The Edge Density Barrier: Computational-Statistical Tradeoffs in Combinatorial Inference

Appendix

A Other Cases of the Lower Bound Results

In this section, we will list various computational lower bound results in detail. First, in §A.1 and §A.2 we formalize the computational lower bound results for clique, nearest neighbor graph and 3-clique versus s-clique problems as corollaries of Theorem 7. Then in §A.3 we give another general computational lower bound theorem which requires slightly weaker assumptions and use it to obtain results for perfectly matched block problem. At last, in §A.4 we give more details for the hypercube detection problem and use it as an example to demonstrate that our technique can show the optimal polynomial query complexities for certain testing problems.

A.1 Clique and Nearest Neighbor Graph Detection

While the information-theoretic lower bounds in Table 1 follows directly from Theorem 4.2 in [2], the computational lower bounds are corollaries of Theorem 7. We list the computational lower bound results here for the sake of completeness.

Corollary A.1 (Computational Lower Bound for Clique Detection)**.** Define

$$\mathcal{C}_0 = \{\mathrm{I}_d\},\ \mathcal{C}_1 = \{\Theta : \exists \mathcal{S} \subset [d] \text{ and } |\mathcal{S}| = s, \theta_{j,k} = \mathbb{1}(j = k) + \theta \cdot \mathbb{1}(j, k \in \mathcal{S}, j \neq k)\}. \tag{A.1}$$

Let η be a positive constant. If $s = O(d^\alpha)$ for some $\alpha \in (0, 1/2)$, and

$$\theta \le \kappa \frac{1}{\sqrt{n}} \wedge \frac{1}{8s},$$

where κ is a small enough constant that only depends on α and η, then when testing empty graph against s-cliques, for all algorithms that queries $T \le d^\eta$ rounds, there exists an oracle r such that

$$\liminf_{n\to\infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1.$$

Proof. See §B.3 for a detailed proof. $\square$

Corollary A.2 (Computational Lower Bound for Nearest Neighbor Graph Detection)**.** For a vertex set $\mathcal{S} = \{v_1, \ldots, v_s\} \subseteq \{1, \ldots, d\}$, we denote

$$\mathcal{P}(\mathcal{S}) = \{(p_1, \ldots, p_s) : (p_1, \ldots, p_s) \text{ is a permutation of } (v_1 \ldots, v_s)\}$$

to be the set of permutations of vertices in $\mathcal{S}$. For $p = (p_1, \ldots, p_s) \in \mathcal{P}(\mathcal{S})$, we define the $s/2$-nearest neighbor edge set as

$$E_{\text{nearest}}(p) = \big\{(p_i, p_j) : 1 \le i, j \le s,\ i \neq j,\ \exists r, -s/4 \le r \le s/4,\ j \equiv i + r \pmod{s}\big\}.$$

Let $A_{\text{nearest}}(p)$ be the adjacency matrix of $(V, E_{\text{nearest}}(p))$. Then in the $s/2$-nearest loop detection problem, $\mathcal{C}_0 = \{\mathrm{I}_d\}$ and $\mathcal{C}_1$ is defined as

$$\mathcal{C}_1 = \big\{\mathrm{I}_d + \theta A_{\text{nearest}}(p) : \mathcal{S} \subset [d],\ |\mathcal{S}| = s,\ p \in \mathcal{P}(\mathcal{S})\big\}. \tag{A.2}$$

Let η be a positive constant. If $s = O(d^\alpha)$ for some $\alpha \in (0, 1/2)$, and

$$\theta \le \kappa \frac{1}{\sqrt{n}} \wedge \frac{1}{16s},$$

where κ is a small enough constant that only depends on α and η, then when testing empty graph against $s/2$-nearest neighbor graphs, for all algorithms that queries $T \le d^\eta$ rounds, there exists an oracle r such that

$$\liminf_{n\to\infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1.$$

Proof. See §B.3 for a detailed proof. □

A.2 Testing s-clique against 3-clique

Our general lower bound result in Theorem 7 works for general hypothesis testing problems of the form (2). In this section, we consider testing s-clique against 3-clique problem. We denote by G_J the graph where vertex i and vertex j are connected if and only if $i, j \in J$. Then for the 3-clique versus s-clique problem, we have $\mathcal{G}_0 = \{G_J : |J| = 3 \text{ and } J \subseteq V\}$ and $\mathcal{G}_1 = \{G_J : |J| = s \text{ and } J \subseteq V\}, s \ge 3$. Since in this case $\mathcal{G}_0 \ne \{(V, \emptyset)\}$, this test is different from the previous examples we present. Applying Theorem 7 gives the following lower bound result.

Corollary A.3 (computational lower bound for 3-clique versus s-clique problem)**.** Define

$$\mathcal{C}_0 = \{\Theta : \exists \mathcal{S} \subset [d] \text{ and } |\mathcal{S}| = 3, \theta_{j,k} = \mathbb{1}(j = k) + \theta \cdot \mathbb{1}(j, k \in \mathcal{S}, j \ne k)\},$$
$$\mathcal{C}_1 = \{\Theta : \exists \mathcal{S} \subset [d] \text{ and } |\mathcal{S}| = s, \theta_{j,k} = \mathbb{1}(j = k) + \theta \cdot \mathbb{1}(j, k \in \mathcal{S}, j \ne k)\}.$$

Let η be a positive constant. If $s = O(d^\alpha)$ for some $\alpha \in (0, 1/2)$, and

$$\theta \le \kappa \frac{1}{\sqrt{n}} \wedge \frac{1}{16\sqrt{2s}},$$

where κ is a small enough constant that only depends on α and η, then when testing 3-clique versus s-clique, for all algorithms that queries $T \le d^\eta$ rounds, there exists an oracle r such that

$$\liminf_{n\to\infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1.$$

Proof of Corollary A.3. Let G_0 be the graph whose edges form a triangle on the first three vertices. Clearly, $\mathcal{E} = \{E[G(\Theta)] \backslash \{(1,2),(1,3),(2,3)\} : \Theta \in \mathcal{C}_1\}$ is a null-alternative separator. By Definition 5, setting $S' = S$ gives

$$\mu \ge \frac{|S|}{|V(S)|^2} = \frac{|V(S)| \cdot (|V(S)| - 1)/2 - 3}{|V(S)|^2} = \frac{1}{2} - \frac{1}{2s} - \frac{3}{s^2} \ge \frac{1}{8},$$

where we use $s \ge 4$ in the last inequality. Moreover, by Lemma B.4, we have $\mu \le 1/2$. Therefore μ is of constant order. For $j = 0, \ldots, k$, define $m_j = |\{S' \in \mathcal{E} : \max_{S \in \mathcal{E}} \gamma(S, S') = k - j\}|$. Then

$$\frac{m_{j+1}}{m_j} = \left[\binom{s}{s-j-1}\binom{d-s}{j+1}\right] \bigg/ \left[\binom{s}{s-j}\binom{d-s}{j}\right] \ge \frac{d}{s^2}.$$

Taking infimum over j gives $\zeta \ge d/s^2 \ge Cd^{1-2\alpha}$ for some absolute constant C. Therefore we have

$$\theta \le \kappa \frac{1}{\sqrt{n}} \le \frac{2\kappa}{1-2\alpha} \frac{\log \zeta}{\log d + \log \zeta} \frac{1}{\sqrt{n}}.$$

Since we have $\liminf_{n\to\infty} \zeta \ge \liminf_{n\to\infty} d^{1-2\alpha} = \infty$, picking κ to be small enough allows us to apply Theorem 7. This completes the proof. □

A.3 A Computational Lower Bound under Weaker Assumptions

In this section we give a slightly more general version of Theorem 7 that can be applied to the perfectly matched block problem defined in §2.1. We begin with generalizing the definition of vertex cut ratio. We remind the reader that in the following definition, $\gamma(S, S')$ is the constrained vertex cut number of edge sets S and S' defined in (11).

Definition A.4 (Partial Vertex Cut Ratio). Let $k = \max_{S,S' \in \mathcal{E}} \gamma(S, S')$. For $r \in \{0, \ldots, k-1\}$ we define the r-partial vertex cut ratio as

$$\zeta_r = \inf_{0 \le j \le r} \frac{|\{S' \in \mathcal{E} : \max_{S \in \mathcal{E}} \gamma(S, S') = k - j\}|}{|\{S' \in \mathcal{E} : \max_{S \in \mathcal{E}} \gamma(S, S') = k - j + 1\}|}. \tag{A.3}$$

Clearly, the vertex cut ratio defined in Definition 6 is also the $(k-1)$-partial vertex cut ratio of the null-alternative separator, and we have $\zeta = \zeta_{k-1} \le \zeta_{k-2} \le \cdots \le \zeta_0$. Therefore replacing the assumption $\liminf_{d \to \infty} \zeta > 1$ with $\liminf_{d \to \infty} \zeta_r > 1$ for some $r < k$ makes the assumption weaker and gives a more general lower bound result.

Theorem A.5. Suppose that we have a null-alternative separator $\mathcal{C}$ with null base G_0 and edge density μ (defined in Definition 5). Let $\eta > 0$, $c > 1$ be constants, $\overline{c} = \sqrt{c}/(\sqrt{c}-1)$, $k = \max_{S,S' \in \mathcal{C}} \gamma(S, S')$ and $r = [k+3-(16\overline{c}^3 \mu n \theta^2)^{-1/2}] \vee 3$. Let ζ_r be the r-partial vertex cut ratio (defined in Definition A.4). Assume that $\liminf_{d \to \infty} \zeta_r \ge c$. If

$$\theta \le \frac{\kappa \log \zeta_r}{\log d + \log \zeta_r} \sqrt{\frac{1}{\mu n}} \wedge \frac{\sqrt{\mu}}{8s} \wedge \frac{1}{2k\sqrt{\mu}}, \tag{A.4}$$

where κ is a small enough constant that only depends on η and c, then any hypothesis test algorithm under oracle computational model that queries $T \le d^\eta$ rounds is asymptotically powerless.

Proof. See §B.3 for a detailed proof. □

With Theorem A.5, we can prove the computational lower bound for perfectly matched block detection problems defined in §2.1.

