Appendix

A. Proof of Theorem 3.1: Computational Lower Bound

For fixed parameter $\theta > 0$ and a given graph $G = (V, E)$, we denote the vector encoding G as $\boldsymbol{\theta} = (\theta_e) \in \mathbb{R}^d$ with $\theta_e = \theta$ for $e \in E(G)$ and $\theta_e = 0$ otherwise. For an edge set S, we denote its encoding vector similarly as $\boldsymbol{\theta}_S$. Moreover, we use $\mathbb{P}_0$ and $\mathbb{E}_0$ to denote the probability measure and expectation of ferromagnetic Ising model with no edges, and $\mathbb{P}_S$, $\mathbb{E}_S$ to denote the probability measure and expectation with encoding vector $\boldsymbol{\theta}_S$.

For statistical query oracle, for any $S \in \mathcal{E}$ and any $q \in \mathcal{Q}_{\mathscr{A}}$, when $|\mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)]|$ is larger than the statstical deviation of the oracle, it would be possible to tell $\boldsymbol{\theta}_S$ from $\boldsymbol{\theta}_0$. Based on this intuition, we define

$$\mathcal{C}(q) = \big\{S \in \mathcal{E} : |\mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)]| \geq \tau_{q,S}\big\},$$

where $\tau_{q,S}$ is defined in (3) with expectations taken under $\mathbb{P}_S$. The following lemma from (Fan et al., 2018) states that when $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{E}|$, there would be an oracle that none of the T rounds can distirbutish $\mathbb{P}_S$ from $\mathbb{P}_0$.

Lemma A.1. *For any algorithm $\mathscr{A}$ that queries the oracle r for at most T rounds, if $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)| < |\mathcal{E}|$, then there exists a statistical oracle r defined in definition 2.1 s.t.*

$$\liminf_{n \to \infty} \mathcal{R}_n(\{\boldsymbol{\theta}_0\}, \{\boldsymbol{\theta}_S\}_{S \in \mathcal{E}}, \mathscr{A}, \mathcal{O}, T) \geq 1.$$

By the above lemma, it suffices to show that $T \cdot \sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}(q)|/|\mathcal{E}|$ is asyptotically smaller than 1. To bound the term $|\mathcal{C}(q)|$, we split it to the following two sets

$$\mathcal{C}^+(q) = \big\{S \in \mathcal{E} : \mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)] > \tau_{q,S}\big\},$$

$$\mathcal{C}^-(q) = \big\{S \in \mathcal{E} : \mathbb{E}_S[q(X)] - \mathbb{E}_0[q(X)] < -\tau_{q,S}\big\}.$$

Then we have an upper bound for $\sup_{q \in \mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^+(q)|$, which is also presented in (Fan et al., 2018):

Lemma A.2. *For any query function q, we have*

$$\frac{1}{|\mathcal{C}^+(q)|^2} \sum_{S, S' \in \mathcal{C}^+(q)} \mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}_{S'}}{d\mathbb{P}_0}(X)\right] > 1 + \frac{2\log(T/\xi)}{3n}.$$

Therefore it remains to upper bound the likelihood ratio $\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}_{S'}}{d\mathbb{P}_0}(X)\right]$, for which we have the following lemma.

Lemma A.3. *For edge sets S and S' with $|V(S)|, |V(S')| \leq s$, if the parameter $\theta \geq 0$ satisfies $\theta < 1/(4s)$, we have an upper bound for the likelihood ratio*

$$\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}_{S'}}{d\mathbb{P}_0}(X)\right] \leq \exp\big(3|V_{S,S'}|^2\theta^2\big),$$

where $\mathbb{P}_S$, $\mathbb{P}_{S'}$ is the corresponding simple zero-field Ising probability measure with parameter θ for S and S'.

Proof of Lemma A.3. Recall that $V(S)$ denotes the vertex set of edge set S. In problems that interest us, we assume $\mathcal{G}_0 = \{(V, \varnothing\}$, and $|V(S)| = s$ for all $s \in \mathcal{E}$. Let Z_0, $Z_S(\theta)$ and $Z_{S'}(\theta)$ denote the partition function for $\mathbb{P}_0$, $\mathbb{P}_S$ and $\mathbb{P}_{S'}$, respectively. Therefore the likelihood ratio is

$$\begin{aligned}\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}'_S}{d\mathbb{P}_0}(X)\right] =& \frac{Z_0^2}{Z_S Z_{S'}}\mathbb{E}_0 \exp\Bigg(\sum_{(u,v)\in S}\theta_{uv}x_u x_v + \sum_{(s,t)\in S'}\theta_{st}x_s x_t\Bigg)\\ =& \frac{Z_0^2}{Z_S Z_{S'}}\mathbb{E}_0 \exp\Bigg(\sum_{(u,v)\in S\cap S'}2\theta_{uv}x_u x_v + \sum_{(s,t)\in S\triangle S'}\theta_{st}x_s x_t\Bigg).\end{aligned}$$

