n\rho^2 \leq (4 - \epsilon) \log n$, we have $\tau^2 = o\left(\frac{1}{n}\right)$ and $\mu b + \nu + 2 - \log b = \frac{(1+o(1))\rho^2 n}{4} + 2 - \log n \leq 0$ for sufficiently large $n$. Thus it follows from (47) in Proposition 2 that
\[
\mathbb{E} \left[ \exp \left( \tau n_2 + \tau^2 N_2 \right) \exp \left\{ \frac{(1 + o(1))\rho^2 n_1^2}{4} \right\} 1_{\{n_2 > \frac{n}{2}\}} \right] = o(1).
\]

Combining the upper bounds for the two terms, we conclude that $\mathbb{E}_Q \left[ \left( \frac{P'(A,B)}{Q(A,B)} \right)^2 \right] = 1 + o(1)$ under the assumption that $\rho^2 \leq (4 - \epsilon) \log n/n$. Thus TV($P, Q$) = $o(1)$ in view of (54).

5. Conditional Second Moment Method: Sparse regime. We focus on the Erdős-Rényi model in the sparse regime of $p = n^{-\Omega(1)}$. The impossibility condition previously obtained in Theorem 3 by the unconditional second moment simplifies to $s^2 \leq (2 - \epsilon) \log n/n$. In this section, we significantly improve this result by showing that if
\[
(60) \quad s^2 \leq \frac{1 - \omega(n^{-1/3})}{np} \land 0.01,
\]
then strong detection is impossible. Moreover, if both $s = o(1)$ and (60) hold, then weak detection is impossible.

Analogous to the proof for the dense case in Section 4 (see also Section 7.3), we will apply the conditional second moment method. However, the argument in the sparse case is much more sophisticated for the following reason. In the dense regime (both Gaussian and Erdős-Rényi graph with $p = n^{-o(1)}$), we have shown that the main contribution to the second moment is due to fixed points of $\sigma = \pi^{-1} \circ \pi$, which can be regulated by conditioning on the edge density of large induced subgraphs in the intersection graph. For sparse Erdős-Rényi graphs with $p = n^{-\Omega(1)}$, we need to control the contribution of not just fixed points, but all edge orbits of length up to $k = \Theta(\log n)$. Indeed, as argued in Section 3.3, the unconditional second moment blows up when $\rho^2 k \geq (2 + \epsilon) \log n/n$ due to the obstructions from the $k$-edge orbits, or more precisely, an atypically large magnitude of $\prod_{|O|=k} X_O$. Note that $\rho = \frac{s(1-p)}{1-ps} = (1+o(1))s$ in the sparse case. Therefore, to show the desired condition (60), we need to regulate $\prod_{|O|=k} X_O$ beyond $k = 1$ by proper conditioning. In fact, for $p = \Theta(1/n)$, since (60) reduces to $\rho \leq 0.1$, it is necessary to control all $k$ up to $\Theta(\log n)$. 
To this end, the crucial observation is as follows. We call a given edge orbit \( O \) of \( \sigma = \pi^{-1} \circ \pi \) complete if it is a subgraph of the intersection graph \( A \cap B^\pi \), i.e. \( O \subset E ( A \cap B^\pi ) \). For each complete orbit \( O \), we have \( A_{ij} = B_{\pi(i)\pi(j)} = B_{\pi(i)\bar{\pi}(j)} = 1 \) for all \((i, j) \in O\) and hence, by (21) and (30), \( X_{ij} = L(1, 1)^2 = 1/p^2 \), so that \( X_O \) attains its maximal possible value, namely

\[
X_O = \left( \frac{1}{p} \right)^{2|O|}, \quad \forall O \subset E ( A \cap B^\pi ).
\]

For incomplete orbits, it is not hard to show (see Proposition 4 below) that

\[
\mathbb{E}_Q [ X_O \mid O \not\subset A \cap B^\pi ] \leq 1.
\]

Hence, the key is to control the contribution of complete edge orbits \( O \) that are subgraphs of \( A \cap B^\pi \). Crucially, under the assumption of Theorem 2 in the sparse regime, \( np\sigma^2 \) is sufficiently small so that \( A \cap B^\pi \) is subcritical and a pseudoforest (each component having at most one cycle) with high probability under the planted model \( P \). This global structure significantly limits the possible configurations of complete edge orbits, since many patterns of co-occurrence of edge orbits in \( A \cap B^\pi \) are forbidden. Motivated by this observation, we truncate the likelihood ratio by conditioning on the global event that \( A \cap B^\pi \) is a pseudoforest. Finally, in order to show the conditional second moment is bounded under the desired condition (60), we carefully control the co-occurrence of edge orbits in \( A \cap B^\pi \) under the pseudoforest constraint, which involves a delicate enumeration of pseudoforests that can be assembled from edge orbits.

Next, let us proceed to the rigorous analysis. Define

\[
\mathcal{E} \triangleq \{ (A, B, \pi) : A \cap B^\pi \text{ is a pseudoforest} \}.
\]

Note that \( A \cap B^\pi \sim \mathcal{G}(n, ps^2) \) under the planted model \( P \). The following result shows that in the subcritical case \( A \cap B^\pi \) is a pseudoforest.

**Lemma 2 ([20, Lemma 2.10])**. If \( np\sigma^2 \leq 1 - \omega \left(n^{-1/3}\right) \), then \( \mathcal{P} ((A, B, \pi) \in \mathcal{E}) \to 1 - o \left( \frac{1}{n} \right) \) as \( n \to \infty \).

Recall from (29) and (34) in Section 3.2 the following representation of the squared likelihood ratio

\[
\frac{\mathcal{P}(A, B)}{\mathcal{Q}(A, B)} = \mathbb{E}_{\pi, \pi} \left[ \prod_{O \in \mathcal{O}} X_O \right],
\]

where for each edge orbit \( O \) of \( \sigma = \pi^{-1} \circ \pi \),

\[
X_O = \prod_{ij \in O} X_{ij}, \quad X_{ij} = L(A_{ij}, B_{\pi(i)\pi(j)}) L(A_{ij}, B_{\pi(i)\bar{\pi}(j)}),
\]

with \( L(\cdot, \cdot) \) is defined in (21). In order to decompose (62) further, let us introduce the following key definitions. Recall from Section 3.1 that \( O_i \) denotes the node-orbit of \( i \) (under the node permutation \( \sigma \)) and \( O_{ij} \) denotes the edge-orbit of \((i, j) \) (under the edge permutation \( \sigma^2 \)). Fix some \( k \) to be specified later.

- Define \( \mathcal{O}_k \) as the set of edge orbits of length at most \( k \) that are formed by node orbits with length at most \( k \), that is,

\[
\mathcal{O}_k = \{O_{ij} : |O_i| \leq k, |O_j| \leq k, |O_{ij}| \leq k, 1 \leq i < j \leq n\}.
\]
• Define \( J_k \) as the set of edge orbits \( O \in \mathcal{O}_k \) that are subgraphs of \( A \lor B^\pi \), i.e.,
\[
J_k = \{ O \in \mathcal{O}_k : A_{ij} = 1, B_{\pi(i)\pi(j)} = 1, \forall (i,j) \in O \}
\]
\[
= \{ O \in \mathcal{O}_k : A_{ij} = 1, B_{\tilde{\pi}(i)\tilde{\pi}(j)} = 1, \forall (i,j) \in O \},
\]
where the second equality holds because \( \{ B_{\pi(i)\pi(j)} \}_{(i,j)\in O} = \{ B_{\tilde{\pi}(i)\tilde{\pi}(j)} \}_{(i,j)\in O} \).