Corollary A.6. Let η be a positive constant. If

$$\theta \le \kappa \frac{1}{\sqrt{n} \log d} \wedge \frac{1}{8\sqrt{d}},$$

where κ is a small enough constant that only depends on η, then when testing empty graph against perfectly matched block defined in §2.1, for all algorithms that queries $T \le d^\eta$ rounds, there exists an oracle r such that

$$\liminf_{n \to \infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1.$$

Proof. See §B.3 for a detailed proof. □

As is mentioned in Theorem 9, since a perfectly matched block is also a clique, the testing algorithms for clique detection works for perfectly matched block problem as well, and therefore the lower bound given by Corollary A.6 is sharp up to a logarithm factor. We also remark that since the inverse of a clique covariance matrix can be directly calculated as is shown in Lemma B.6, the information-theoretic lower bound in Table 1 follows from [1].

A.4 Hypercube Detection and Necessary Computational Complexity

In this section we consider the hypercube detection problem. In hypercube detection problem, the d coordinates in X corresponds to d points in a D-dimensional lattice, where D is a constant integer that does not scale with n, s and d. Without loss of generality, we assume that $d' = d^{1/D}$, $s' = s^{1/D}$ and $p = d'/s'$ are integers. Then a D-dimensional vector $a = (a_1, \ldots, a_D) \in \{1, \ldots, d'\}^D$ uniquely determines $i \in \{1, \ldots, d\}$ with the map

$$i = i(a) = a_1 + (a_2 - 1)d' + (a_3 - 1)d'^2 + \cdots + (a_D - 1)d'^{D-1}.$$

We consider d/s disjoint hypercubes with side length s'. The location of these hypercubes can be determined by the D-dimensional vector $b = (b_1, \dots, b_D) \in \{1, \dots, p\}^D$. More specifically, the vertex set of the $(b_1, \dots, b_D)$-th hypercube is

$$V_{b_1,\dots,b_D} = \{a = (a_1, \dots, a_D) : s'(b_j - 1) + 1 \le a_j \le s'b_j,\ j = 1, \dots, D\}, \tag{A.5}$$

and the lattice graph is obtained by connecting every two adjacent vertices in $V_{b_1,\dots,b_D}$. Denote by $\mathrm{A}_{b_1,\dots,b_D} \in \mathbb{R}^{d\times d}$ the adjacency matrix of this lattice graph. Then in the hypercube detection problem, $\mathcal{C}_0 = \{\mathrm{I}_d\}$ and

$$\mathcal{C}_1 = \big\{\mathrm{I}_d + \theta \mathrm{A}_{b_1,\dots,b_D} : (b_1, \dots, b_D) \in \{1, \dots, p\}^D\big\}. \tag{A.6}$$

Note that distinct graphs under alternative have no edge intersection, and the null-alternative separator only contains d/s different edge sets, which implies that the computation cost should be low. This matches the results in Theorem 8. For consistency, we first restate Theorem 8.

Theorem A.7. If there exists a constant κ such that $\theta \le \kappa/(\sqrt{sn})$, then when testing empty graph against lattice graphs with fixed lattice dimension D, for all algorithms that queries $T = o(d/s)$ rounds, there exists an oracle r such that

$$\liminf_{n\to\infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1.$$

Proof. See §B.3 for a detailed proof. □

Theorem A.8. Assume $\theta \le 1/(2D)$. For $b = (b_1, \dots, b_D) \in \{1, \dots, p\}^D$, let V_b be the vertex set defined in (A.5) and E_b be the corresponding edge set of the hypercube graph. We consider the queries

$$q_b(X) = \frac{1}{|E_b|} \sum_{(i,j)\in E_b} X_i X_j.$$

If

$$\theta \ge \kappa \sqrt{\frac{\log(d/s)}{ns}}$$

for some large enough constant κ, then for the test $\psi = \mathbb{1}\left[\sup_{b\in\{1,\dots,p\}^D} Z_{q_b(X)} \le -\frac{\theta}{4}\right]$ and any feasible oracle r and n, we have

$$\liminf_{n\to\infty} \left[\sup_{\Theta\in\mathcal{C}_0} \mathbb{P}_\Theta(\psi = 1) + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta(\psi = 0)\right] = 0.$$

Proof. See §B.3 for a detailed proof. □

Theorem A.7 and Theorem A.8 together show a new type of result that is different from our previous examples: there exists an asymptotically powerful algorithm with computational complexity $T = d/s$. However all algorithms with computational complexity $T = o(d/s)$ are asymptotically powerless.

B Proofs of the Main Results

In this section, we first establish the computational lower bounds for combinatorial inference problems. Then provide the proofs of upper bounds.

B.1 Proofs of Lower Bounds

In the sequel, we provide the proofs of lower bounds.

B.1.1 Proof of Theorem 7

Given $G_0 = (V, E_0) \in \mathcal{G}_0$ and $S \in \mathcal{E}$, where $\mathcal{E}$ is a null-alternative separator with null base G_0 defined in 4. Recall that Θ_0 and Θ_S are defined as

$$\Theta_0 = \mathrm{I} + \theta \mathrm{A}_0, \;\; \Theta_S = \mathrm{I} + \theta(\mathrm{A}_0 + \mathrm{A}_S),$$

where A_0 and A_S are the adjacency matrices of G_0 and $G_S = (V, S)$ respectively. We have

$$R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) \geq R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{E}\}, \mathscr{A}, r). \tag{B.1}$$

We next give lower bound for $R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{E}\}, \mathscr{A}, r)$. Intuitively, for any $S \in \mathcal{E}$, in order to succeed with the worst-case oracle, a test has to utilize at least one query q that can distinguish Θ_S from Θ_0. We define

$$\mathcal{C}(q) = \{S \in \mathcal{E} : |\mathbb{E}_S q(X) - \mathbb{E}_0 q(X)| \geq \|q(X)\|_{\psi_1,0} \cdot \tau\},$$

where $\|q(X)\|_{\psi_1,0}$ is the ψ_1-norm of $q(X)$ when X follows distribution $\mathbb{P}_0$, and τ is defined in Definition 3. By the definition of $\mathcal{C}(q)$, if $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{E}|$, then there must be some $S' \in \mathcal{E}$ such that none of the T queries used by the test can distinguish $\Theta_{S'}$ from Θ_0. Therefore the worst case oracle that returns $\mathbb{E}_{S'} q(X)$ when $X \sim \mathbb{P}_0$ can still satisfy the definition 3 but will make all the tests fail for sure. This gives the following lemma.

Lemma B.1. For any algorithm $\mathscr{A}$ that queries the oracle at most T rounds, if $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{E}|$, then there exists an oracle r defined in Definition 3 such that $R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{E}\}, \mathscr{A}, r) \geq 1$.

Proof. See §C for a detailed proof. □

By (B.1) and Lemma B.1, to prove $\liminf_{n\to\infty} R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) = 1$, it suffices to show that $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|/|\mathcal{E}|$ is asymptotically smaller than one. In the rest of the proof, for any $q \in \mathcal{Q}_{\mathscr{A}}$, we derive an upper bound on $|\mathcal{C}(q)|$. To do so, we first split $\mathcal{C}(q)$ into two subsets $\mathcal{C}^+(q)$ and $\mathcal{C}^-(q)$, which are given by

$$\mathcal{C}^+(q) = \{S \in \mathcal{E} : \mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)] > \|q(X)\|_{\psi_1,0} \cdot \tau\}, \tag{B.2}$$

$$\mathcal{C}^-(q) = \{S \in \mathcal{E} : \mathbb{E}_0[q(X)] - \mathbb{E}_S[q(X)] > \|q(X)\|_{\psi_1,0} \cdot \tau\}. \tag{B.3}$$

We now bound $|\mathcal{C}^+(q)|$. $|\mathcal{C}^-(q)|$ can be bounded in exactly the same way. The following lemma summarizes an inequality derived from the definition (B.2).

Lemma B.2. For any query function q, we have

$$\frac{1}{|\mathcal{C}^+(q)|^2} \sum_{S, S' \in \mathcal{C}^+(q)} \mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0} \frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] > 1 + \frac{1}{n}. \tag{B.4}$$

Proof. See §C for a detailed proof. □

It remains to calculate the left-hand side of (B.4). Plugging in the definition of Gaussian density gives

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0} \frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] = \left[\frac{\det(\Theta_S)}{\det(\Theta_0)} \frac{\det(\Theta_{S'})}{\det(\Theta_0)}\right]^{1/2} \mathbb{E}_0\Big\{\exp\big[-X^T\theta(\mathrm{A}_S + \mathrm{A}_{S'})X\big]/2\Big\}.$$

Therefore, if we define $\Theta_{S,S'} = \Theta_0 + \theta \mathrm{A}_S + \theta \mathrm{A}_{S'}$, the equation above reduces to

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0} \frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] = \left[\frac{\det(\Theta_S)}{\det(\Theta_0)} \frac{\det(\Theta_{S'})}{\det(\Theta_{S,S'})}\right]^{1/2}. \tag{B.5}$$

The right hand side of (B.5) can be written as

$$\left[\frac{\det(\Theta_S)}{\det(\Theta_0)} \frac{\det(\Theta_{S'})}{\det(\Theta_{S,S'})}\right]^{1/2} = \exp\left\{\sum_{j=1}^{\infty} \frac{(-\theta)^j}{2j} \mathrm{Tr}\left[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0 + \mathrm{A}_S)^j - (\mathrm{A}_0 + \mathrm{A}_{S'})^j\right]\right\}, \tag{B.6}$$

where $\mathrm{A}_{S,S'} = \mathrm{A}_0 + \mathrm{A}_S + \mathrm{A}_{S'}$. We introduce two lemmas summarized from [2] to further bound (B.6). The key observation is that for an adjacency matrix M, $\mathrm{Tr}(\mathrm{M}^k)$ represents the number of length-k closed walks on the corresponding graph.

Lemma B.3. For any $j \geq 1$, we have

$$\mathrm{Tr}\left[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0 + \mathrm{A}_S)^j - (\mathrm{A}_0 + \mathrm{A}_{S'})^j\right] \geq 0.$$

Lemma B.3 essentially shows that in the right hand side of (B.6), all terms for odd k can be ignored. To bound the rest terms, we notice that $\mathrm{Tr}[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0 + \mathrm{A}_S)^j - (\mathrm{A}_0 + \mathrm{A}_{S'})^j]$ actually counts the number of length-k closed walks that contain an edge from the set S and another edge from the set S'.

We have the following lemma that shows the relation between constrained vertex cut number and null-alternative separator edge density.

Lemma B.4. For $S, S' \in \mathcal{E}$, we have $|S \cap S'| \leq \mu\gamma^2(S, S') \leq \gamma^2(S, S')/2$.