For simplicity, we reparametrize as μ_{uv} with $\mu_{uv} = 2\theta_{uv}$ if $(u, v) \in S \cap S'$ and $\mu_{uv} = \theta_{uv}$ otherwise. Therefore by definition of Z_S and $Z_{S'}$,

$$\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}'_S}{d\mathbb{P}_0}(X)\right] = \frac{Z_0^2}{Z_S Z_{S'}}\mathbb{E}_0 \exp\Big(\sum_{(u,v)\in S\cup S'} \lambda_{uv} x_u x_v\Big)$$
$$= \frac{\mathbb{E}_0 \exp\big(\sum_{(u,v)\in S\cup S'} \lambda_{uv} x_u x_v\big)}{\mathbb{E}_0 \exp\big(\sum_{(u,v)\in S} \theta_{uv} x_u x_v\big)\mathbb{E}_0 \exp\big(\sum_{(u,v)\in S'} \theta_{uv} x_u x_v\big)}.$$

We first look at the term $\mathbb{E}_0\big[\exp\big(\sum_{(u,v)\in S} \theta_{uv} x_u x_v\big)\big]$ for general $\widetilde{\boldsymbol{\theta}}$ and S. Using Taylor expansion of exponential function we know

$$\mathbb{E}_0\bigg[\exp\Big(\sum_{(u,v)\in S} \theta_{uv} x_u x_v\Big)\bigg] = 1 + \mathbb{E}_0\bigg[\sum_{k=1}^{\infty}\frac{1}{k!}\Big(\sum_{(u,v)\in S}\theta_{uv} x_u x_v\Big)^k\bigg].$$

Here the crossterms are

$$\frac{1}{k!}\Big(\sum_{(u,v)\in S}\theta_{uv} x_u x_v\Big)^k = \frac{1}{k!}\sum_{\sum_{i=1}^{|E(S)|} k_i = k} \theta_{u_1v_1}^{k_1}\cdots\theta_{u_sv_s}^{k_{|E(S)|}} x_1^{n_1}\cdots x_s^{n_s}\cdot\frac{k!}{\prod_{i=1}^{|E(S)|} k_i!}$$
$$= \sum_{\sum_{i=1}^{|E(S)|} k_i = k}\frac{\theta_{e_1}^{k_1}}{k_1!}\cdots\frac{\theta_{e_{|E(S)|}}^{k_{|E(S)|}}}{(k_{|E(S)|})!} x_1^{n_1}\cdots x_s^{n_s},$$

where $n_u = \sum_{v, e_j=(u,v)\in E(S)} k_j$ is the total times that x_u appears in the correlation terms $x_u x_v$.

Note that under $\mathbb{P}_0$, all vertices x_i are independent of each other and have expectation zero. Therefore $\mathbb{E}_0[x_1^{n_1}\cdots x_s^{n_s}] = 1$ if all n_i's are even, and $\mathbb{E}_0[x_1^{n_1}\cdots x_s^{n_s}] = 0$ otherwise. Let vector $\mathbf{k} = (k_1, \ldots, k_{|E(S)|})$ denote the vector of powers for each θ_{uv} in term $\theta_{u_1v_1}^{k_1}\cdots\theta_{u_sv_s}^{k_{|E(S)|}}$, in a given order. Define $\mathcal{K}$ to be the set of vectors

$$\mathcal{K} = \bigg\{(k_1, \ldots, k_{|E(S)|})\bigg|\sum_{v: e_j=(u,v)\in E(S)} k_j \text{ is even for all } u \in V(S)\bigg\},$$

which correspond to terms with nonzero expectations. Therefore

$$\mathbb{E}_0\left[\exp\left(\sum_{(u,v)\in S}\theta_{uv} x_u x_v\right)\right] = \sum_{\mathbf{k}\in\mathcal{K}}\frac{\theta_{e_1}^{k_1}}{k_1!}\cdots\frac{\theta_{e_{|E(S)|}}^{k_{|E(S)|}}}{k_{|E(S)|}!}.$$

Each term of the form $\theta_{u_1v_1}^{k_1}\cdots\theta_{u_sv_s}^{k_{|E(S)|}}$ corresponds to a graph where there could be multiple edges between any pair of vertices. Note that the graph with no edges also belong to this set. For $\mathbf{k} \in \mathcal{K}$, it corresponds to a graph where each node has even degree.