• Define
\[
(63) \quad H_k = \bigcup_{O \in J_k} O.
\]

Note that while \( \mathcal{O}_k \) depends only on the random permutation \( \sigma = \pi^{-1} \circ \tilde{\pi} \), both \( J_k \) and \( H_k \) depend in addition on the random graph \( A \lor B^\pi \).

As will be discussed at length in Section 5.1, each edge orbit can be viewed as a subgraph of the complete graph \( K_n \). Different edge orbits are by definition edge disjoint, and the union of all edge orbits is the edge set of \( K_n \). We shall call a graph an orbit graph if it is union of edge orbits. Importantly, by definition, the orbit graph \( H_k \) is a subgraph of \( A \lor B^\pi \).

To compute the conditional second moment, by Lemma 2, it follows from (52) that
\[
(64) \quad \mathbb{E}_Q \left[ \left( \frac{p'(A,B)}{Q(A,B)} \right)^2 \right] = (1 + o(1)) \mathbb{E}_{\pi \lor \tilde{\pi}} \left[ \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O 1_{\{ (A,B,\pi) \in E \}} 1_{\{ (A,B,\tilde{\pi}) \in E \}} \right] \right]
\]
\[
\leq (1 + o(1)) \mathbb{E}_{\pi \lor \tilde{\pi}} \left[ \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O 1_{\{ H_k \text{ is a pseudoforest} \}} \right] \right],
\]
where the last inequality holds because on the event that \( A \lor B^\pi \) is a pseudoforest, its subgraph \( H_k \) is also one.

To further upper bound the right hand side of (64), we decompose the product over edge orbits into three terms:
\[
\prod_{O \in \mathcal{O}} X_O = \prod_{O \in \mathcal{O} \setminus J_k} X_O \times \prod_{O \in \mathcal{O} \setminus \bar{J}_k} X_O \times \prod_{O \in J_k} X_O
\]
which correspond to the contributions of long orbits, short incomplete orbits (that are not subgraphs of \( A \lor B^\pi \)), and short complete orbits (that are subgraphs), respectively. As shown earlier in (61), for each complete edge orbit \( O \), we have \( X_O = (1/p)^{2|O|} \). Therefore in view of (63), the collective contribution of short complete orbits are
\[
(65) \quad \prod_{O \in J_k} X_O = \left( \frac{1}{p} \right)^{2e(H_k)}.
\]

Thus, fixing \( \sigma = \pi^{-1} \circ \tilde{\pi} \), we have
\[
\mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O 1_{\{ H_k \text{ is a pseudoforest} \}} \right]
\]
\[
= \mathbb{E}_Q \left[ \prod_{O \notin \mathcal{O}_k} X_O \right] \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}_k} X_O 1_{\{ H_k \text{ is a pseudoforest} \}} \right]
\]
\[
(66) \quad = \mathbb{E}_Q \left[ \prod_{O \notin \mathcal{O}_k} X_O \right] \mathbb{E}_{\bar{J}_k} \left[ \left( \frac{1}{p} \right)^{2e(H_k)} 1_{\{ H_k \text{ is a pseudoforest} \}} \right] \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O} \setminus \bar{J}_k} X_O \right].
\]
where the first equality holds because \( \{ X_O \}_{O \in \mathcal{O}} \) are mutually independent and \( J_k \subset O_k \), so that \( \{ X_O \}_{O \in \mathcal{O} \setminus O_k} \) is independent of \( \{ X_O \}_{O \in O_k} \) and the event that \( H_k \) is a pseudoforest; the second equality holds because \( H_k \) is measurable with respect to \( J_k \).

The contributions of long orbits and incomplete orbits can be readily bounded as follows whose proofs are deferred till Sections 8.1 and 8.2.

**Proposition 3 (Long orbits).** Fix any \( \sigma = \pi^{-1} \circ \bar{\pi} \). For any \( k \in \mathbb{N} \),

\[
\mathbb{E}_Q \left[ \prod_{O \in \mathcal{O} \setminus O_k} X_O \right] \leq \left( 1 + \rho^k \right)^{\frac{n^2}{2}}.
\]

**Proposition 4 (Incomplete orbits).** Fix any \( \sigma = \pi^{-1} \circ \bar{\pi} \). If \( p \leq 1/2 \) and \( s \leq 1/2 \), then

\[
\mathbb{E}_Q \left[ \prod_{O \in O_k \setminus J_k} X_O \right] \leq 1.
\]

Applying Proposition 3 and Proposition 4 to (66), we get that for any \( \sigma = \pi^{-1} \circ \bar{\pi} \),

\[
(67) \quad \mathbb{E}_Q \left[ \prod_{O \in \mathcal{O}} X_O 1_{\{H_k \text{ is a pseudoforest}\}} \right] \leq \left( 1 + \rho^k \right)^{\frac{n^2}{2}} \mathbb{E}_{J_k} \left[ \left( \frac{1}{p} \right)^{2e(H_k)} \right] 1\{H_k \text{ is a pseudoforest}\}
\]

It remains to further upper bound the RHS of (67). Let \( \mathcal{H}_k \) denote the set of all orbit graphs that consist of edge orbits in \( O_k \) and are pseudoforests – we call such graphs orbit pseudoforests. As such \( \mathcal{H}_k \) depends only on \( \sigma \) but not the graph \( A \) and \( B \). Therefore,

\[
(68) \quad \mathbb{E}_{J_k} \left[ \left( \frac{1}{p} \right)^{2e(H_k)} \right] 1\{H_k \text{ is a pseudoforest}\} = \sum_{H \in \mathcal{H}_k} Q(H_k = H) \left( \frac{1}{p} \right)^{2e(H)} 1\{H \text{ is a pseudoforest}\} \leq \sum_{H \in \mathcal{H}_k} s^{2e(H)},
\]

where the last step holds because

\[
Q(H_k = H) \leq Q \left( A_{ij} = 1, B_{\pi(i) \pi(j)} = 1, \forall (i,j) \in E(H) \right) = (ps)^{2e(H)}.
\]

In view of (68), to further upper bound the second moment, it boils down to bounding the the generating function of the class \( \mathcal{H}_k \) of orbit pseudoforests. This is done in the following theorem in terms of the cycle type of \( \sigma \). The proof involves a delicate enumeration of orbit pseudoforests, which constitutes the most crucial part of the analysis. We note that if we ignore the orbit structure and treat \( \mathcal{H}_k \) as arbitrary pseudoforests, the resulting bound will be too crude to be useful.