Proof. For vertex set $\widetilde{V} \subseteq V(S \cup S')$ which is a vertex cut for $V(S)\backslash\widetilde{V}$ and $V(S')\backslash\widetilde{V}$, by the definition of vertex cut, all vertices in $V(S) \cap V(S')$ must be contained in $\widetilde{V}$, because otherwise $V(S)\backslash\widetilde{V}$ and $V(S')\backslash\widetilde{V}$ will share a vertex. Therefore $|\widetilde{V}| \geq |V(S) \cap V(S')| \geq |V(S \cap S')|$. Taking minimum over all vertex cuts gives $\gamma(S, S') \geq |V(S \cap S')|$. Plugging this into the definition of μ gives the first inequality. For the second inequality, note that $S \cap S'$ can have at most $\binom{|V(S\cap S')|}{2} \leq \frac{|V(S\cap S')|^2}{2}$ edges. So we always have $\mu \leq 1/2$, and the second inequality holds. ☐

Lemma B.4 gives an important observation that for arbitrary test problems and arbitrary null-alternative separators, μ is always bounded by a constant. The weak edge density μ is a counterpart of the strong edge density μ' defined by [2] as follows,

$$\mu' := \max_{S,S'\in\mathcal{E}, |V(S\cap S')|\neq 0} \frac{|S \cap S'|}{|V(S \cap S')|}.$$

For a null-alternative separator $\mathcal{E}$, when calculating μ and μ', we need to search for S and S' in $\mathcal{E}$ that maximize $|S \cap S'|/|V(S \cap S')|^2$ and $|S \cap S'|/|V(S \cap S')|$. Intuitively, for local edge density μ, the maximal order can be achieved by S and S' that only have a few edge intersections. On the other hand, the maximal of μ' is usually obtained with S and S' that have a large number of edge overlaps.

Lemma B.5. For S and S' in $\mathcal{C}(q)$, we have

$$\mathrm{Tr}\left[\mathrm{A}_{S,S'}^2 + \mathrm{A}_0^2 - (\mathrm{A}_0 + \mathrm{A}_S)^2 - (\mathrm{A}_0 + \mathrm{A}_{S'})^2\right] \leq 4|S \cap S'|,$$

and for $j \geq 4$,

$$\mathrm{Tr}\left[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0 + \mathrm{A}_S)^j - (\mathrm{A}_0 + \mathrm{A}_{S'})^j\right] \leq 4\gamma^2(S, S') \cdot (2\|\mathrm{A}_{S,S'}\|_1)^{j-2}.$$

By Lemma B.3, Lemma B.5 and the assumption that $\max_{S,S'\in\mathcal{E}} \|\mathrm{A}_{S,S'}\|_1\theta < 2s\theta < 1/4$, we obtain

$$\begin{aligned}
&\sum_{j=1}^{\infty} \frac{(-\theta)^j}{2j} \mathrm{Tr}\left[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0 + \mathrm{A}_S)^j - (\mathrm{A}_0 + \mathrm{A}_{S'})^j\right] \\
&\qquad \leq |S \cap S'|\theta^2 + 4\gamma^2(S, S') \cdot (2\|\mathrm{A}_{S,S'}\|_1)^{-2} \cdot \sum_{j\geq 2} \frac{(2\|\mathrm{A}_{S,S'}\|_1\theta)^{2j}}{4j} \\
&\qquad \leq |S \cap S'|\theta^2 + 4\gamma^2(S, S') \cdot \|\mathrm{A}_{S,S'}\|_1^2\theta^4.
\end{aligned}$$

By the above inequality, (B.5), (B.6), and Lemma B.4, we have

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] \leq \exp\left[\mu\gamma^2(S, S')\theta^2 + 16s^2\gamma^2(S, S')\theta^4\right].$$

Since $\theta \leq \sqrt{\mu}/(4s)$, we have

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] \leq \exp\left[2\mu\gamma^2(S, S')\theta^2\right].$$

Notice that $2\mu\gamma^2(S,S')\theta^2 \le 2\mu k^2\theta^2 \le 1/2$. By the inequality $\exp(x) \le 1+2x$ for $x \le 1/2$, we have

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] \le \exp\left[2\mu\gamma^2(S,S')\theta^2\right] \le 1+4\mu\gamma^2(S,S')\theta^2.$$

Therefore, by Lemma B.2, we get

$$\frac{1}{n} < \frac{1}{|\mathcal{C}^+(q)|^2}\sum_{S,S'\in\mathcal{C}^+(q)} 4\mu\gamma^2(S,S')\theta^2 \le \sup_{S\in\mathcal{E}}\frac{1}{|\mathcal{C}^+(q)|}\sum_{S'\in\mathcal{C}^+(q)} 4\mu\gamma^2(S,S')\theta^2. \tag{B.7}$$

For $j=0,\ldots,k$, define $m_j = |\{S'\in\mathcal{E} : \max_{S\in\mathcal{E}}\gamma(S,S') = k-j\}|$. Then clearly we have $\sum_{j=0}^k m_j = |\mathcal{E}| \ge |\mathcal{C}^+(q)|$. Therefore there exists integer $l^+(q)\ge 1$ such that

$$\textstyle\sum_{j=0}^{l^+(q)} m_j > |\mathcal{C}^+(q)| \ge \sum_{j=0}^{l^+(q)-1} m_j. \tag{B.8}$$

We define

$$\overline{m}^+ = |\mathcal{C}^+(q)| - \sum_{j=0}^{l^+(q)-1} m_j.$$

Note that $h(j) := 4\mu(k-j)^2\theta^2$ is a decreasing function of j, and $\sum_{S'\in\mathcal{C}^+(q)} 4\mu\gamma^2(S,S')\theta^2$ is a sum of $m_1+\ldots+m_{l^+(q)-1}+\overline{m}$ terms, with at most m_j terms being $h(j)$. Therefore by (B.7), we have

$$\frac{1}{n} \le \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j + h(l^+(q))\cdot\overline{m}^+}{\sum_{j=0}^{l^+(q)-1} m_j + \overline{m}^+} \le \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j}{\sum_{j=0}^{l^+(q)-1} m_j}. \tag{B.9}$$

By assumption, for $i<j$ we have $m_i\zeta^j - m_j\zeta^i < 0$ and $h(i)-h(j) > 0$. Therefore we have $\sum_{1\le i<j\le l^+(q)-1}(m_i\zeta^j - m_j\zeta^i)[h(i)-h(j)] \le 0$. Rearranging terms gives

$$\frac{\sum_{j=0}^{l^+(q)-1} h(j)m_j}{\sum_{j=0}^{l^+(q)-1} m_j} \le \frac{\sum_{j=0}^{l^+(q)-1} h(j)\zeta^j}{\sum_{j=0}^{l^+(q)-1}\zeta^j} = \frac{\sum_{j=0}^{l^+(q)-1} h(j)\zeta^{-(k-j)}}{\sum_{j=0}^{l^+(q)-1}\zeta^{-(k-j)}}. \tag{B.10}$$

Note that $\zeta^{-1} \le c^{-1/2} < 1$ for large enough d. If $x \le c^{-1/2}$, for the function $\sum_{i=k-l+1}^k i^2x^i$, we have

$$\sum_{i=k-l+1}^{k} i^2x^i \le \sum_{i=k-l+1}^{\infty}(i+1)(i+2)x^i = \left(x^{k-l+3}\sum_{i=0}^{\infty}x^i\right)'' \le 2\overline{c}^3(k-l+3)^2x^{k-l+1}, \tag{B.11}$$

where $\overline{c} = \sqrt{c}/(\sqrt{c}-1)$. Combining (B.9), (B.10) and (B.11) gives

$$\frac{1}{n} \le 8\overline{c}^3\mu(k-l^+(q)+3)^2\theta^2.$$

Therefore, for large enough d we have

$$k - l^+(q) \ge \sqrt{\frac{1}{8\overline{c}^3\mu\theta^2 n}} - 3. \tag{B.12}$$

On the other hand, by the definition of $l^+(q)$ in (B.8), we have

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}^+(q)| \le \sum_{j=0}^{l^+(q)} m_j \le m_k\cdot\sum_{j=0}^{l^+(q)}\zeta^{j-k} \le \frac{\zeta^{-[k-l^+(q)]}|\mathcal{E}|}{1-\zeta^{-1}} \le 2\overline{c}\zeta^{-[k-l^+(q)]}\cdot|\mathcal{E}|, \tag{B.13}$$

where the last inequality follows from the fact that $\zeta^{-1} \le 1/\sqrt{c}$ and $1/(1-\zeta^{-1}) \le \overline{c}$. Plugging (B.12) into (B.13) gives

$$\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^{+}(q)| \le \overline{c}|\mathcal{E}| \exp\left[-\log(\zeta) \cdot \left(\sqrt{\frac{1}{8\overline{c}^3 \mu \theta^2 n}} - 3 \right) \right].$$

Applying the same analysis to $\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^{-}(q)|$, we obtain

$$\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^{-}(q)| \le \overline{c}|\mathcal{E}| \exp\left[-\log(\zeta) \cdot \left(\sqrt{\frac{1}{8\overline{c}^3 \mu \theta^2 n}} - 3 \right) \right].$$

Therefore

$$T \cdot \frac{\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|}{|\mathcal{E}|} \le 2\overline{c} \exp\left[\log(T) - \left(\sqrt{\frac{1}{8\overline{c}^3 \mu \theta^2 n}} - 3 \right) \cdot \log \zeta \right].$$

If $T \le d^{\eta}$, then

$$T \cdot \frac{\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|}{|\mathcal{E}|} \le \exp\left[\log(2\overline{c}) + \eta \log(d) - \left(\sqrt{\frac{1}{8\overline{c}^3 \mu \theta^2 n}} - 3 \right) \cdot \log \zeta \right].$$

Let $\kappa = [(p+1) \vee 3]^{-1} (8\overline{c}^3)^{-1/2}$. If $\theta \le \kappa \frac{\log \zeta}{\log d + \log \zeta} \sqrt{\frac{1}{\mu n}}$, then for large enough d we have

$$\log(2\overline{c}) + p \log(d) - \left(\sqrt{\frac{1}{8\mu\theta^2 n}} - 3 \right) \cdot \log \zeta \le -1,$$

and therefore $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|/|\mathcal{E}| < 1$. By Lemma B.1, when d is large enough, there exists an oracle r such that $R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{E}\}, \mathscr{A}, r) \ge 1$. This completes the proof.

B.2 Proofs of Upper Bounds

In this section, we provide the proofs of the upper bounds in §3.3. Before starting our proof, we first introduce a lemma.