For clarity we define some notations. We call a graph where there are multiple edges between pairs of vertices as a *general praph*, and denote the set of general graphs over edge set S as $\mathcal{G}_S$. We call a graph where there is at most one edge between each pair of nodes as *simple graph*, and denote the set of simple graphs over edge set S as $\mathcal{S}_S$.

We reduce a general graph $\widetilde{G}$ to a simple graph G by canceling the edge (u, v) if it appears for even times and preserve it otherwise. Therefore we have a mapping $f : \mathcal{G}_S \mapsto \mathcal{S}_S$. Given $\widetilde{G} \in \mathcal{G}_S$, $f(\widetilde{G}) \in \mathcal{S}_S$ is called its *simple version*. Vice versa, $\widetilde{G}$ is the *general version* of $f(\widetilde{G})$. Clearly, for a general graph, its simple version is deterministic but a simple graph have infinitely many general versions. Also note that if $v \in E(\mathcal{G}_S)$ has even degree, after the mapping f, it still has even degree, and likewise for those vertices with odd degree. For a graph $G \in \mathcal{G}_S$, we denote its preimage as $f^{-1}(G)$, which is an infinite set. The vector $\mathbf{k}$, after the mapping, is in fact modulus 2 for each element.

Now return to our analysis. Each $\mathbf{k} \in \mathcal{K}$ corresponds to a general graph, where we do not distinguish $\mathbf{k}$ from the general graph, and since f does not change the parity of vertex degree, after the mapping the corresponding $\mathbf{k}$ still belongs to $\mathcal{K}$. For brevity we define the subset of $\mathcal{S}_S$ that each vertex has even degree to be $\mathcal{D}_S$, then

$$\mathbb{E}_0\left[\exp\left(\sum_{(u,v)\in S}\theta_{uv}x_ux_v\right)\right]=\sum_{\mathbf{k}\in\mathcal{K}}\frac{\theta_{e_1}^{k_1}}{k_1!}\cdots\frac{\theta_{e_{|E(S)|}}^{k_{|E(S)|}}}{k_{|E(S)|}!}=\sum_{G\in\mathcal{D}_S}\sum_{\mathbf{k}\in\mathcal{G}_S,f(\mathbf{k})=G}\frac{\theta_{e_1}^{k_1}}{k_1!}\cdots\frac{\theta_{e_{|E(S)|}}^{k_{|E(S)|}}}{k_{|E(S)|}!}.$$

For each $G\in\mathcal{D}_S$, all its general versions $\mathbf{k}\in\mathcal{G}_S$ can be obtained by adding even amounts of edges between each pair of nodes. Therefore

$$\mathbb{E}_0\left[\exp\left(\sum_{(u,v)\in S}\theta_{uv}x_ux_v\right)\right]=\sum_{G\in\mathcal{D}_S}\prod_{e_j\in E(G)}\left(\sum_{l_j=0}^{\infty}\frac{\theta_{e_j}^{2l_j+1}}{(2l_j+1)!}\right)\prod_{e_j\in S\setminus E(G)}\left(\sum_{l_j=0}^{\infty}\frac{\theta_{e_j}^{2l_j}}{(2l_j)!}\right),$$

which, by Taylor expansion can be written as

$$\begin{aligned}\mathbb{E}_0\left[\exp\left(\sum_{(u,v)\in S}\theta_{uv}x_ux_v\right)\right]&=\sum_{G\in\mathcal{D}_S}\left(\prod_{(u,v)\in E(G)}\sinh(\theta_{uv})\prod_{(u,v)\in S\setminus E(G)}\cosh(\theta_{uv})\right)\\&=\left(\prod_{(u,v)\in E(S)}\cosh(\theta_{uv})\right)\left(\sum_{G\in\mathcal{D}_S}\prod_{(u,v)\in E(G)}\tanh(\theta_{uv})\right).\end{aligned}$$

Plugging the above result into the likelihood we get

$$\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0}\frac{d\mathbb{P}_S'}{d\mathbb{P}_0}(X)\right]=\frac{\prod_{(u,v)\in S\cup S'}\cosh(\lambda_{uv})}{\left(\prod_{(u,v)\in S}\cosh(\theta_{uv})\right)\left(\prod_{(u,v)\in S'}\cosh(\theta_{uv})\right)}\tag{17}$$

$$\times\frac{\sum_{G\in\mathcal{D}_{S\cup S'}}\prod_{(u,v)\in G}\tanh(\lambda_{uv})}{\left(\sum_{G\in\mathcal{D}_S}\prod_{(u,v)\in E(G)}\tanh(\theta_{uv})\right)\left(\sum_{G\in\mathcal{D}_{S'}}\prod_{(u,v)\in E(G)}\tanh(\theta_{uv})\right)}.\tag{18}$$