**Theorem 4 (Generating function of orbit pseudoforests).** For any \( k \in \mathbb{N} \), \( \sigma = \pi^{-1} \circ \bar{\pi} \), and any \( s \in [0, 1] \),

\[
(69) \quad \sum_{H \in \mathcal{H}_k} s^{2e(H)} \leq \prod_{m=1}^{k} \left( 1 + s^m n_m 1_{\{m \text{ even}\}} + 2s^{2m} \sum_{t=1}^{m} \ell n_{\ell t} + s^{4m} mn_{2m} 1_{\{2m \leq k\}} \right)^{n_m},
\]

where \( n_m \) is the number of \( m \)-node orbits in \( \sigma = \pi^{-1} \circ \bar{\pi} \) for \( 1 \leq m \leq k \).
Combining (64), (67), (68), and (69), we get that
\[
\mathbb{E}_Q \left[ \left( \frac{P'(A, B)}{Q(A, B)} \right)^2 \right] 
\]
\[
\leq (1 + o(1)) \left( 1 + \rho^k \right) \frac{s^2}{2} \mathbb{E}_{\Pi \perp \tilde{Q}} \left[ \prod_{m=1}^{k} \left( 1 + s^m n_m 1_{\{m: \text{even}\}} + 2s^{2m} \sum_{\ell \leq m} \ell n_\ell + s^{4m} m n_{2m} 1_{\{2m \leq k\}} \right) \right]^{n_m},
\]
which is further bounded by the next result.

**Proposition 5.** Suppose \( k(\log k)^4 = o(n) \). If \( s \leq 0.1 \),
\[
\mathbb{E}_{\Pi \perp \tilde{Q}} \left[ \prod_{m=1}^{k} \left( 1 + s^m n_m 1_{\{m: \text{even}\}} + 2s^{2m} \sum_{\ell \leq m} \ell n_\ell + s^{4m} m n_{2m} 1_{\{2m \leq k\}} \right) \right]^{n_m} = O(1).
\]
Furthermore, if \( s = o(1) \),
\[
\mathbb{E}_{\Pi \perp \tilde{Q}} \left[ \prod_{\ell = m}^{k} \left( 1 + s^m n_m 1_{\{m: \text{even}\}} + 2s^{2m} \sum_{\ell \leq m} \ell n_\ell + s^{4m} m n_{2m} 1_{\{2m \leq k\}} \right) \right]^{n_m} = 1 + o(1).
\]

The proof of Proposition 5 is involved and deferred to Section 8.3. To provide some concrete idea, the following simple calculation shows that \( s = o(1) \) is necessary for (72) to hold. Indeed, consider \( k = 1 \) for which the LHS reduces to \( \mathbb{E} \left[ (1 + 2s^2 n_1)^{n_1} \right] \). By Poisson approximation (see Appendix 10), replacing \( n_1 \) by \( \text{Poi}(1) \) yields
\[
\mathbb{E} \left[ (1 + 2s^2 n_1)^{n_1} \right] \approx e^{-1} \sum_{a=0}^{\infty} (1 + 2s^2 a) \frac{1}{a!} \geq e^{-1} \sum_{a=0}^{\infty} (1 + 2s^2) \frac{1}{a!} = e^{2s^2},
\]
which is \( 1 + o(1) \) if and only if \( s = o(1) \). To evaluate the full expectation in (72), note that even if we use Poisson approximation to replace \( n_m \)'s by independent Poissons, the terms inside the product over \([k]\) are still dependent. To this end, we carefully partition the product into disjoint parts, and recursively peeling off the expectation backwards.

We are now ready to complete the proof of Theorem 2 in the sparse case.

**Proof of Theorem 2: Impossibility Result in Sparse Regime.** Let \( k = 3 \log n \). If \( s \leq \frac{1}{2} \), then \( n^2 s^k = o(1) \) and thus
\[
\left( 1 + \rho^k \right)^{\frac{s^2}{2}} \leq \exp \left( \frac{n^2 \rho^k}{k} \right) \leq \exp \left( \frac{n^2 s^k}{k} \right) = 1 + o(1).
\]
Note that \( k(\log k)^4 = o(n) \). Combining (70) with (71) and (72) yields that \( \mathbb{E}_Q \left[ \left( \frac{P'(A, B)}{Q(A, B)} \right)^2 \right] = O(1) \) for \( s \leq 0.1 \) and \( \mathbb{E}_Q \left[ \left( \frac{P'(A, B)}{Q(A, B)} \right)^2 \right] = 1 + o(1) \) for \( s = o(1) \), which completes the proof in view of (53) and (54).

The remainder of this section is organized as follows. To prepare for the proof of Theorem 4, we study the graph structure and the classification of edge orbits in Section 5.1.
equivalent representation of orbit graphs as backbone graphs is given in Section 5.2 to aid the enumeration argument. As a warm-up, we first enumerate orbit forests (orbit graphs that are forests) and bound their generating function in Section 5.3. The more challenging case of orbit pseudoforests is tackled in Section 5.4, completing the proof of Theorem 4. Sections 8.1–8.3 contain the proofs of Propositions 3–5.

<table>
<thead>
<tr>
<th>Type</th>
<th>Edge orbit</th>
<th>Orbit graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>(13,24)</td>
<td><img src="https://example.com/diagram1.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>(14,23)</td>
<td><img src="https://example.com/diagram2.png" alt="Diagram" /></td>
</tr>
<tr>
<td>B</td>
<td>(15,26,17,28)</td>
<td><img src="https://example.com/diagram3.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>(16,27,18,25)</td>
<td><img src="https://example.com/diagram4.png" alt="Diagram" /></td>
</tr>
<tr>
<td>C</td>
<td>(35,46,37,48)</td>
<td><img src="https://example.com/diagram5.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>(36,47,38,45)</td>
<td><img src="https://example.com/diagram6.png" alt="Diagram" /></td>
</tr>
<tr>
<td>S</td>
<td>(12)</td>
<td><img src="https://example.com/diagram7.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>(34)</td>
<td><img src="https://example.com/diagram8.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>(57,68)</td>
<td><img src="https://example.com/diagram9.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>

**Table 2**

Edge orbits corresponding to the node permutation $\sigma = (12)(34)(5678)$. When representing an edge orbit in cycle notation, each edge $(i,j)$ is abbreviated as $ij$. As a convention, nodes in each node orbit are vertically aligned and arranged in the order of the permutation $\sigma$. For edge orbits, type M are in green, type B in red, type C in blue, and type S in black.
5.1. Classification of edge orbits. To prove Theorem 4, we are interested in orbit graphs consisting of short edge orbits, and the main task lies in enumerating those that are pseudo-forests. To this end, we need to understand the graph structure of edge orbits.

Throughout this subsection, fix a node permutation σ. For a given edge \((i, j)\), its edge orbit can be viewed as a graph with vertex set \(O_i \cup O_j\) and edge set \(O_{ij}\). Let \(|O_i| = \ell\) and \(|O_j| = m\). Each edge orbit can be classified into the following four categories (see Table 2 for a concrete example).