Lemma B.6. The inverse matrix of $\theta \cdot \mathbf{1}_{m \times m} + (1-\theta) \cdot \mathrm{I}_m$ is

$$\frac{\theta}{(\theta-1)(m\theta - \theta + 1)} \cdot \mathbf{1}_{m \times m} + \frac{1}{1-\theta} \cdot \mathrm{I}_m, \tag{B.14}$$

where m is some integer.

Proof. This can be proved by direct calculation. □

B.2.1 Proof of Theorem 9

We first consider the case that $\theta > \kappa \sqrt{\log d/n}$ with a sufficient large constant κ. Note that we have

$$\mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q_{jk}(X)] = 0 \tag{B.15}$$

for any $j \ne k \in [d]$, since $(X_j + X_k)^2 \sim 2\chi_1^2$, $X_j^2 \sim \chi_1^2$ and $X_k^2 \sim \chi_1^2$ under $\mathbb{P}_0$. Invoking Lemma B.6 with $m = s$, for any $\Theta \in \mathcal{C}_1$, if $\theta_{jk} \ne 0$ we have

$$\mathbb{E}_{\mathbb{P}_{\Theta}}[q_{jk}(X)] = -\frac{\theta}{(1-\theta)(\theta s - \theta + 1)}, \tag{B.16}$$

since $(X_j + X_k)^2 \sim 2(\theta s - 3\theta + 1)/[(1-\theta)(\theta s - \theta + 1)] \cdot \chi_1^2$ and $X_j^2, X_k^2 \sim (\theta s - 2\theta + 1)/[(1-\theta)(\theta s - \theta + 1)] \cdot \chi_1^2$ under $\mathbb{P}_\Theta$. Thus we have

$$\mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q_{jk}(X)] - \mathbb{E}_{\mathbb{P}_\Theta}[q_{jk}(X)] = \frac{\theta}{(1-\theta)(\theta s - \theta + 1)}. \tag{B.17}$$

Let K denote the ψ_1-norm of Y, where $Y \sim \chi_1^2$. By Definition 3 $||q(\mathbf{X})||_{\psi_1, \mathbb{P}_{\mathrm{I}_d}} \cdot \tau$ equals

$$K \cdot \sqrt{\frac{\log[d(d-1)/2] + \log(1/\xi)}{n}} < \frac{\theta}{4} < \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}. \tag{B.18}$$

The first inequality lies on the fact that $\theta > \kappa\sqrt{\log d/n}$ with a sufficient large constant κ and the second inequality lies on the fact that $s\theta < 1/\sqrt{2}$ and $\theta < c$ for a small constant c, which implies

$$\frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)} > \frac{\theta(1 - 1/\sqrt{2})}{2 \cdot 1/2 \cdot 1} > \frac{\theta}{4},$$

when d is large enough. Similarly $||q(\mathbf{X})||_{\psi_1, \mathbb{P}_\Theta} \cdot \tau$ equals

$$K \cdot \frac{1 + \theta s - 3\theta}{(1-\theta)(\theta s - \theta + 1)} \cdot \sqrt{\frac{\log[d(d-1)/2] + \log(1/\xi)}{n}} < \frac{\theta}{4} < \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}. \tag{B.19}$$

The first inequality comes from the fact that $\theta > \kappa\sqrt{\log d/n}$ with a sufficient large constant κ and

$$\frac{1 + \theta s - 3\theta}{(1-\theta)(\theta s - \theta + 1)} < \frac{1 + 1/\sqrt{2}}{1/2 \cdot 1} < 4,$$

when d is large enough. Then we have

$$\begin{aligned}
R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) &\le \sup_{\Theta \in \mathcal{C}_0} \mathbb{P}_\Theta(\psi = 1) + \sup_{\Theta \in \mathcal{C}_1} \mathbb{P}_\Theta(\psi = 0) \\
&= \mathbb{P}_{\mathrm{I}_d}\left[\sup_{i \neq j} Z_{q_{i,j}} \le 1 - \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}\right] \\
&\quad + \sup_{\Theta \in \mathcal{C}_1} \mathbb{P}_\Theta\left[\sup_{i \neq j} Z_{q_{i,j}} > 1 - \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}\right] \\
&\le \mathbb{P}_{\mathrm{I}_d}\left[\left|\sup_{i \neq j} z_{q_{i,j}} - \mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q(X)]\right| > \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}\right] \\
&\quad + \sup_{\Theta \in \mathcal{C}_1} \mathbb{P}_\Theta\left[\left|\sup_{i \neq j} z_{q_{i,j}} - \mathbb{E}_{\mathbb{P}_\Theta}[q(X)]\right| > \frac{\theta(1 + \theta - \theta s)}{2(1-\theta)(\theta s - \theta + 1)}\right] \\
&\le 2\xi,
\end{aligned}$$

where the first and second inequalities are from (8), (B.15)-(B.19) and Definition 3.

For $\theta > \kappa\sqrt{\log d/(ns)}$ with a sufficient large constant κ, we have

$$\mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q_{\mathcal{S}}(X)] = 1, \tag{B.20}$$

since $1/s \cdot (\sum_{i \in \mathcal{S}} X_i)^2 \sim \chi_1^2$ under $\mathbb{P}_{\mathrm{I}_d}$. By invoking Lemma B.6 with $m = s$, there exists a $\Theta \in \mathcal{C}_1$ such that

$$\mathbb{E}_{\mathbb{P}_\Theta}[q_{\mathcal{S}}(X)] = \frac{1}{(\theta s - \theta + 1)}, \tag{B.21}$$

since $1/s \cdot (\sum_{i\in\mathcal{S}} X_i)^2 \sim 1/(\theta s - \theta + 1) \cdot \chi_1^2$ under $\mathbb{P}_\Theta$. Thus we have

$$\mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q_{\mathcal{S}}(X)] - \mathbb{E}_{\mathbb{P}_\Theta}[q_{\mathcal{S}}(X)] = \frac{(s-1)\theta}{s\theta - \theta + 1}. \tag{B.22}$$

Since $s\theta < 1/\sqrt{2}$, then we have

$$\frac{(s-1)\theta}{s\theta - \theta + 1} > \frac{(s-1)\theta}{2}, \tag{B.23}$$

when d is large enough. Let K denote the ψ_1-norm of Y, where $Y \sim \chi_1^2$. According to Definition 3 $||q(\mathbf{X})||_{\psi_1,\mathbb{P}_{\mathrm{I}_d}} \cdot \tau$ equals

$$K \cdot \sqrt{\frac{s\log d + \log(1/\xi)}{n}} < \frac{(s-1)\theta}{4} < \frac{(s-1)\theta}{2(s\theta - \theta + 1)}. \tag{B.24}$$

The first inequality comes from the fact that $\theta > \kappa\sqrt{\log d/(ns)}$ with a sufficient large constant κ and the second inequality comes from (B.23). Similarly $||q(\mathbf{X})||_{\psi_1,\mathbb{P}_\Theta} \cdot \tau$ equals

$$K \cdot \frac{1}{\theta s - \theta + 1} \cdot \sqrt{\frac{s\log d + \log(1/\xi)}{n}}. \tag{B.25}$$

Notice that $1/(\theta s - \theta + 1) < 1$, then from (B.24) we have

$$||q(\mathbf{X})||_{\psi_1,\mathbb{P}_\Theta} \cdot \tau = \frac{1}{\theta s - \theta + 1} \cdot ||q(\mathbf{X})||_{\psi_1,\mathbb{P}_{\mathrm{I}_d}} \cdot \tau < \frac{(s-1)\theta}{2(s\theta - \theta + 1)}. \tag{B.26}$$

Finally we have

$$\begin{aligned}
R_n(\mathcal{C}_0, \mathcal{C}_1, \mathscr{A}, r) &\le \sup_{\Theta\in\mathcal{C}_0} \mathbb{P}_\Theta(\psi = 1) + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta(\psi = 0) \\
&= \mathbb{P}_{\mathrm{I}_d}\left[\sup_{|\mathcal{S}'|=s} Z_{q_{\mathcal{S}'}} \le 1 - \frac{(s-1)\theta}{2(\theta s - \theta + 1)}\right] \\
&\quad + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta\left[\sup_{|\mathcal{S}'|=s} Z_{q_{\mathcal{S}'}} > 1 - \frac{(s-1)\theta}{2(\theta s - \theta + 1)}\right] \\
&\le \mathbb{P}_{\mathrm{I}_d}\left[\Big|\sup_{|\mathcal{S}'|=s} z_{q_{\mathcal{S}'}} - \mathbb{E}_{\mathbb{P}_{\mathrm{I}_d}}[q(X)]\Big| > \frac{(s-1)\theta}{2(\theta s - \theta + 1)}\right] \\
&\quad + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta\left[\Big|\sup_{|\mathcal{S}'|=s} z_{q_{\mathcal{S}'}} - \mathbb{E}_{\mathbb{P}_\Theta}[q(X)]\Big| > \frac{(s-1)\theta}{2(\theta s - \theta + 1)}\right] \\
&\le 2\xi,
\end{aligned}$$

where the first and second inequalities are from (B.20)-(B.26) and Definition 3.

Now we provide the proofs of the uppers for $s/2$-nearest neighbor detection in §3.3. Before starting our proof, we provide the following lemma.

Lemma B.7. Without loss of generality we assume that $m/4$ is an integer. First we define the matrix A_i as following,

$$\mathrm{A}_i = \begin{bmatrix} 0 & \mathrm{I}_{m-i} \\ \mathrm{I}_i & 0 \end{bmatrix}_{m\times m}. \tag{B.27}$$

Then we have the following equation,

$$\left(\mathrm{I}_m + \theta \cdot \sum_{i=1}^{m/4} \mathrm{A}_i + \theta \cdot \sum_{i=m-m/4}^{m-1} \mathrm{A}_i\right)^{-1} = \mathrm{B}, \tag{B.28}$$

where θ is some constant and the ij-th entry of B is

$$b_{ij} = \sum_{k=1}^{m} \frac{\mu^{k(j-i)}}{m \cdot a_k}.$$

Here $\mu = \exp(2\pi\mathbf{i}/m)$, $a_k = 1 + \theta \cdot \sum_{i=1}^{m/4} \mu^{ik} + \theta \cdot \sum_{i=m-m/4}^{m-1} \mu^{ik}$ and $\mathbf{i}$ is the imaginary unit.