In our setting where $\theta_{uv}=\theta\geq 0$, Equation (17) is actually

$$\frac{\prod_{(u,v)\in S\cup S'}\cosh(\lambda_{uv})}{\left(\prod_{(u,v)\in S}\cosh(\theta_{uv})\right)\left(\prod_{(u,v)\in S'}\cosh(\theta_{uv})\right)}=\prod_{(u,v)\in S\cap S'}\frac{\cosh(2\theta_{uv})}{\cosh(\theta_{uv})^2}=\left(\frac{2\left(e^{2\theta}+e^{-2\theta}\right)}{e^{2\theta}+e^{-2\theta}+2}\right)^{|S\cap S'|}.$$

And since $e^{2\theta}+e^{-2\theta}=2+4\theta^2+O(\theta^4)$, we have

$$\frac{2\left(e^{2\theta}+e^{-2\theta}\right)}{e^{2\theta}+e^{-2\theta}+2}=\frac{4+8\theta^2+O(\theta^4)}{4+4\theta^2+O(\theta^4)}\leq 1+2\theta^2\leq\exp(2\theta^2).$$

Therefore

$$\frac{\prod_{(u,v)\in S\cup S'}\cosh(\lambda_{uv})}{\left(\prod_{(u,v)\in S}\cosh(\theta_{uv})\right)\left(\prod_{(u,v)\in S'}\cosh(\theta_{uv})\right)}\leq\exp\left(2|S\cap S'|\theta^2\right)\leq\exp\left(|\mathcal{V}_{S,S'}|^2\theta^2\right).\tag{19}$$

It remains to bound the second term in Equation (18). We obtain an upper bound by deleting edges in $S\cup S'$ and then bound the remaining term for the case $S\cup S'=\varnothing$. Before dealing with Equation (18), we first consider the general case

$$\mathcal{W}(S):=\sum_{G\in\mathcal{D}_S}\prod_{(u,v)\in G}\tanh(\lambda_{uv})=\sum_{G\in\mathcal{D}_S}W(G),\tag{20}$$

where for a simple graph G with edge parameter (λ_{uv}) we define its weight as $W(G)=\prod_{(u,v)\in E(G)}\tanh(\lambda_{uv})$. For brevity, denote $t_{uv}:=\tanh(\lambda_{uv})$.

We are interested in how Equation (20) would change if we delete (or inversely add) an edge in S. Suppose we add an edge (u,v) into S where $u,v\in V(S)$. Denote $\widetilde{S}=S\cup\{(u,v)\}$. Then

$$\mathcal{W}(\widetilde{S})=\mathcal{W}(S)+\sum_{G\in\mathcal{D}_{\widetilde{S}}\setminus\mathcal{D}_S}W(G)=\mathcal{W}(S)+\sum_{G\in\mathcal{D}_{\widetilde{S}},(u,v)\in E(G)}W(G).$$

Thus it remains to upper bound the new components: the sum of weights of those simple graphs containing the edge (u, v). To properly categorize the simple graphs in $\mathcal{D}_{\widetilde{S}} \backslash \mathcal{D}_S$, note that for any simple graph G with even vertex degrees, it can be separated into the union of several cycles. The separation may be not unique, but for all $\widetilde{G} \in \mathcal{D}_{\widetilde{S}}$ with $(u, v) \in \widetilde{G}$, the edge (u, v) must be contained in some cycle C of length $l + 2$, $l \geq 1$. The cycle can be represented by a sequence of vertices $C = (u, v, u_1, \ldots, u_l)$ with no repetition. If we cancel all edges in cycle C from G, we would end up with a graph $G \in \mathcal{D}_S$, since the edge (u, v) is deleted, and the degree of all vertices are still even. We further look at the cycle C. In fact, it consists of edge (u, v) and a path $P = \{(u, v), (v, u_1), \ldots, (u_{l-1}, u_l), (u_l, u)\}$ connecting u and v, where all edges in P belongs to S. We denote the set of all paths connecting u and v in S as $\mathcal{P}_{uv}(S)$, and denote $W(P) = \prod_{e \in P} t_e$. In this way, we obtain a map

$$m : \mathcal{D}(\widetilde{S}) \backslash \mathcal{D}(S) \to \mathcal{D}(S) \times \mathcal{P}_{uv}(S) : \quad \widetilde{G} \mapsto (G, P),$$

where G is obtained from $\widetilde{G}$ by deleting a cycle $C = (u, v) \cup P$. The cycle to be deleted may be not unique, but we can fix it for each $\widetilde{G} \in \mathcal{D}(\widetilde{S}) \backslash \mathcal{D}(S)$ beforehand. In this way, for each $\widetilde{G} \in \mathcal{D}(\widetilde{S}) \backslash \mathcal{D}(S)$, we have