Type M (Matching): \(i\) and \(j\) belong to different node orbits of the same length. In this case, \(|O_{ij}| = m\) and \(O_{ij}\) is a perfect matching. We call such \(O_{ij}\) an \(M_m\) edge orbit (or a matching). Furthermore, for two distinct node orbits \(O\) and \(O'\) of length \(m\), the total number of possible \(M_m\) edge orbit is \(m\).

Type B (Bridge): \(i\) and \(j\) belong to different node orbits of different lengths. Without loss of generality, assume that the orbit of \(i\) is shorter than that of \(j\), i.e. \(\ell < m\). In this case, let \(M = \text{lcm}(\ell, m)\). Then \(|O_{ij}| = M\) and \(O_{ij}\) consists of \(\frac{\ell m}{M}\) vertex-disjoint copies of the complete bipartite graphs \(K_{M/\ell, M/m}\). We call such edge orbit a \(B_{m, \ell}\) edge orbit (or a bridge). Furthermore, for two node orbits \(O\) and \(O'\) with \(|O| = \ell < |O'| = m\), the total number of possible bridges is \(\frac{\ell m}{M}\).

Of special interest is the case where \(\ell\) is a divisor of \(m\) and the orbit is \(\ell K_{1, \frac{m}{\ell}}\) (i.e. \(\ell\) copies of \(m/\ell\)-stars). These are the only bridges that are cycle-free; otherwise the bridge contains a component with at least two cycles. This observation is useful for the enumeration argument in Sections 5.3 and 5.4 under constraints on the number of cycles.

Type C (Cycle): \(i\) and \(j\) belong to the same node orbit of length \(m\) and \(j \neq \sigma^{m/2}(i)\). In this case, \(|O_{ij}| = m\) and \(O_{ij}\) is an \(m\)-cycle. We call such \(O_{ij}\) a \(C_m\) edge orbit (or a cycle), and there are a total number of \(\left\lfloor \frac{m-1}{2} \right\rfloor\) of them for the same node orbit.

Type S (Split): \(i\) and \(j\) belong to the same node orbit (of even length \(m\)) and \(j = \sigma^{m/2}(i)\). In this case, \(|O_{ij}| = m/2\) and \(O_{ij}\) is a perfect matching. We call such \(O_{ij}\) an \(S_m\) edge orbit (or a split). Clearly, for each node orbit of even length, there is a unique way for it to split into an \(S_m\) edge orbit.

In summary, matchings and bridges are edge orbits formed by two distinct node orbits, which are bipartite graphs with vertex sets \(O_i\) and \(O_j\). Cycles and splits are edge orbits formed by a single node orbit \(O_i\), which can either form a full cycle or split into a perfect matching.

5.2. Orbit graph and backbone graph. Every orbit graph \(H\) can be equivalently and succinctly represented as a backbone graph \(\Gamma\) defined as follows.

**Definition 2** (Backbone graph). Given an orbit graph \(H\), its backbone graph is an undirected labeled multigraph, whose nodes and edges (referred to as giant nodes and giant edges) correspond to node orbits and edge orbits in \(H\), respectively. Each giant node carries a binary label (represented as shaded or non-shaded) indicating whether the node orbit forms a Type S edge orbit (split) or not. Each giant edge carries a label (an integer) encoding the specific realization of the edge orbit. Specially,

- A Type S edge orbit (split) is represented by a shaded giant node.
- A Type \(C_m\) edge orbit (cycle) is represented by a self-loop, whose edge label takes values in \(\left[\left\lfloor \frac{m-1}{2} \right\rfloor\right]\).
- A Type \(M_m\) edge orbit (matching) is represented by a giant edge between two \(m\)-node orbits, with edge label taking values in \([m]\).
- A Type \(B_{m, \ell}\) edge orbit (bridge) is represented by a giant edge between a \(\ell\)-node orbit and a \(m\)-node orbit (\(\ell < m\)), with edge label taking values in \(\left[\frac{\ell m}{\text{lcm}(\ell, m)}\right]\).
See Fig. 2 for an example of an orbit graph and its corresponding backbone graph. As a convention, for backbone graph, the labeled giant edges representing Type M, Type B, and Type C edge orbits are colored green, red, and blue, respectively. Each shaded giant node represents a Type S edge orbit. For convenience, the number inside each giant node represents the length of its corresponding node orbit.

Recall that $\mathcal{H}_k$ denotes the collection of orbit pseudoforests consisting of edge orbits of length at most $k$ formed by node orbits of size at most $k$. To enumerate $H \in \mathcal{H}_k$, it is equivalent to enumerating the corresponding backbone graph $\Gamma$. To facilitate the enumeration, we introduce the following definitions:

- Let $S_m$ denote the set of giant nodes corresponding to $m$-node orbits.
- Let $\Gamma_m = \Gamma[S_m]$ denote the subgraph of $\Gamma$ induced by node set $S_m$ for $1 \leq m \leq k$. Let $\Gamma_{m,\ell} = \Gamma[S_m, S_{\ell}]$ denote the (bipartite) subgraph of $\Gamma$ induced by edges between $S_m$ and $S_{\ell}$, for $1 \leq \ell < m \leq k$. Each giant edge in $\Gamma_{m,\ell}$ corresponds to a $B_{m,\ell}$ edge orbit (bridge).
- A connected component of $\Gamma_m$ is called plain if it contains no split and is not incident to any bridge in $\bigcup_{\ell<m} \Gamma_{m,\ell}$.

Following [27, page 112], we define the excess of a graph $G$, denoted by $\text{ex}(G)$, as its number of edges minus its number of nodes. Given a connected component $C$ in $\Gamma_m$, let $H_C$ denote the orbit graph consisting of edge orbits (including splits, matchings, and cycles) in $C$, as well as bridges in $\bigcup_{\ell<m} \Gamma_{m,\ell}$ that are incident to $C$. The following two operations can be recursively applied to $C$ to increase $\text{ex}(H_C)$:

(O1) Adding one split in $C$ increases $\text{ex}(H_C)$ by $m/2$;
(O2) Adding one $B_{m,\ell}$ bridge ($\ell < m$) to $C$ increases $\text{ex}(H_C)$ by at least $\text{lcm}(\ell, m) - \ell$.

In addition, we need the following fact about the excess of an orbit graph:

**Lemma 3.** For any connected component $C$ in $\Gamma_m$, $\text{ex}(H_C) \geq -m$, where the equality holds if and only if $C$ is a plain tree component in $\Gamma_m$.

**Proof.** Given a connected component $C$ in $\Gamma_m$, let $a$ and $b$ denote the total number of giant edges and giant nodes in $C$, respectively. If $C$ is a plain tree component, we have $a + 1 = b$. Since each giant edge in $\Gamma_m$ represents an $m$-edge orbit, and each giant node
represent an \( m \)-node orbit, we have \( \text{ex}(H_C) = am - bm = -m \). By (O1), (O2), and the fact that adding one self-loop in \( C \) increases \( \text{ex}(H_C) \) by \( m \), we have \( \text{ex}(H_C) \geq -m \), where the equality holds if and only if \( C \) does not contain any split or self-loop and is not incident to any bridge in \( \cup_{\ell < m} B_{m,\ell} \) that is, \( C \) is a plain tree component in \( \Gamma_m \).