Let μ be a primitive mth root of unity, which means $\mu^k \neq 1$ for $k = 1, \ldots, m-1$ and $\mu^m = 1$. More precisely, we just take $\mu = \exp(2\pi\mathbf{i}/m)$, where $\mathbf{i}$ is the imaginary unit. Then we consider vectors $e_j^\top = (\mu^j, \mu^{2j}, \ldots, \mu^{mj})^\top$, where $j = 1, 2, \ldots, m$. For the matrix A_i defined in (B.27), we have

$$\mathrm{A}_i e_j = \mu^{ij} \cdot e_j, \tag{B.29}$$

for $i = 1, \ldots, m-1$ and $j = 1, \ldots, m$. We use B to denote $(\mathrm{I}_m + \theta \cdot \sum_{i=1}^{m/4} \mathrm{A}_i + \theta \cdot \sum_{i=m-m/4}^{m-1} \mathrm{A}_i)$ in (B.28). Then we have

$$\mathrm{B}e_j = \biggl(1 + \theta \cdot \sum_{i=1}^{m/4} \mu^{ij} + \theta \cdot \sum_{i=m-m/4}^{m-1} \mu^{ij}\biggr) e_j.$$

We use a_j to denote $1 + \theta \cdot \sum_{i=1}^{m/4} \mu^{ij} + \theta \cdot \sum_{i=m-m/4}^{m-1} \mu^{ij}$ above for $j = 1, \ldots, m$. Then we calculate a_j,

$$\begin{aligned}
a_j &= 1 + \theta \cdot \sum_{i=1}^{m/4} \left[\mu^{ij} + \mu^{(m-i)j}\right] \\
&= 1 + \theta \cdot \sum_{i=1}^{m/4} \left\{ \cos\left(\frac{2ij\pi}{m}\right) + \mathbf{i}\sin\left(\frac{2ij\pi}{m}\right) + \cos\left[\frac{2(m-i)j\pi}{m}\right] + \mathbf{i}\sin\left[\frac{2(m-i)j\pi}{m}\right] \right\} \\
&= 1 + 2\theta \cdot \sum_{i=1}^{m/4} \cos\left(\frac{2ij\pi}{m}\right) \\
&= 1 + 2\theta \cdot \left[\sum_{i=1}^{m/4} \cos\left(\frac{2ij\pi}{m}\right)\right] \cdot \sin\left(\frac{j\pi}{m}\right) / \sin\left(\frac{j\pi}{m}\right) \\
&= 1 - \theta + \theta\left[\cos\left(\frac{j\pi}{2}\right) + \sin\left(\frac{j\pi}{2}\right)\cot\left(\frac{j\pi}{m}\right)\right].
\end{aligned}$$

The last equality comes from trigonometric identities and we define $\sin(j\pi/2) \cdot \cot(j\pi/m) = m/2$ when $j = m$. Now we use Λ to denote the diagonal matrix with diagonal entries $\{a_1, \ldots, a_m\}$ and $\mathrm{P} = (e_1, \ldots, e_m)$. Then we have $\mathrm{BP} = \mathrm{P}\Lambda$, which implies that $\mathrm{B}^{-1} = \mathrm{P}^{-1}\Lambda^{-1}\mathrm{P}$. Notice that $\bar{\mathrm{P}}\mathrm{P} = m \cdot \mathrm{I}$, so $\mathrm{P}^{-1} = 1/m \cdot \bar{\mathrm{P}}$. Here $\bar{\mathrm{P}}$ represents the conjugate matrix of P. By calculation we know that the ij-th entry of B is

$$b_{ij} = \sum_{k=1}^{m} \frac{\mu^{k(j-i)}}{m \cdot a_k}.$$

By applying Lemma B.7 with $m = s$, we can write out the covariance matrix under the alternative hypothesis. Then we follow the same proof as in B.2.1 and complete the proof.

Theorem B.8. For the 3-clique versus s-clique problem, if

$$\theta > \kappa\sqrt{\log d/n}$$

for some large enough constant κ, then we consider the local minimum test as follows

$$q_{jk}(X) = [(X_j + X_k)^2 - X_j^2 - X_k^2]/2, \tag{B.30}$$

$$\psi = \mathbb{1}\left[\inf_{j_1\neq k_1, j_2\neq k_2, j_3\neq k_3, j_4\neq k_4} \max_{1\leq i\leq 4} z_{q_{j_i k_i}} \leq -\frac{\theta(1+\theta-\theta s)}{2(1-\theta)(\theta s - \theta + 1)}\right], \tag{B.31}$$

where $j_1 \neq k_1, \ldots, j_4 \neq k_4 \in [d]$ and $z_{q_{j_1k_1j_2k_2j_3k_3j_4k_4}}$ is the random realization of query function $q_{j_1k_1j_2k_2j_3k_3j_4k_4}(\cdot)$ given by an oracle. We have

$$\liminf_{n\to\infty}\left[\sup_{\Theta\in\mathcal{C}_0}\mathbb{P}_\Theta(\psi=1)+\sup_{\Theta\in\mathcal{C}_1}\mathbb{P}_\Theta(\psi=0)\right]=0.$$

Proof of Theorem B.8. First, under the null hypothesis, for any $\Theta \in \mathcal{C}_0$, by Lemma B.6 we have

$$\mathbb{E}_{\mathbb{P}_\Theta}[q_{jk}(X)] = \begin{cases} -\frac{\theta}{(1-\theta)(2\theta+1)}, & \text{if } (j,k) \text{ is an edge of the 3-clique,} \\ 0, & \text{otherwise.} \end{cases}$$

Similar to the proof of Theorem 9, since under null hypothesis $q_{jk}(X)$ is a combination of χ^2 random variables, by Definition 3, for $\Theta \in \mathcal{C}_0$, $||q(\mathbf{X})||_{\psi_1,\mathbb{P}_{\mathbb{I}_d}} \cdot \tau$ equals

$$K\cdot\sqrt{\frac{\log[d(d-1)/2]+\log(1/\xi)}{n}} < \frac{\theta}{4} < \frac{\theta(1+\theta-\theta s)}{2(1-\theta)(\theta s-\theta+1)}. \tag{B.32}$$

The first inequality lies on the fact that $\theta > \kappa\sqrt{\log d/n}$ with a sufficient large constant κ and the second inequality lies on the fact that $s\theta < 1/\sqrt{2}$ and $\theta < c$ for a small constant c, which implies

$$\frac{\theta(1+\theta-\theta s)}{2(1-\theta)(\theta s-\theta+1)} > \frac{\theta(1-1/\sqrt{2})}{2\cdot 1/2\cdot 1} > \frac{\theta}{4},$$

when d is large enough. Note that for a 3-clique, among any four distinct pairs $(j_1,k_1),(j_2,k_2),(j_3,k_3),(j_4,k_4)$, at most three pairs of indices can represent an edge of the graph. Therefore we have

$$\sup_{\Theta\in\mathcal{C}_0}\mathbb{P}_\Theta(\psi=1)\leq\xi. \tag{B.33}$$

Similarly, for any $\Theta \in \mathcal{C}_1$, under the alternative hypothesis we have

$$\mathbb{E}_{\mathbb{P}_\Theta}[q_{jk}(X)] = \begin{cases} -\frac{\theta}{(1-\theta)(2\theta+1)}, & \text{if } (j,k) \text{ is an edge of the } s\text{-clique,} \\ 0, & \text{otherwise,} \end{cases}$$

Moreover, for $\Theta \in \mathcal{C}_1$, $||q(\mathbf{X})||_{\psi_1,\mathbb{P}_\Theta} \cdot \tau$ equals

$$K\cdot\frac{1+\theta s-3\theta}{(1-\theta)(\theta s-\theta+1)}\cdot\sqrt{\frac{\log[d(d-1)/2]+\log(1/\xi)}{n}} < \frac{\theta}{4} < \frac{\theta(1+\theta-\theta s)}{2(1-\theta)(\theta s-\theta+1)}. \tag{B.34}$$

The first inequality comes from the fact that $\theta > \kappa\sqrt{\log d/n}$ with a sufficient large constant κ and

$$\frac{1+\theta s-3\theta}{(1-\theta)(\theta s-\theta+1)} < \frac{1+1/\sqrt{2}}{1/2\cdot 1} < 4,$$

when d is large enough. Now if the four pairs of indices $(j_1,k_1),(j_2,k_2),(j_3,k_3),(j_4,k_4)$ all represent edges in the s-clique, then by Definition 3, we have

$$\mathbb{P}_\Theta\left[\max_{1\leq i\leq 4} z_{q_{j_ik_i}} \leq -\frac{\theta(1+\theta-\theta s)}{2(1-\theta)(\theta s-\theta+1)}\right]\leq\xi.$$

Therefore, we have

$$\sup_{\Theta\in\mathcal{C}_1}\mathbb{P}_\Theta(\psi=0)\leq\xi. \tag{B.35}$$

Adding (B.35) to (B.33) gives

$$R_n(\mathcal{C}_0,\mathcal{C}_1,\mathscr{A},r)\leq\sup_{\Theta\in\mathcal{C}_0}\mathbb{P}_\Theta(\psi=1)+\sup_{\Theta\in\mathcal{C}_1}\mathbb{P}_\Theta(\psi=0)\leq 2\xi,$$

which completes the proof. $\square$

B.3 Proofs of Discussion

In this section we provide the proofs in section A.