$$W(\widetilde{G}) = W(G) \cdot \prod_{e \in E(C)} t_e = t_{uv} \cdot W(G) \cdot \prod_{e \in P} t_e = t_{uv} \cdot W(G) W(P),$$

where C is the canceled cycle and $m(\widetilde{G}) \in \mathcal{D}_S$. Moreover, the map m is injective, since when given $G \in \mathcal{D}(\widetilde{S}) \backslash \mathcal{D}(S)$ and $C \in \mathcal{P}_{uv}(S)$, the preimage $\widetilde{(G)}$ is obviously determined. Since all parameters for the edges are nonnegative,

$$\begin{aligned}
\sum_{\widetilde{G} \in \mathcal{D}_{\widetilde{S}}, (u,v) \in E(\widetilde{G})} W(\widetilde{G}) &= t_{uv} \cdot \sum_{\widetilde{G} \in \mathcal{D}_{\widetilde{S}}, (u,v) \in E(\widetilde{G})} W(m_1(G)) \cdot W(m_2(G)) \\
&\leq t_{uv} \cdot \Big(\sum_{G \in \mathcal{D}_S} W(G) \Big) \Big(\sum_{P \in \mathcal{P}_{uv}(S)} W(P) \Big) \\
&= t_{uv} \cdot \mathcal{W}(S) \cdot \Big(\sum_{P \in \mathcal{P}_{uv}(S)} W(P) \Big).
\end{aligned}$$

Hence

$$\mathcal{W}(\widetilde{S}) \leq \mathcal{W}(S) \Big(1 + t_{uv} \sum_{P \in \mathcal{P}_{uv}(S)} W(P) \Big). \tag{21}$$

We proceed to bound the summation in Equation (21). Note that $(u, v) \notin S$, so the length of any path in $\mathcal{P}_{uv}(S)$ is at least 2. Suppose $0 \leq t_{uv} \leq t$ for some fixed t and any $(u, v) \in S$, then

$$\sum_{P \in \mathcal{P}_{uv}(S)} W(P) = \sum_{l=2}^{\infty} \sum_{P \in \mathcal{P}_{uv}(S), |P| = l} W(P) \leq \sum_{l=2}^{\infty} \sum_{P \in \mathcal{P}_{uv}(S), |P| = l} t^l = \sum_{l=2}^{\infty} N_{uv}(S, l) \cdot t^l.$$

Here $N_{uv}(S, l) = |\{P \in \mathcal{P}_{uv}(S) : P \text{ is of length } l\}|$ the number of paths connecting u and v in S with length l.

We upper bound Equation (21) by comparing the sequence $N_{uv}(S, l)$ to a geometric sequence. Suppose there exists some $\alpha_{uv}(S)$, $\beta_{uv}(S)$ such that $t \cdot \beta_{uv}(S) < c$ for some $c < 1$, then

$$N_{uv}(S, l) \leq \alpha_{uv}(S) \cdot \beta_{uv}(S)^l$$

for all $l \geq 2$, then we have

$$\mathcal{W}(\widetilde{S}) \leq \mathcal{W}(S) \Big(1 + t_{uv} \sum_{P \in \mathcal{P}_{uv}(S)} W(P) \Big) \leq \mathcal{W}(S) \Big(1 + \frac{\alpha_{uv}(S) \beta_{uv}(S)^2 t^3}{1 - \beta_{uv}(S) t} \Big).$$

We could choose $\alpha_{uv}(S)$ and $\beta_{uv}(S)$ to be a uniform value over all S. Specifically, a path in S of length l consist of consecutive edges connecting u, v and $(l - 1)$ other distinct vertices in $V(S)$. Therefore we have $N_{uv}(S, l) \leq |V(S)|^{l-1}$. Therefore we could fix $\alpha_{uv}(S) = 1/|V(S)|$ and $\beta_{uv}(S) = |V(S)|$. Hence if $t \cdot |V(S)| < c_1 < 1$, we will have

$$\mathcal{W}(\widetilde{S}) \leq \mathcal{W}(S) \Big(1 + \frac{\alpha_{uv}(S) \beta_{uv}(S)^2 t^3}{1 - \beta_{uv}(S) t} \Big) \leq \mathcal{W}(S) \Big(1 + \frac{|V(S)| t^3}{1 - |V(S)| t} \Big) \leq \mathcal{W}(S) \big(1 + c t^2 \big), \tag{22}$$

where $c > 0$ is a constant.