As we will see next, the pseudoforest (forest) constraint of \( H \) restricts the possible configurations of \( \Gamma_m \) and forbids certain operations on its components (which would otherwise generate too many cycles).

5.3. Warm-up: Generating function of orbit forests. Fix \( \sigma = \pi^{-1} \circ \tilde{\pi} \) and recall that \( n_m \) denotes the number of \( m \)-node orbits in \( \sigma \). Our enumeration scheme crucially exploits the classification of edge orbits and orbit graphs in Section 5.1 and the representation of orbit graphs as backbone graphs introduced in Section 5.2. As a warm-up, in this section we bound the generating function of orbit forests, which is much simpler than orbit pseudoforests. Restricting the summation to the set \( F_k \) of orbit forests, a strict subset of \( H_k \), we show the following improved version of (69):

\[
\sum_{H \in F_k} s^{2e(H)} \leq \prod_{1 \leq m \leq k} \left( 1 + s^m \mathbf{1}_{\{m:\text{even}\}} + s^{2m} \sum_{\ell \leq m} \ell n_{\ell} \right)^{n_m}.
\]

(73)

When the orbit graph \( H \) is a forest, its corresponding backbone graph \( \Gamma \) must satisfy the following four conditions:

(T1) For each \( 1 \leq m \leq k \), \( \Gamma_m \) is a forest with simple edges (of multiplicity 1);
(T2) For each \( 1 \leq \ell < m \leq k \), \( \Gamma_{m,\ell} \) is empty unless \( \ell \) is a divisor of \( m \);
(T3) There is no self-loop;
(T4) For each \( 1 \leq m \leq k \), each component of \( \Gamma_m \) either contains at most 1 split or is incident to at most 1 bridge in \( \cup_{\ell < m} \Gamma_{m,\ell} \), but not both.

Otherwise, \( H \) contains at least one cycle. Indeed, (T1)-(T3) can be readily verified based on the classification of edge orbits and orbit graphs in Section 5.1. Suppose the condition in (T4) does not hold. Then by (O1), (O2) and Lemma 3, there exists a component \( C \) in \( \Gamma_m \) such that \( \text{ex}(H_C) \geq 0 \), contradicting \( H \) being a forest. See Fig. 3 for an illustration of forbidden patterns that violate (T4) for \( m = 4 \) and \( \ell = 2 \).

\[\text{(a) A component in } \Gamma_4 \text{ is incident to 2 bridges in } \Gamma_{4,2}^4.\]
\[\text{(b) A component in } \Gamma_4 \text{ contains 2 splits.}\]
\[\text{(c) A component in } \Gamma_4 \text{ contains 1 split and is incident to 1 bridge in } \Gamma_{4,2}^4.\]

Fig 3: Examples of backbone graphs violating (T4), whose corresponding orbit graphs contain cycles.

Next, we describe an algorithm for generating all possible backbone graphs \( \Gamma \) that satisfy the aforementioned conditions (T1)–(T4). Given a sequence of integers \( (a, b, c) = (a_m, b_m, c_m)_{1 \leq m \leq k} \) with \( b_m = 0 \) for odd \( m \), we construct \( \Gamma \) as follows:
Algorithm 1 Forest enumeration algorithm

1: for each $t = 1, \ldots, k$ do
2: \hspace{1em} \textbf{Step 1: Matching stage.} Construct a rooted forest $\Gamma_t$ with $n_t$ giant nodes and $a_t$ giant edges; Attach a label from $[t]$ to each giant edge;
3: \hspace{1em} \textbf{Step 2: Splitting stage.} Choose $b_t$ components from $n_t - a_t$ tree components of $\Gamma_t$, and within each chosen component, add a split to the root;
4: \hspace{1em} \textbf{Step 3: Bridging stage.} Choose $c_t$ out of the remaining $n_t - a_t - b_t$ tree components of $\Gamma_t$, and for each chosen component, add a bridge connecting its root to a giant node in $\Gamma_\ell$ for some $\ell < t$ that is a divisor of $t$. Attach a label from $[\ell]$ to the added bridge.
5: \hspace{1em} end for

We claim that any orbit forest can be generated by Algorithm 1. To verify this claim formally, let $H$ be an orbit forest and $\Gamma$ denote the its corresponding backbone graph in Definition 2, which, for $1 \leq m \leq k$, contains
- $a_m$ matchings corresponding to Type $M_m$ edge orbits;
- $b_m$ splits corresponding to Type $S_m$ edge orbits;
- $c_m$ bridges corresponding to Type $B_{m, \ell}$ edge orbits for some $\ell < m$ that is a divisor of $m$.

For each $\Gamma_m$, we arbitrarily choose the root for each plain tree component, and specify the root in each non-plain tree component as the unique giant node that either splits or is incident to a bridge in $\cup_{\ell < m} \Gamma_{m, \ell}$. Then clearly Steps 1–3 can realize any configuration of matchings, splits and bridges in $\Gamma$, thanks to the properties (T1)-(T4).

Note that the total number of edges in the corresponding orbit forest $H$ is determined by the input parameter $(a, b, c)$ as

$$
\sum_{m=1}^{k} \left[ m(a_m + c_m) + mb_m/2 \right].
$$

To enumerate the orbit forests, it suffices to count all possible output backbone graphs $\Gamma$ of Algorithm 1 as follows. For $t = 1, \ldots, k$,

1. It is well-known that the total number of rooted forests on $n$ vertices with $a$ edges is

$$
\binom{n-1}{a} n^a
$$

(see e.g. [19, II.18, p. 128].) Moreover, each giant edge added in Step 1 has $t$ possible labels. Therefore, the total number of rooted backbone graphs $\Gamma_t$ is at most

$$
\binom{n_t - 1}{a_t} (tn_t)^{a_t} \leq \binom{n_t}{a_t} (tn_t)^{a_t}.
$$

(75)

2. The total number of ways of placing $b_t$ splits is at most

$$
\binom{n_t - a_t}{b_t}.
$$

(76)

3. The total number of ways of placing $c_t$ bridges is at most

$$
\binom{n_t - a_t - b_t}{c_t} \left( \sum_{\ell < t} \ell n_\ell \right)^{c_t}.
$$

(77)

Note that we could further restrict the summation over $\ell$ to divisors of $t$ and get a tighter upper bound, but this is not needed for the main results.
Combining (75), (76), and (77), we get that the total number of output backbone graphs $\Gamma$ with input parameter $(a, b, c)$ is at most

\[
\prod_{1 \leq t \leq k} 1_{\{b_t = 0 \text{ for odd } t\}} \left( \frac{n_t}{a_t, b_t, c_t} \right)^{\sum_{\ell < t} \ell n_{\ell}} c_t .
\]

Then the desired (73) readily follows from

\[
\sum_{H \in \mathcal{F}_k} s^{2e(H)} \leq \sum_{a, b, c} \prod_{1 \leq t \leq k} 1_{\{b_t = 0 \text{ for odd } t\}} \left( \frac{n_t}{a_t, b_t, c_t} \right)^{\sum_{\ell < t} \ell n_{\ell}} c_t \left( n t a_t, b_t, c_t \right)^{s^{2t a_t + t b_t + 2 t c_t}}
\]

\[
\leq \prod_{1 \leq t \leq k} \left( 1 + s^t 1_{\{t: \text{even}\}} + s^{2t} \sum_{\ell \leq t} \ell n_{\ell} \right)^{n_t} .
\]

5.4. Proof of Theorem 4: Generating function of orbit pseudoforests. Fix $\sigma = \pi^{-1} \circ \tilde{\pi}$ and recall $n_m$ denotes the number of $m$-node orbits in $\sigma$. In this section we bound the generating function (68) of orbit pseudoforests $H \in \mathcal{H}_k$ and prove Theorem 4. Recall that each orbit graph $H$ can be equivalently represented as a backbone graph $\Gamma$ as in Definition 2. In addition, we need the following vocabularies: For $1 \leq m \leq k$ and each $u \in S_m$, let $C(u)$ denote the connected component in $\Gamma_m$ containing $u$.