B.3.1 Proof of Corollary A.1

Proof. Let $G_0 = (V, \emptyset)$. Clearly, $\mathcal{C} = \{E[G(\Theta)] : \Theta \in \mathcal{C}_1\}$ is a null-alternative separator. By Definition 5, setting $S' = S$ gives

$$\mu \geq \frac{|S|}{|V(S)|^2} = \frac{|V(S)| \cdot (|V(S)| - 1)}{2|V(S)|^2} = \frac{1}{2} - \frac{1}{2|V(S)|} \geq \frac{1}{4},$$

where we use $|V(S)| \geq 2$ in the last inequality. Moreover, by Lemma B.4, we have $\mu \leq 1/2$. Therefore μ is of constant order. For $j = 0, \ldots, k$, define $m_j = |\{S' \in \mathcal{E} : \max_{S \in \mathcal{E}} \gamma(S, S') = k - j\}|$. Then

$$\frac{m_{j+1}}{m_j} = \left[\binom{s}{s-j-1}\binom{d-s}{j+1}\right] \Big/ \left[\binom{s}{s-j}\binom{d-s}{j}\right] \geq \frac{d}{s^2}.$$

Taking infimum over j gives $\zeta \geq d/s^2 \geq Cd^{1-2\alpha}$ for some absolute constant C. Therefore we have

$$\theta \leq \kappa\frac{1}{\sqrt{n}} \leq \frac{2\kappa}{1-2\alpha}\frac{\log\zeta}{\log d + \log\zeta}\frac{1}{\sqrt{n}}.$$

Since we have $\liminf_{n\to\infty}\zeta \geq \liminf_{n\to\infty} d^{1-2\alpha} = \infty$, picking κ to be small enough allows us to apply Theorem 7. This completes the proof. □

B.3.2 Proof of Corollary A.2

Proof. Let $G_0 = (V, \emptyset)$. Clearly, $\mathcal{C} = \{E[G(\Theta)] : \Theta \in \mathcal{C}_1\}$ is a null-alternative separator. By Definition 5, setting $S' = S$ gives

$$\mu \geq \frac{|S|}{|V(S)|^2} = \frac{|V(S)| \cdot (|V(S)| - 1)}{4|V(S)|^2} = \frac{1}{4} - \frac{1}{4|V(S)|} \geq \frac{1}{8},$$

where we use $|V(S)| \geq 2$ in the last inequality. Moreover, by Lemma B.4, we have $\mu \leq 1/2$. Therefore μ is of constant order. For $j = 0, \ldots, k$, define $m_j = |\{S' \in \mathcal{E} : \max_{S \in \mathcal{E}} \gamma(S, S') = k - j\}|$. Then

$$\frac{m_{j+1}}{m_j} = \left[\binom{s}{s-j-1}\binom{d-s}{j+1}\cdot s!\right] \Big/ \left[\binom{s}{s-j}\binom{d-s}{j}\cdot s!\right] \geq \frac{d}{s^2}.$$

Taking infimum over j gives $\zeta \geq d/s^2 \geq Cd^{1-2\alpha}$ for some absolute constant C. Therefore we have

$$\theta \leq \kappa\frac{1}{\sqrt{n}} \leq \frac{2\kappa}{1-2\alpha}\frac{\log\zeta}{\log d + \log\zeta}\frac{1}{\sqrt{n}}.$$

Since we have $\liminf_{n\to\infty}\zeta \geq \liminf_{n\to\infty} d^{1-2\alpha} = \infty$, picking κ to be small enough allows us to apply Theorem 7. This completes the proof. □

B.3.3 Proof of Theorem A.5

The first several steps in this proof is exactly the same as the proof of Theorem 7. The precision matrices are constructed as

$$\Theta_0 = \mathrm{A} + \theta\mathrm{A}_0, \;\; \Theta_S = \mathrm{A} + \theta(\mathrm{A}_0 + \mathrm{A}_S).$$

We next give lower bound for $R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{C}\}, \mathscr{A}, r)$. Intuitively, for any $\sigma \in \mathcal{C}$, in order to succeed with the worst-case oracle, a test has to utilize at least one query q that can distinguish Θ_S from Θ_0. We define

$$\mathcal{C}(q) = \{S \in \mathcal{C} : |\mathbb{E}_S q(X) - \mathbb{E}_0 q(X)| \geq \|q(X)\|_{\psi_{1,0}} \cdot \tau\},$$

where $|q(X)|_{\psi_1,0}$ is the ψ_1-norm of $q(X)$ when $X \sim \mathbb{P}_0$, and $\overline{\tau} := \sqrt{2/n}$ is a lower bound of τ defined in (7). By Lemma B.1, we only need to show $T \cdot \sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{C}|$ for large enough d. In the rest of this proof, for any $q \in \mathcal{Q}_{\mathscr{A}}$, we derive an upper bound on $|\mathcal{C}(q)|$. Same as before, we define the sets

$$\mathcal{C}^+(q) = \{S \in \mathcal{C} : \mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)] > \|q(X)\|_{\psi_1,0} \cdot \tau\}\,, \tag{B.36}$$

$$\mathcal{C}^-(q) = \{S \in \mathcal{C} : \mathbb{E}_0[q(X)] - \mathbb{E}_S[q(X)] > \|q(X)\|_{\psi_1,0} \cdot \tau\}\,. \tag{B.37}$$

We now bound $|\mathcal{C}^+(q)|$. $|\mathcal{C}^-(q)|$ can be bounded in exactly the same way. The following lemma summarizes an inequality derived from the definition (B.2). By Lemma B.2, for any query function q, we have

$$\frac{1}{|\mathcal{C}^+(q)|^2} \sum_{S,S'\in\mathcal{C}^+(q)} \mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] > 1 + \frac{1}{n}. \tag{B.38}$$

For the left-hand side of (B.38), we have

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] = \exp\left\{\sum_{k=1}^{\infty}\frac{(-\theta)^k}{2k}\operatorname{Tr}\big[\mathrm{A}_{S,S'}^k + \mathrm{A}_0^k - (\mathrm{A}_0+\mathrm{A}_S)^k - (\mathrm{A}_0+\mathrm{A}_{S'})^k\big]\right\}, \tag{B.39}$$

where $\Theta_{S,S'} = \Theta_0 + \theta\mathrm{A}_S + \theta\mathrm{A}_{S'}$, and $\mathrm{A}_{S,S'} = \mathrm{A}_0 + \mathrm{A}_S + A_{S'}$. Then by Lemma B.3, Lemma B.5, and the assumption that $\max_{S,S'\in\mathcal{C}} \|\mathrm{A}_{S,S'}\|_1\theta < 2s\theta < 1/4$, we obtain

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{(-\theta)^k}{2k}\operatorname{Tr}\left[\mathrm{A}_{S,S'}^k + \mathrm{A}_0^k - (\mathrm{A}_0+\mathrm{A}_S)^k - (\mathrm{A}_0+\mathrm{A}_{S'})^k\right]&\\ \le |S\cap S'|\theta^2 + 4\gamma^2(S,S')\|\mathrm{A}_{S,S'}\|_1^2\theta^4.&\end{aligned}$$

By the above inequality, (B.39), and Lemma B.4, we have

$$\mathbb{E}_0\bigg[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\bigg] \le \exp\big[\mu\gamma^2(S,S')\theta^2 + 16s^2\gamma^2(S,S')\theta^4\big].$$

Since $\theta \le \sqrt{\mu}/(4s)$, we have

$$\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right] \le \exp\big[2\mu\gamma^2(S,S')\theta^2\big] \le 1 + 4\mu\gamma^2(S,S')\theta^2.$$

Therefore, by Lemma B.2, we get

$$\frac{1}{n} < \frac{1}{|\mathcal{C}^+(q)|^2}\sum_{S,S'\in\mathcal{C}^+(q)} 4\mu\gamma^2(S,S')\theta^2 \le \sup_{S\in\mathcal{C}}\frac{1}{|\mathcal{C}^+(q)|}\sum_{S'\in\mathcal{C}^+(q)} 4\mu\gamma^2(S,S')\theta^2. \tag{B.40}$$

For $j = 0, \ldots, k$, define $m_j = |\{S' \in \mathcal{E} : \max_{S\in\mathcal{E}} \gamma(S,S') = k - j\}|$. Then by definition, for any query function q, there exists integer $l^+(q)$ that satisfies

$$\textstyle\sum_{j=0}^{l^+(q)} m_j > |\mathcal{C}^+(q)| \ge \sum_{j=0}^{l^+(q)-1} m_j. \tag{B.41}$$

We define

$$\overline{m}^+ = |\mathcal{C}^+(q)| - \sum_{j=0}^{l^+(q)-1} m_j.$$

Note that $h(j) := 4\mu(k-j)^2\theta^2$ is a decreasing function of j, and $\sum_{S'\in\mathcal{C}^+(q)} h[\gamma(S,S')]$ is a sum of $m_1+\ldots+m_{l^+(q)-1}+\overline{m}$ terms, with at most m_j terms being $h(j)$. Therefore by (B.40), we have

$$\frac{1}{n} \le \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j + h[l^+(q)]\cdot\overline{m}^+}{\sum_{j=0}^{l^+(q)-1} m_j + \overline{m}^+} \le \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j}{\sum_{j=0}^{l^+(q)-1} m_j}. \tag{B.42}$$

For $l \le r$, by assumptions for $i < j \le l$ we have $m_i\zeta_r^j - m_j\zeta_r^i < 0$ and $h(i) - h(j) > 0$. Therefore we have $\sum_{1\le i<j\le l^+(q)-1}(m_i\zeta_r^j - m_j\zeta_r^i)[h(i) - h(j)] \le 0$. Rearranging terms gives

$$\frac{\sum_{j=0}^{l-1} h(j)m_j}{\sum_{j=0}^{l-1} m_j} \le \frac{\sum_{j=0}^{l-1} h(j)\zeta_r^j}{\sum_{j=0}^{l-1} \zeta_r^j} = \frac{\sum_{j=0}^{l-1} h(j)\zeta_r^{-(k-j)}}{\sum_{j=0}^{l-1} \zeta_r^{-(k-j)}}. \tag{B.43}$$

Note that $\zeta_r^{-1} \le c^{-1/2} < 1$ for large enough d. If $x \le c^{-1/2}$, for the function $\sum_{i=k-l+1}^{k} i^2x^i$, we have

$$\sum_{i=k-l+1}^{k} i^2x^i \le \sum_{i=k-l+1}^{\infty}(i+1)(i+2)x^i = \left(x^{k-l+3}\sum_{i=0}^{\infty}x^i\right)'' \le 2\overline{c}^3(k-l+3)^2x^{k-l+1}, \tag{B.44}$$

where $\overline{c} = \sqrt{c}/(\sqrt{c}-1)$. Combining (B.42), (B.43) and (B.44) gives

$$\mathbb{E}\left\{h\left[\sup_{S\in\mathcal{C}}\gamma(S,S')\right]\middle|\sup_{S\in\mathcal{C}}\gamma(S,S') \ge k-l\right\} = \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j}{\sum_{j=0}^{l^+(q)-1} m_j} \le 8\overline{c}^3\mu(k-l+3)^2\theta^2, \tag{B.45}$$

where the expectation is taken with respect to the uniform distribution over $S' \in \mathcal{C}$. Note that (B.45) holds when $l = r$. Plugging in the definition of r gives

$$\mathbb{E}\left\{h\left[\sup_{S\in\mathcal{C}}\gamma(S,S')\right]\middle|\sup_{S\in\mathcal{C}}\gamma(S,S') \ge k-r\right\} \le 8\overline{c}^3\mu(k-r+3)^2\theta^2. \tag{B.46}$$