Based on Equation (22), we could upper bound Equation (18) as follows. At each time, we delete an edge $e = (u, v)$ with $u, v \in \mathcal{V}_{S,S'}$, then if for all $u, v \in V(S) \cap V(S')$, $\tanh(\lambda_{uv}) \le t$ and $t \cdot |S \cup S'| \le c_1$ for some $0 < c_1 < 1$, we have

$$\sum_{G \in \mathcal{D}_{S \cup S'}} \prod_{(u,v) \in G} \tanh(\lambda_{uv}) = \mathcal{W}(S \cup S') \le \mathcal{W}(S \triangle S') \cdot (1 + ct^2)^{|S \cap S'|},$$

for some constant $c > 0$. Here $S \triangle S'$ denotes the set obtained from $S \cup S'$ by deleting all aforementioned edges. In this way, $S \triangle S'$ contains no edge with vertices all in $\mathcal{V}_{S,S'}$.

It is obvious that the number of such edges (u, v) with $u, v \in \mathcal{V}_{S,S'}$ is less than $|\mathcal{V}_{S,S'}|^2/2$, therefore

$$\sum_{G \in \mathcal{D}_{S \cup S'}} \prod_{(u,v) \in G} \tanh(\lambda_{uv}) \le \mathcal{W}(S \triangle S') \exp(c|\mathcal{V}_{S,S'}|^2 t^2).$$

For brevity we denote $\widetilde{S} := S \backslash S'$ and $\widetilde{S}' := S' \backslash S$. Since deleting an edge reduces the summation of the weights of all its simple graph with even node degrees, we have

$$\begin{aligned}
&\frac{\sum_{G \in \mathcal{D}_{S \cup S'}} \prod_{(u,v) \in G} \tanh(\lambda_{uv})}{\Big(\sum_{G \in \mathcal{D}_S} \prod_{(u,v) \in E(G)} \tanh(\theta_{uv})\Big)\Big(\sum_{G \in \mathcal{D}_{S'}} \prod_{(u,v) \in E(G)} \tanh(\theta_{uv})\Big)} \\
&\le \frac{\mathcal{W}(\widetilde{S} \triangle \widetilde{S}')}{\mathcal{W}(\widetilde{S}) \cdot \mathcal{W}(\widetilde{S}')} \cdot \exp(c|\mathcal{V}_{S,S'}|^2 t^2) = \frac{\mathcal{W}(\widetilde{S} \cup \widetilde{S}')}{\mathcal{W}(\widetilde{S}) \cdot \mathcal{W}(\widetilde{S}')} \cdot \exp(c|\mathcal{V}_{S,S'}|^2 t^2). \qquad (23)
\end{aligned}$$

In our case, we can choose $t = \tanh(2\theta) \le 2\theta$ for $0 \le \theta \le 1/(4s)$. Then we could set $c_1 = 1/2$ and $c = 1$. Thus it remains to bound the term $\frac{\mathcal{W}(\widetilde{S} \cup \widetilde{S}')}{\mathcal{W}(\widetilde{S}) \cdot \mathcal{W}(\widetilde{S}')}$ for disjoint $\widetilde{S}$ and $\widetilde{S}'$. We consider the general case for $S \cap S' = \varnothing$.

For future use, for edge sets S, S' with $S \cap S' = \varnothing$ and $\{(u, v) \in S \cup S' | u, v \in V(S) \cap V(S')\} = \varnothing$, we denote $\mathcal{D}(S, S') = \mathcal{D}(S \cup S')$ and the set

$$\mathcal{F}(S, S') := \big\{G \in \mathcal{D}(S, S') \,|\, G \text{ contains no cycle } C \subset S \text{ or } C \subset S'\big\},$$

with $\varnothing \in \mathcal{F}(S, S')$ and

$$\mathcal{H}(S, S') := \Big\{G = \bigcup_j C_j \,|\, C_j \text{ are cycles, } C_j \subset S \text{ or } C_j \subset S'\Big\},$$

with $\varnothing \in \mathcal{H}(S, S')$. This means that for all possible loops in $G \in \mathcal{F}(S, S')$ (since the way we separate loops in G may be not unique), they can not consist merely of edges in S or S'. And for $G \in \mathcal{H}(S, S')$, G can be decomposed into the union of cycles in S or in S', i.e. for any $G \in \mathcal{H}(S, S')$, it can be decomposed as $G = G_1 \cup G_2$ where $G_1 \in \mathcal{D}(S)$ and $G_2 \in \mathcal{D}_{S'}$. It corresponds to a mapping

$$m' : \mathcal{H}(S, S') \to \mathcal{D}(S) \times \mathcal{D}(S'). \qquad (24)$$

Clearly m' is bijection. Also, recall that for any simple graph G with even vertex degrees, it can be decomposed into the union of several cycles $C_1, \ldots, C_r$ with no overlapping edges in a certain way. For $G \in \mathcal{D}(S \cup S')$, we decompose it into as many loops in $\mathcal{H}(S, S')$ as possible. Therefore $G = G_1 \cup G_2$ where $G_1 \cap G_2 = \varnothing$, meanwhile $G_1 \in \mathcal{F}(S, S')$ and $G_2 \in \mathcal{H}(S, S')$. In this way we obtain a mapping

$$m'' : \mathcal{D}(S, S') \to \mathcal{F}(S, S') \times \mathcal{H}(S, S') \qquad (25)$$

if we prefix the way we decompose a certain G. It is obvious that m'' is injective.