Similar to the reasoning in Section 5.3, when $H$ is a pseudoforest, its backbone graph $\Gamma$ must satisfy the following properties:

(P1) For each $1 \leq m \leq k$, $\Gamma_m$ is a pseudoforest (with self-loops and parallel edges counted as cycles);

(P2) For each $1 \leq \ell < m \leq k$, $\Gamma_{m,\ell}$ is empty unless $\ell$ is a divisor of $m$.

(P3) Each unicyclic component of $\Gamma_m$ is plain.

(P4) A tree component in $\Gamma_m$ contains at most two splits.

(P5) Let $(u, v) \in \Gamma_{m,\ell_1}$ and $(u', v') \in \Gamma_{m,\ell_2}$ be two bridges with $\ell_1, \ell_2 < m$, such that $u$ and $u'$ belong to the same tree component in $\Gamma_m$. Then $m$ must be even and $\ell_1 = \ell_2 = m/2$.

(P6) Let $(u, v) \in \Gamma_{m,\ell}$ be a bridge with $\ell < m$ such that $u$ belongs to a tree component that contains a split in $\Gamma_m$. Then $m$ must be even and $\ell = m/2$. Furthermore, $v$ must belong to a plain tree component in $\Gamma_{m/2}$.

(P7) For each $(u, v)$ and $(u', v')$ that satisfy either (P5) or (P6) where $v \neq v'$, the ending points $v$ and $v'$ must belong to distinct plain tree components in $\Gamma_{m/2}$.

Otherwise, $H$ contains a component with at least two cycles, violating the pseudoforest constraint. See Fig. 4 - Fig. 6 for illustrations of forbidden patterns that violate (P4) - (P7).
(a) A component in $\Gamma_4$ contains 3 splits.
(b) A component in $\Gamma_4$ is incident to a bridge $(u,v) \in \Gamma_{4,1}$ and a bridge $(u',v') \in \Gamma_{4,2}$.

Fig 4: Examples of backbone graphs violating (P4) and (P5), shown in (a) and (b), respectively, and the corresponding orbit graphs.

(a) A component in $\Gamma_4$ contains 1 split and is incident to 1 bridge $(u,v) \in \Gamma_{4,1}$.
(b) A component in $\Gamma_4$ contains 1 split and is incident to 1 bridge $(u,v) \in \Gamma_{4,2}$ where $v$ is in a non-plain component in $\Gamma_2$ that is incident to 1 bridge in $\Gamma_{2,1}$.
(c) A component in $\Gamma_4$ contains 1 split and is incident to 1 bridge $(u,v) \in \Gamma_{4,2}$ where $v$ is in a non-plain component in $\Gamma_2$ that contains a split.

Fig 5: Examples of backbone graphs violating (P6) and the corresponding orbit graphs.

Properties (P1)–(P7) are justified by the following arguments:

• Paralleling conditions (T1) and (T2) for the forest constraint, (P1) and (P2) follows from the classification of edge orbits and orbit graphs in Section 5.1;
• Suppose (P3) does not hold. Since the excess of the corresponding orbit graph of a plain unicyclic component in $\Gamma_m$ is 0, by (O1) and (O2), there exists a unicyclic component component $C$ in $\Gamma_m$ such that $ex(H_C) > 0$, contradicting $H$ being a pseudo-forest;
• Suppose (P4) does not hold. Then by (O1) and Lemma 3, there exists a tree component component $C$ in $\Gamma_m$ such that $ex(H_C) > 0$, contradicting $H$ being a pseudo-forest;
• Suppose (P5) does not hold. Then by (O2) and Lemma 3, there exists a tree component component $C$ in $\Gamma_m$ such that $ex(H_C) > 0$, contradicting $H$ being a pseudo-forest;
• To prove (P6), let $G_1$ denote the orbit graph of $C(u)$ consisting of edge orbits (including splits, matchings, and cycles). Let $G_2$ denote the orbit graph of $C(v)$ consisting of edge orbits (including splits, matchings, and cycles) in $C(v)$, as well as bridges in $\cup_{\ell < m/2 \Gamma_{m/2,\ell}}$ that are incident to $C(v)$. Let $G_{new}$ denote the edge-disjoint union of $G_1$, $G_2$, and the edge orbit corresponding to the bridge $(u,v)$. Since $C(u)$ contains a split, by (O1) and Lemma 3, $ex(G_1) \geq -m/2$. Then we have

$$ex(G_{new}) = ex(G_1) + ex(G_2) + m \geq ex(G_2) + m/2 \geq 0,$$
where the last inequality is met with equality if and only if $C(v)$ is a plain tree component in $\Gamma_{m/2}$ by Lemma 3. Hence, (P6) follows.

- To prove (P7), let $C = C(u) \cup C(u')$. Let $G_1$ denote the orbit graph of $C$ consisting of edge orbits (including splits, matchings, and cycles), as well as bridges in $\cup_{\ell \leq m} \Gamma_{m, \ell}$ except for $(u,v)$ and $(u',v')$ that are incident to $C$. If $C(u) = C(u')$, then $\text{ex}(G_1) \geq -m$ by Lemma 3. If $C(u) \neq C(u')$, then $G_1$ is an edge-disjoint union of $H_1$ and $H_1'$, where $H_1$ (resp. $H_1'$) is the orbit graph of $C(u)$ (resp. $C(u')$) consisting of edge orbits (including splits, matchings, and cycles) in $C(u)$ (resp. $C(u')$), as well as bridges in $\cup_{\ell < m} \Gamma_{m, \ell}$ except for $(u,v)$ (resp. $(u',v')$) that are incident to $C(u)$ (resp. $C(u')$). By assumption, together with (O1), (O2) and Lemma 3, $\text{ex}(H_1) \geq -m/2$ and $\text{ex}(H_1') \geq -m/2$ and thus $\text{ex}(G_1) \geq \text{ex}(H_1) + \text{ex}(H_1') \geq -m$.