We now prove that $8\overline{c}^3\mu(k-r+3)^2\theta^2 < 1/n$. If $k+3-(16\overline{c}^3\mu n\theta^2)^{-1/2} < 3$, then $r = 3$ and

$$(16\overline{c}^3\mu n\theta^2)^{-1/2} > k,$$

which implies that $8\overline{c}^3\mu(k-r+3)^2\theta^2 = 8\overline{c}^3\mu k^2\theta^2 < 1/n$. If $k+3-(16\overline{c}^3\mu n\theta^2)^{-1/2} \ge 3$, then $r = k+3-(16\overline{c}^3\mu n\theta^2)^{-1/2}$ and

$$8\overline{c}^3\mu(k-r+3)^2\theta^2 = \frac{1}{2n} < \frac{1}{n}.$$

Therefore, by (B.46), we have

$$\mathbb{E}\left\{h\left[\sup_{S\in\mathcal{C}}\gamma(S,S')\right]\middle|\sup_{S\in\mathcal{C}}\gamma(S,S') \ge k-r\right\} < \frac{1}{n}. \tag{B.47}$$

From (B.42), (B.47), and the fact that $\mathbb{E}\left\{h\left[\sup_{S\in\mathcal{C}}\gamma(S,S')\right]\middle|\sup_{S\in\mathcal{C}}\gamma(S,S') \ge k-l\right\}$ is a decreasing function of l, we obtain that $l^+(q) \le r$. Therefore inequality (B.45) holds for $l = l^+(q)$ as well. By B.42, we get

$$\frac{1}{n} \le 8\overline{c}^3\mu\left[k-l^+(q)+3\right]^2\theta^2.$$

Therefore, for large enough d we have

$$k - l^+(q) \ge \sqrt{\frac{1}{8\overline{c}^3\theta^2 n}} - 3.$$

Subtracting $k-r$ on both sides gives

$$r - l^+(q) \ge \sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}} - 3. \tag{B.48}$$

On the other hand, by the definition of $l^+(q)$ in (B.8), we have

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^+(q)| \le \sum_{j=0}^{l^+(q)} m_j \le m_r \cdot \sum_{j=0}^{l^+(q)} \zeta_r^{j-r} \le \frac{\zeta_r^{-[r-l^+(q)]}|\mathcal{C}|}{1-\zeta^{-1}} \le \overline{c}\zeta_r^{-[r-l^+(q)]} \cdot |\mathcal{C}|, \tag{B.49}$$

where the last inequality follows from the fact that $\zeta_r^{-1} \le c^{-1/2}$ and $1/(1-\zeta_r^{-1}) \le \overline{c}$. Plugging (B.48) into (B.49) gives

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^+(q)| \le \overline{c}|\mathcal{C}| \exp\left\{ -\log(\zeta)\cdot\left(\sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}}-3\right)\right\}.$$

Applying the same analysis to $\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^-(q)|$, we obtain

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^-(q)| \le \overline{c}|\mathcal{C}| \exp\left\{ -\log(\zeta)\cdot\left(\sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}}-3\right)\right\}.$$

Therefore

$$T\cdot\frac{\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|}{|\mathcal{C}|} \le \exp\left\{\log(2\overline{c}) + \log(T) - \left(\sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}}-3\right)\cdot\log\zeta\right\}.$$

If $T \le d^\eta$, then

$$T\cdot\frac{\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|}{|\mathcal{C}|} \le \exp\left\{\log(2\overline{c}) + \eta\log(d) - \left(\sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}}-3\right)\cdot\log\zeta\right\}.$$

Let $\kappa = [(p+1)\vee 3]^{-1}(16\overline{c}^3)^{-1/2}$. If $\theta \le \kappa\frac{\log\zeta}{\log d+\log\zeta}\sqrt{\frac{1}{\mu n}}$, then for large enough d we have

$$\log(2\overline{c}) + \eta\log d - \left(\sqrt{\frac{1}{16\overline{c}^3\mu\theta^2 n}}-3\right)\cdot\log\zeta \le -1,$$

and therefore $T\cdot\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|/|\mathcal{C}| < 1$. By Lemma B.1, when d is large enough, there exists an oracle r such that $R_n(\{\Theta_0\},\{\Theta_S : S\in\mathcal{C}\},\mathscr{A},r)\ge 1$.. This completes the proof.

B.3.4 Proof of Corollary A.6

Let $G_0 = (V,\emptyset)$. Clearly, $\mathcal{C} = \{E[G(\Theta)] : \Theta\in\mathcal{C}_1\}$ is a null-alternative separator. By Definition 5, setting $S' = S$ gives

$$\mu \ge \frac{|S|}{|V(S)|^2} = \frac{|V(S)|\cdot(|V(S)|-1)}{2|V(S)|^2} = \frac{1}{2} - \frac{1}{2|V(S)|} \ge \frac{1}{4},$$

where we use $|V(S)|\ge 2$ in the last inequality. Moreover, by Lemma B.4, we have $\mu\le 1/2$. Therefore μ is of constant order. By counting the number of derangements, we have $k = s$,

$$m_j := |\{S'\in\mathcal{E} : \max_{S\in\mathcal{E}}\gamma(S,S') = s-j\}| = \binom{s}{s-j}\sum_{i=0}^{j+1}\frac{(-1)^i j!}{i!}.$$

Therefore for $j\le r$, we have

$$\frac{m_{j+1}}{m_j} = \frac{\sum_{i=0}^{j+1}(-1)^i/i!}{\sum_{i=0}^{j}(-1)^i/i!}\cdot(s-j) \ge (s-r)/3 = (16\mu n\theta^2)^{-1/2}/3.$$

Taking infimum over $0 \le j \le r$ gives

$$\zeta_r \ge (16\mu n\theta^2)^{-1/2}/3.$$

If $\theta \le \kappa/(\sqrt{n}\log d)$, when d is large enough we have $\zeta_r \ge (16\mu n\theta^2)^{-1/2}/3 \ge e$. Therefore for large enough d, we have

$$\theta \le \kappa/(\sqrt{n}\log d) \le 2\kappa\frac{1}{\log d + \log\zeta_r}\frac{1}{\sqrt{n}} \le 2\kappa\frac{\log\zeta_r}{\log d + \log\zeta_r}\frac{1}{\sqrt{n}}.$$

Applying Theorem A.5 completes the proof.

B.3.5 Proof of Theorem A.7

Similar to the proofs for Theorem 7 and Theorem A.5, we define the sets

$$\mathcal{C}^+(q) = \{S \in \mathcal{C} : \mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)] > \|q(X)\|_{\psi_1,0}\cdot\tau\}, \tag{B.50}$$
$$\mathcal{C}^-(q) = \{S \in \mathcal{C} : \mathbb{E}_0[q(X)] - \mathbb{E}_S[q(X)] > \|q(X)\|_{\psi_1,0}\cdot\tau\}. \tag{B.51}$$

And it suffices to show that $T\cdot\max_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|/|\mathcal{C}| < 1$. We now bound $\mathcal{C}^+(q)$. With the same derivation as Theorem 7 and Theorem A.5, we obtain

$$\mathbb{E}_0\biggl[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\biggr] = \exp\Biggl\{\sum_{j=1}^{\infty}\frac{(-\theta)^j}{2j}\operatorname{Tr}\bigl[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0+\mathrm{A}_S)^j - (\mathrm{A}_0+\mathrm{A}_{S'})^j\bigr]\Biggr\}. \tag{B.52}$$

We introduce the following lemma from [2], which is slightly different from Lemma B.5.

Lemma B.9. For S and S' in $\mathcal{C}$, we have

$$\operatorname{Tr}\bigl[\mathrm{A}_{S,S'}^2 + \mathrm{A}_0^2 - (\mathrm{A}_0+\mathrm{A}_S)^2 - (\mathrm{A}_0+\mathrm{A}_{S'})^2\bigr] \le 4|S\cap S'|,$$

and for $j \ge 4$,

$$\operatorname{Tr}\bigl[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0+\mathrm{A}_S)^j - (\mathrm{A}_0+\mathrm{A}_{S'})^j\bigr] \le 4\gamma(S,S')\cdot\|\mathrm{A}_S\|_2\cdot\|\mathrm{A}_{S'}\|_2\cdot(2\|\mathrm{A}_{S,S'}\|_2)^{j-2}.$$

By Lemma B.3, Lemma B.9 and the inequality $\max_{S,S'\in\mathcal{C}}\|\mathrm{A}_{S,S'}\|_2\theta \le 5\theta < 1/4$ for large enough n, we obtain

$$\begin{aligned}
&\sum_{j=1}^{\infty}\frac{(-\theta)^j}{2j}\operatorname{Tr}\bigl[\mathrm{A}_{S,S'}^j + \mathrm{A}_0^j - (\mathrm{A}_0+\mathrm{A}_S)^j - (\mathrm{A}_0+\mathrm{A}_{S'})^j\bigr] \\
&\quad\le |S\cap S'|\theta^2 + 4\gamma(S,S')\cdot\|\mathrm{A}_S\|_2\cdot\|\mathrm{A}_{S'}\|_2\cdot(2\|\mathrm{A}_{S,S'}\|_2)^{-2}\cdot\sum_{j\ge 2}\frac{(2\|\mathrm{A}_{S,S'}\|_1\theta)^{2j}}{4j} \\
&\quad\le |S\cap S'|\theta^2 + 4\gamma(S,S')\cdot\|\mathrm{A}_S\|_2\cdot\|\mathrm{A}_{S'}\|_2\cdot\|\mathrm{A}_{S,S'}\|_2^2\cdot\theta^4.
\end{aligned}$$

By the above inequality and Lemma B.4, we have

$$\mathbb{E}_0\biggl[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\biggr] \le \exp\bigl[|S\cap S'|\theta^2 + 4\cdot 15^2\gamma(S,S')\theta^4\bigr].$$

For large enough n we have $\theta < 1/30$. Hence

$$\mathbb{E}_0\biggl[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\biggr] \le \exp\bigl\{[|S\cap S'| + \gamma(S,S')]\theta^2\bigr\}.$$

By Lemma B.2, we have

$$1 + \frac{1}{n} \leq \frac{1}{|\mathcal{C}^+(q)|^2} \sum_{S,S' \in \mathcal{C}^+(q)} \exp\left\{[|S \cap S'| + \gamma(S,S')]\theta^2\right\}.$$

Note that in hypercube detection problem, for different S and S' in $\mathcal{C}$, we have $V(S) \cap V(S') = \emptyset$. Meanwhile $|S| \leq Ds$ and $\gamma(S,S) = s$. Therefore by $Ds\theta^2 \leq 1/4$, we have

$$1 + \frac{1}{n} \leq \frac{[|\mathcal{C}^+(q)| - 1] \cdot 1 + \exp[(D+1)s\theta^2]}{|\mathcal{C}^+(q)|} \leq 1 + \frac{\exp(2Ds\theta^2) - 1}{|\mathcal{C}^+(q)|} \leq 1 + \frac{4Ds\theta^2}{|\mathcal{C}^+(q)|}.$$

Plugging in $|\mathcal{C}| = d/s$ gives

$$T \cdot |\mathcal{C}^+(q)|/|\mathcal{C}| \leq 4DTns^2\theta^2/d.$$

Similarly, for $\mathcal{C}^-(q)$, we have

$$T \cdot |\mathcal{C}^-(q)|/|\mathcal{C}| \leq 4DTns^2\theta^2/d.$$

Summing the two inequalities above and plugging in the condition that $\theta \leq \kappa/\sqrt{ns}$, we obtain

$$T \cdot \max_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|/|\mathcal{C}| \leq 8\kappa Ds/d.$$

Since κ and D are absolute constants and $T = o(d/s)$, for large enough d we have

$$T \cdot \max_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|/|\mathcal{C}| < 1.$$

By Lemma B.1, when d is large enough, there exists an oracle r such that $R_n(\{\Theta_0\}, \{\Theta_S : S \in \mathcal{C}\}, \mathscr{A}, r) \geq 1$. This completes the proof.