Since $S \cap S' = \varnothing$, we have $\lambda_{uv} = \theta_{uv}$ for all $(u, v) \in S \cup S'$. Therefore for brevity we denote

$$\begin{aligned}
\mathcal{R}(S, S') := \frac{\mathcal{W}(S \triangle S')}{\mathcal{W}(S) \cdot \mathcal{W}(S')} &= \frac{\sum_{G \in \mathcal{D}(S,S')} W(G)}{\Big(\sum_{G \in \mathcal{D}(S)} W(G)\Big)\Big(\sum_{G \in \mathcal{D}(S')} W(G)\Big)} \\
&= \frac{\sum_{\substack{G = G_1 \sqcup G_2 \in \mathcal{D}(S,S'),\\ G_1 \in \mathcal{F}(S,S'), G_2 \in \mathcal{H}(S,S')}} W(G_1) W(G_2)}{\Big(\sum_{G \in \mathcal{D}(S)} W(G)\Big)\Big(\sum_{G \in \mathcal{D}(S')} W(G)\Big)},
\end{aligned}$$

where $\sqcup$ denotes nonoverlapping union. Clearly the sum over the weights $W(G_1)W(G_2)$ where $G = G_1 \sqcup G_2 \in \mathcal{D}(S, S')$ with $G_1 \in \mathcal{F}(S, S')$, $G_2 \in \mathcal{H}(S, S')$ is bounded by the sum of $W(G_1)W(G_2)$ of all pairs $G_1 \in \mathcal{F}(S, S')$, $G_2 \in \mathcal{H}(S, S')$. Therefore

$$\begin{aligned}\mathcal{R}(S, S') \le& \frac{\left(\sum_{G_1\in\mathcal{F}(S,S')} W(G_1)\right)\left(\sum_{G_2\in\mathcal{H}(S,S')} W(G_2)\right)}{\left(\sum_{G\in\mathcal{D}(S)} W(G)\right)\left(\sum_{G\in\mathcal{D}(S')} W(G)\right)}\\ =& \frac{\left(\sum_{G_1\in\mathcal{F}(S,S')} W(G_1)\right)\left(\sum_{G_2\in\mathcal{H}(S,S')} W(m'(G_2)_1)W(m'(G_2)_2)\right)}{\left(\sum_{G\in\mathcal{D}(S)} W(G)\right)\left(\sum_{G\in\mathcal{D}(S')} W(G)\right)}.\end{aligned}$$

Here the second term in the numerator, the summation of the products of the weights of two graphs $m'(G_2)_1$ and $m'(G_2)_2$ can be bounded by the product of the summations of all such graph weights, i.e.

$$\mathcal{R}(S, S') \le \frac{\left(\sum_{G_1\in\mathcal{F}(S,S')} W(G_1)\right)\left(\sum_{G\in\mathcal{D}(S)} W(G))\right)\left(\sum_{G\in\mathcal{D}(S')} W(G))\right)}{\left(\sum_{G\in\mathcal{D}(S)} W(G)\right)\left(\sum_{G\in\mathcal{D}(S')} W(G)\right)} = \sum_{G\in\mathcal{F}(S,S')} W(G). \tag{26}$$

Note that in this way, $G_0 = \varnothing \in \mathcal{F}(S, S')$ with $W(G_0) = 1$. So it remains to bound Equation (26).

Before dealing with Equation (26), we first look at some properties of elements in $\mathcal{F}(S, S')$. For clarity, we call a cycle C with $C \cap S \neq \varnothing$ and $C \cap S' \neq \varnothing$ a *mixed loop*, and denote the set of all such cycle as $\mathcal{M}(S, S')$. Note that for $M \in \mathcal{M}(S, S')$, we can separate it into several paths in either S or S', with the endpoints of each path belonging to $\mathcal{V}_{S,S'}$. It means

$$M = \left(\cup_j P_j^S\right) \cup \left(\cup_j P_j^{S'}\right),$$

where $P_j^S \in \mathcal{P}_{uv}(S)$ and $P_j^{S'} \in \mathcal{P}_{uv}(S')$ with $u, v \in \mathcal{V}_{S,S'}$. Since there are no edges (u, v) such that $u, v \in \mathcal{V}_{S,S'}$, all P_j^S and $P_j^{S'}$ are of length $l \ge 2$. We pick out the endpoints of these paths sequentially as $\{u_1, \ldots, u_r\} \subset \mathcal{V}_{S,S'}$, where the path connecting u_1 and u_2 belongs to S.