Let $C' = C(v) \cup C(v')$. Note that by (P5) and (P6), both $C(v)$ and $C(v')$ are components in $\Gamma_{m/2}$. Let $G_2$ denote the orbit graph of $C'$ consisting of edge orbits (including splits, matchings, and cycles) in $C'$, as well as bridges in $\cup_{\ell < m/2} \Gamma_{m/2, \ell}$ that are incident to $C'$. Let $G_{\text{new}}$ denote the edge-disjoint union of $G_1$, $G_2$, and the edge orbits corresponding to the two bridges $(u,v)$ and $(u',v')$. Then,

$$\text{ex}(G_{\text{new}}) \geq \text{ex}(G_1) + \text{ex}(G_2) + 2m \geq -m + \text{ex}(G_2) + 2m = \text{ex}(G_2) + m.$$ 

By assumption, $G_{\text{new}}$ is a pseudo-forest and thus $\text{ex}(G_{\text{new}}) \leq 0$. It follows that $\text{ex}(G_2) \leq -m$ and hence $v$ and $v'$ must be in distinct plain tree components in $\Gamma_{m/2}$ by Lemma 3.

The implication of (P4)-(P7) is the following. For each $m \in [k]$, define

$$\mathcal{E}(m) \triangleq \cup_{\ell < m} E(\Gamma_{m, \ell})$$

consisting of all bridges between $m$-node orbits and shorter orbits. Then $\mathcal{E}(m)$ can be divided into two sets of bridges as follows. For each $u \in S_m$, recall that $C(u)$ denotes the connected
component in \( \Gamma_m \) containing \( u \). A bridge is denoted by a giant edge \((u, v) \in \Gamma_{m, \ell} \) with \( \ell < m \), where \( u \in S_m \) in the longer orbit is called the \emph{starting point} and \( v \in S_\ell \) in the shorter orbit is called the \emph{ending point}. Define

\[
\mathcal{E}_{\text{single}}(m) \triangleq \{(u, v) \in E(\Gamma) : u \in S_m, v \in \cup_{\ell<m} S_\ell, C(u) \text{ contains no split and is not incident to any bridge in } \cup_{\ell<m} \Gamma_{m, \ell} \text{ other than } (u, v)\}
\]

(79)

\[
\mathcal{E}_{\text{double}}(m) \triangleq \{(u, v) \in E(\Gamma) : u \in S_m, v \in S_{m/2}, C(u) \text{ contains a split or is incident to some bridge in } \cup_{\ell<m} \Gamma_{m, \ell} \text{ other than } (u, v)\}
\]

(80)

By Properties (P6)–(P7), we have \( \mathcal{E}(m) = \mathcal{E}_{\text{single}}(m) \cup \mathcal{E}_{\text{double}}(m) \). Moreover,

- For each \((u, v), (u', v') \in \mathcal{E}_{\text{single}}(m)\), the starting points \( u \) and \( u' \) belong to separate tree components in \( \Gamma_m \), i.e., \( C(u) \) and \( C(u') \) are distinct tree components in \( \Gamma_m \). Furthermore, \( C(u) \) (resp. \( C(u') \)) contains no split and is not incident to any bridge other than \((u, v)\) (resp. \((u', v')\)). (This is just repeating definition).
- For each \((u, v), (u', v') \in \mathcal{E}_{\text{double}}(m)\), the ending points \( v \) and \( v' \) belong to separate plain tree components in \( \Gamma_{m/2} \), by (P7).

The above observation suggests that to specify the bridges in \( \mathcal{E}_{\text{single}}(m) \), one can use the \emph{forward construction} by first choosing their starting points from separate components of \( \Gamma_m \) then choosing the ending points from shorter orbits \( \cup_{\ell<m} S_\ell \) in an unconstrained way; to specify the bridges in \( \mathcal{E}_{\text{double}}(m) \), one can use the \emph{backward construction} by first choosing their ending points from separate components of \( \Gamma_{m/2} \) then choosing the starting points from \( S_m \) in an unconstrained way. This separate account of bridges is useful in the enumeration scheme which we describe next.

Next, we describe an algorithm for generating all possible backbone graphs \( \Gamma \) that satisfy the properties (P1)–(P7). Given a sequence of integers \((a, b, c, d) = (a_1, b_1, c_1, d_1)_{1 \leq t \leq k} \) with \( b_t = 0 \) for odd \( t \) and \( d_t = 0 \) if \( 2t > k \), we construct \( \Gamma \) as follows:

\begin{algorithm}
1: for each \( t = 1, \ldots, k \) do
2: \hspace{1em} \textbf{Step 1: Matching stage.} Construct a rooted pseudoforest \( \Gamma_t \) with \( n_t \) giant nodes and \( a_t \) giant edges (allowing self-loops and multiple edges). Attach a label from \([t]\) to each giant edge and a label from \( \left[ \frac{t-1}{2} \right] \) to each self-loop;
3: \hspace{1em} \textbf{Step 2: Splitting stage.} Choose \( b_t \) components from \( n_t - a_t \) tree components of \( \Gamma_t \), and within each chosen component, choose a node: if the node chosen is the same as the root, add a split to the root; otherwise, add two splits, one at the root and the other one at the chosen node;
4: \hspace{1em} \textbf{Step 3: Forward bridging stage.} Choose \( c_t \) out of the remaining \( n_t - a_t - b_t \) tree components of \( \Gamma_t \), and for each chosen component, add a bridge connecting its root to a giant node in \( \Gamma_\ell \) for some \( \ell < t \) that is a divisor of \( t \). Attach a label from \([t]\) to the added bridge.
5: \hspace{1em} \textbf{Step 4: Backward bridging stage.} Choose \( d_t \) from the remaining \( n_t - a_t - b_t - c_t \) tree components of \( \Gamma_t \). For each chosen component, add a bridge by connecting its root to a giant node in \( \Gamma_{2t} \). Attach a label from \([t]\) to the added bridge.
6: end for
\end{algorithm}

We note that an output graph of Algorithm 2 is not necessarily a pseudoforest; nevertheless any orbit pseudoforest can be generated by Algorithm 2, which is what we need for upper bounding the generating function of orbit pseudoforests, \( \sum_{H \in \mathcal{H}_t} s^{2e(H)} \). To verify this claim formally, let \( \bar{H} \) be an orbit pseudoforest and let \( \Gamma \) denote its backbone graph as in Definition 2, where for \( 1 \leq m \leq k \) there are:
• $a_m$ giant edges (including self-loops) corresponding to either Type $M_m$ or $C_m$ edge orbits;
• $b_m$ components that contain splits corresponding to Type $S_m$ edge orbits;
• $c_m$ giant edges corresponding to Type $B_{m,\ell}$ edge orbits for some $\ell < m$ that is a divisor of $m$;
• $d_m$ giant edges corresponding to Type $B_{m,2m}$ edge orbits.