B.3.6 Proof of Theorem A.8

We first bound the entries in the covariance matrix. Let A_b be the adjacency matrix of a lattice graph and $\Theta_b = \mathrm{I}_d + \theta\mathrm{A}_b$. Under the assumption that $theta \leq 1/(2D)$, we have $\|\theta\mathrm{A}_b\|_2 \leq 1/2$. Therefore, if $(\mathrm{A}_b)_{ij} = 1$, then

$$e_i^T\Theta^{-1}e_j = e_i^T\mathrm{I}_d e_j + \sum_{k=1}^{\infty}(-1)^k\theta^k e_i^T\mathrm{A}_b^k e_j \leq -\theta + \sum_{k=2}^{\infty}(-1)^k\theta^k\|\mathrm{A}_b\|_2^k \leq -\theta + \frac{1}{2}\theta = -\frac{1}{2}\theta.$$

Therefore under the alternative hypothesis with $\theta = \theta_b$, we have

$$\mathbb{E}_{\mathbb{P}_{\Theta_b}}[X_iX_j] \leq -\theta/2.$$

Now we proceed to derive concentration results for $q_b(X)$. Note that we have

$$\frac{\sqrt{|E_b|}}{2\sqrt{2}} \cdot q_b(X) = \frac{1}{4\sqrt{2|E_b|}}X^T\mathrm{A}_bX = \frac{1}{8\|\mathrm{A}_b\|_F}X^T\mathrm{A}_bX = \frac{1}{2}X^T\mathrm{M}_bX,$$

where $\mathrm{M}_b = \mathrm{A}_b/(4\|\mathrm{A}_b\|_F)$. Then

$$\log\mathbb{E}_{\mathbb{P}_{\Theta_b}}\exp(q_b(X)) = \frac{1}{2}\log\left[\frac{\det(\Theta_b)}{\det(\Theta_b + \mathrm{M}_b)}\right] = \sum_{k=1}^{\infty}\frac{(-1)^k}{2k}\mathrm{Tr}[(\theta\mathrm{A}_b + \mathrm{M}_b)^k - (\theta\mathrm{A}_b)^k].$$

Under our assumptions, we have $\|\theta\mathrm{A}_b + \mathrm{M}_b\|_F \le 1/2$, $\|\theta\mathrm{A}_b\|_F \le 1/2$. Hence

$$\log \mathbb{E}_{\mathbb{P}_{\Theta_b}} \exp(q_b(X)) \le \frac{1}{2}\sum_{k=1}^{\infty} \|\theta\mathrm{A}_b + \mathrm{M}_b\|_F^k + \|\theta\mathrm{A}_b\|_F^k \le 1.$$

Therefore by (5.16) in [3], we have

$$\|q_b(X)\|_{\psi_1,\mathbb{P}_{\Theta_b}} \le C\frac{1}{\sqrt{|E_b|}},$$

where C is an absolute constant. With similar proof, we also have

$$\|q_b(X)\|_{\psi_1,\mathbb{P}_{\mathrm{I}_d}} \le C'\frac{1}{\sqrt{|E_b|}}$$

for some absolute constant C'. Note that we have $\sqrt{s} \le \sqrt{|E_b|} \le \sqrt{Ds}$. Therefore, similar to the proof of Theorem 9, we have

$$\begin{aligned} R_n(\mathcal{C}_0,\mathcal{C}_1,\mathscr{A},r) &\le \sup_{\Theta\in\mathcal{C}_0} \mathbb{P}_\Theta(\psi=1) + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta(\psi=0) \\ &= \mathbb{P}_{\mathrm{I}_d}\left[\sup_b Z_{q_b} \le -\theta/4\right] + \sup_{\Theta\in\mathcal{C}_1} \mathbb{P}_\Theta\left[\sup_b Z_{q_b} > -\theta/4\right] \\ &\le 2\xi. \end{aligned}$$

C Proofs of Auxiliary Results in §B

Proof of Lemma B.1. Given an algorithm $\mathscr{A}$ which makes queries $q_1,\ldots,q_T \in \mathcal{Q}$. If $T \cdot \sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{E}|$, there exists $S_0 \in \mathcal{E}\setminus\bigcup_{t=1}^T \mathcal{C}(q_t)$. Then by definition, for $t=1,\ldots,T$ we have

$$|\mathbb{E}_{\mathbb{P}_{S_0}} q_t(X) - \mathbb{E}_{\mathbb{P}_0} q_t(X)| \le \|q_t(X)\|_{\psi_1,\mathbb{P}_0} \cdot \tau.$$

We set r to be the oracle that returns Z_{q_t} such that

$$\begin{aligned} &\mathbb{P}_0(Z_{q_t} = \mathbb{E}_{\mathbb{P}_{S_0}}[q_t(X)]) = 1, \\ &\mathbb{P}_S(Z_{q_t} = \mathbb{E}_{\mathbb{P}_S}[q_t(X)]) = 1,\ S\in\mathcal{E}. \end{aligned}$$

Then clearly

$$\mathbb{P}_0(|Z_{q_t} - \mathbb{E}_{\mathbb{P}_{S_0}}[q_t(X)]| \le \|q_t(X)\|_{\psi_1,\mathbb{P}_0}\cdot\tau) = 1,$$

and hence r satisfies the definition 1. However for $t=1,\ldots,T$, the oracle always returns the same Z_{q_t} under $\mathbb{P}_0$ and $\mathbb{P}_{S_0}$. Therefore we have

$$\mathbb{P}_0(\psi=1) + \mathbb{P}_{S_0}(\psi=0) = 1.$$

This completes the proof. □

Proof of Lemma B.2. Define $\overline{q}(X) = q(X) - \mathbb{E}_0[q(X)]$, then by (B.2), we have

$$\begin{aligned} \|q(X)\|_{\psi_1,0}\cdot\overline{\tau} &< \frac{1}{|\mathcal{C}^+(q)|}\sum_{S\in\mathcal{C}^+(q)} \{\mathbb{E}_S[\overline{q}(X)] - \mathbb{E}_0[\overline{q}(X)]\} \\ &= \mathbb{E}_0\left\{\overline{q}(X)\cdot\frac{1}{|\mathcal{C}^+(q)|}\sum_{S\in\mathcal{C}^+(q)}\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}(X) - 1\right]\right\}. \end{aligned}$$

Applying Cauch-Schwartz inequality on the right-hand side above gives

$$\|q(X)\|_{\psi_1,0}\cdot\tau < \underbrace{\{\mathbb{E}_{\mathbb{P}_0}[\overline{q}^2(X)]\}^{1/2}}_{\text{(i)}}\cdot\underbrace{\left(\mathbb{E}_{\mathbb{P}_0}\left\{\frac{1}{|\mathcal{C}^+(q)|}\sum_{S\in\mathcal{C}^+(q)}\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}(X)-1\right]\right\}^2\right)^{1/2}}_{\text{(ii)}}. \tag{C.1}$$

For term (i), by the definition of $\bar{q}(X)$ and ψ_1-norm we have

$$\begin{aligned}(\mathbb{E}_0\{[\overline{q}(X)]^2\})^{1/2} &= [\mathbb{E}_0(\{q(X)-\mathbb{E}_0[q(X)]\}^2)]^{1/2}\\ &\le \sup_{p\ge1} 2/p\cdot\{\mathbb{E}_0|q(X)-\mathbb{E}_0[q(X)]|^p\}^{1/p} = 2\|q(X)\|_{\psi_1,0}.\end{aligned} \tag{C.2}$$

For term (ii), we have

$$\begin{aligned}&\left[\mathbb{E}_0\left(\left\{\frac{1}{|\mathcal{C}^+(q)|}\sum_{S\in\mathcal{C}^+(q)}\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}(X)-1\right]\right\}^2\right)\right]^{1/2}\\ &=\left(\frac{1}{|\mathcal{C}^+(q)|^2}\sum_{S,S'\in\mathcal{C}^+(q)}\mathbb{E}_0\left\{\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}(X)-1\right]\cdot\left[\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)-1\right]\right\}\right)^{1/2}\\ &=\left\{\frac{1}{|\mathcal{C}^+(q)|^2}\sum_{S,S'\in\mathcal{C}^+(q)}\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}(X)\right]-1\right\}^{1/2}\end{aligned} \tag{C.3}$$

Plugging (C.2) and (C.3)into (C.1) together with $\tau=\sqrt{\frac{2}{n}}$, we obtain

$$\frac{1}{|\mathcal{C}^+(q)|^2}\sum_{S,S'\in\mathcal{C}^+(q)}\mathbb{E}_0\left[\frac{\mathrm{d}\mathbb{P}_S}{\mathrm{d}\mathbb{P}_0}\frac{\mathrm{d}\mathbb{P}_{S'}}{\mathrm{d}\mathbb{P}_0}\right] > 1+\frac{1}{n}.$$

Therefore we conclude the proof. □

References

[1] ARIAS-CASTRO, E., BUBECK, S. and LUGOSI, G. (2015). Detecting positive correlations in a multivariate sample. *Bernoulli* **21** 209–241.

[2] NEYKOV, M., LU, J. and LIU, H. (2016). Combinatorial inference for graphical models. *arXiv preprint arXiv:1608.03045* .

[3] VERSHYNIN, R. (2010). Introduction to the non-asymptotic analysis of random matrices. *arXiv preprint arXiv:1011.3027* .