For each $\Gamma_m$ where $1 \leq m \leq k$, we arbitrarily choose the root for each plain tree component, and specify the root in each non-plain tree component as the giant node that either splits or is incident to a bridge in $E_{\text{single}}(m) \cup E_{\text{double}}(2m)$ (when there are two giant nodes that split in a tree component, we choose any one of them as the root; otherwise, the choice of the root is unique). Then it is clear that Steps 1 and 2 can realize any configuration of splits and matchings in $\Gamma$, thanks to Properties (P1)–(P4). Finally, note that bridges in $E_{\text{single}}(m)$ are added by Step 3 (forward bridging) at iteration $t = m$ with $c_m = |E_{\text{single}}(m)|$, and bridges in $E_{\text{double}}(m)$ are added by Step 4 (backward bridging) at iteration $t = m/2$ with $d_{m/2} = |E_{\text{double}}(m)|$.

Next we bound the generating function $\sum_{H \in \mathcal{H}_k} s^{2e(H)}$ from above. We first state an auxiliary lemma, which extends the well-known formula (74) for enumerating rooted forests.

**Lemma 4.** The number of rooted pseudoforests on $n$ nodes with $a$ edges (allowing self-loops and multiple edges) is at most

\[
\binom{n}{a} (2n)^a.
\]

**Proof.** To see this, let $m$ denote the number of cycles (including self-loops and parallel edges). Then the number of connected components is $n - a + m$. To enumerate all such rooted pseudoforests, we first enumerate all rooted forests on $n$ vertices with $a - m$ edges, then choose $m$ roots out of $n - a + m$ roots, and finally add one edge to each chosen root to form a cycle within its corresponding component. Each added edge can either be a self-loop at the root or connect the root to some other node, so there are at most $n$ different choices of the added edge. Therefore, the total number of rooted pseudoforests on $n$ vertices with $a$ edges is at most

\[
\sum_{m=0}^{a} \binom{n}{a-m} \binom{n-a+m}{m} n^m = n^a \sum_{m=0}^{a} \binom{n}{a-m} \binom{n-a+m}{m} = \binom{n}{a} (2n)^a.
\]

Now, we can enumerate all possible output backbone graphs $\Gamma$ of Algorithm 2 as follows.

For $t = 1, \ldots, k$,

1. Note that $\Gamma_t$ constructed in Step 1 is a rooted pseudoforest with $n_t$ giant nodes and $a_t$ giant edges. Moreover, each giant edge added in Step 1 carries at most $t$ possible labels. Hence, the total number of all possible rooted pseudoforests $\Gamma_t$ constructed in Step 1 is at most:

\[
\binom{n_t}{a_t} (2tn_t)^{a_t}.
\]

2. The total number of different ways of splitting is at most

\[
\binom{n_t - a_t}{b_t} n_t^{b_t}.
\]
3. The total number of different ways of forward bridging is at most:

\[(n_t - a_t - b_t) \left( \sum_{\ell < t} \ell n_\ell \right)^{c_t}. \]  

4. The total number of different ways of backward bridging is at most:

\[(n_t - a_t - b_t - c_t) \left( t n_{2t} \right)^{d_t}. \]  

Combining (82), (83), (84), and (85), we conclude that the total number of possible output backbone graphs $\Gamma$ with input parameter $(a, b, c, d)$ is at most

\[\prod_{t=1}^{k} \left( 1_{\{b_t = 0 \text{ for odd } t\}} \sum_{\ell < t} \ell n_\ell \right)^{c_t} \left( t n_{2t} \right)^{d_t}. \]

Note that for each output backbone graph, the total number of edges in the corresponding orbit graph $H$ satisfies

\[e(H) \geq \sum_{t=1}^{k} t \left( a_t + b_t/2 + c_t + 2d_t \right). \]

Combining the above two displays, we obtain

\[\sum_{H \in H_k} s^{2e(H)} \leq \sum_{a,b,c,d} \prod_{t=1}^{k} \left( 1_{\{b_t = 0 \text{ for odd } t\}} \sum_{\ell < t} \ell n_\ell \right)^{c_t} \left( t n_{2t} \right)^{d_t} \times 2^{s(t_n + t_b + 2t_c + 4t_d - 1)}. \]

6. Conclusion and Open Questions. In this paper, we formulate the general problem of testing network correlation and characterize the statistical detection limit. For both Gaussian-weighted complete graphs and dense Erdős-Rényi graphs, we determine the sharp threshold at which the asymptotic optimal testing error probability jumps from 0 to 1. For sparse Erdős-Rényi graphs, we determine the threshold within a constant factor. The proof of the impossibility results relies on a delicate application of the truncated second moment method, and in particular, leverages the pseudoforest structure of subcritical Erdős-Rényi graphs in the sparse setting. We conclude the paper with a few important open questions.

1. In a companion paper [31], we show that a polynomial-time test based on counting trees achieves strong detection when the average degree $np \geq n^{-o(1)}$ and the correlation $\rho \geq c$ for an explicit constant $c$. In particular, this result combined with our negative results in Theorem 2 imply that the detection limit is attainable in polynomial-time up to a constant factor in the sparse regime when $np = \Theta(1)$. However, achieving the optimal detection threshold in polynomial time remains largely open.
2. It is of interest to study the detection limit under general weight distributions. Our proof

techniques are likely to work beyond the Gaussian Wigner and Erdős-Rényi graphs model.

For example, for general distributions $P$ and $Q$, as shown in the proof of Proposition 1,
the second moment is determined by the eigenvalues of the kernel operator defined by
the likelihood ratio $L(x, y) = \frac{P(x, y)}{Q(x, y)}$. Another interesting direction is testing correlations
between hypergraphs.

3. Another important open problem is to determine the sharp threshold for detection in the
sparse Erdős-Rényi graphs with $p = n^{-\Omega(1)}$. In particular, to improve our positive result,
one may need to analyze a more powerful test statistic beyond QAP. For the negative di-
rection, one needs to consider the case where the intersection graph $A \land B^\pi$ is supercritical
and a more sophisticated conditioning beyond the pseudoforest structure may be required.

Acknowledgment. The authors thank Cristopher Moore for simplifying the proof of
Proposition 1. J. Xu would like to thank Tselil Schramm for helpful discussions on the hy-
pothesis testing problem at the early stage of the project.

Y. Wu is supported in part by the NSF Grant CCF-1527105, an NSF CAREER award
CCF-1651588, and an Alfred Sloan fellowship.

J. Xu is supported by the NSF Grants CCF-1850743, CCF-1856424, and IIS-1932630.

S. H. Yu is supported by the NSF Grant CCF-1856424.

REFERENCES


ability 1567–1591.


for the Graph Matching Problem on Correlated Random Graphs. In Advances in Neural Information
Processing Systems 9186–9194.

network alignment. ACM Transactions on Knowledge Discovery from Data (TKDD) 7 1–31.

tortion correspondences. In 2005 IEEE computer society conference on computer vision and pattern
recognition (CVPR’05) I 26–33. IEEE.


Graph Alignment via k-Core Alignment. Proceedings of the ACM on Measurement and Analysis of
Computing Systems 3 1–21.

beling algorithm for the alignment of correlated Erdos-Renyi graphs. Proceedings of the ACM on

**SUPPLEMENTARY MATERIAL**

*Supplementary material for “TESTING CORRELATION OF UNLABELED RANDOM GRAPHS”*

(; .pdf). The supplementary collects several technical proofs postponed due to space constraints and auxiliary facts on concentration inequalities and random permutations.