Each mixed cycle M can be cut into two paths connecting u_1 and u_2 with length ≥ 2. Therefore, for each graph $F = \bigcup M_j \in \mathcal{F}(S, S')$ with cycles M_j's having no overlapping edges, each mixed cycle M_j can be cut into two paths in the aforementioned way. On the other side, given $u, v \in \mathcal{V}_{S,S'}$, for any $F \in \mathcal{F}(S, S')$, there can be at most one mixed cycle in F that is cut off at u, v, since otherwise there would be two non-overlapping paths in S that connects u and v that forms a cycle in S. This contradicts with the fact that there is no cycle contained entirely in S. Therefore

$$\begin{aligned}\sum_{F\in\mathcal{F}(S,S')} W(F) =& \sum_{F\in\mathcal{F}(S,S')} \prod_{F=\sqcup M_j} W(M_j)\\ =& \sum_{F\in\mathcal{F}(S,S')} \Big(\prod_{\substack{F=\sqcup M_j\\ M_j=P_{j1}\cup P_{j2}}} W(P_{j1})W(P_{j2})\Big),\end{aligned} \tag{27}$$

where the weight of each mixed cycle M_j is decomposed as the product of the weights of two sub-paths, where $P_{j1}, P_{j2} \in \mathcal{P}_{uv}(S \triangle S')$.

Similar to former arguments, the right-handed summation in Equation (27) of the products of two sub-paths can be bounded by the product of summations of such sub-paths, i.e.

$$\sum_{F\in\mathcal{F}(S,S')} W(F) \le \prod_{(u,v)\in\mathcal{V}_{S,S'}\times\mathcal{V}_{S,S'}} \left[1 + \Big(\sum_{P_1\in\mathcal{P}_{uv}(S\triangle S')} W(P_1)\Big)\cdot\Big(\sum_{P_2\in\mathcal{P}_{uv}(S\triangle S')} W(P_2)\Big)\right],$$

where the upper bound is obtained by considering all graphs in $\mathcal{F}(S, S')$ that contain a mixed cycle which cuts at u, v. And the 1 in the product corresponds to the case when no mixed cycle cuts at u, v. Similar to previous statements, since paths $P_1 \in \mathcal{P}_{uv}(S \triangle S')$ are of length at least 2 since there is no edge with both nodes in $S \cap S'$, if $t_{ij} \le t$ for all $(i, j) \in S \triangle S'$, we have

$$\sum_{P_1\in\mathcal{P}_{uv}(S\triangle S')} W(P_1) \le \alpha_{uv}(S \triangle S')\beta_{uv}(S \triangle S')^2 t^2. \tag{28}$$

Still in our case of $\widetilde{S} \triangle \widetilde{S}'$, we can choose parameters in Equation (28) to be $\beta_{uv}(S \triangle S') = 2s \geq |S \triangle S'|$ and $\beta_{uv} = 1/(2s)$. Therefore if $0 < t \leq 1/(4s)$, we will have

$$\sum_{F \in \mathcal{F}(S,S')} W(F) \leq \prod_{(u,v) \in \mathcal{V}_{S,S'} \times \mathcal{V}_{S,S'}} \left[1 + \left(\frac{\alpha_{uv}(S \triangle S') \cdot \beta_{uv}(S \triangle S') t^2}{1 - \beta_{uv}(S \triangle S')t}\right)^2\right]$$

$$= \left[1 + \left(\frac{2st^2}{1/2}\right)^2\right]^{|\mathcal{V}_{S,S'}|^2/2} \leq \left[1 + t^2\right]^{|\mathcal{V}_{S,S'}|^2/2} \leq \exp\left(|\mathcal{V}_{S,S'}|^2 t^2\right). \tag{29}$$

Combining Equations (23), (26), (29), we have that if $\theta \leq 1/(4s)$, we have

$$\frac{\sum_{G \in \mathcal{D}_{S \cup S'}} \prod_{(u,v) \in G} \tanh(\lambda_{uv})}{\left(\sum_{G \in \mathcal{D}_S} \prod_{(u,v) \in E(G)} \tanh(\theta_{uv})\right) \left(\sum_{G \in \mathcal{D}_{S'}} \prod_{(u,v) \in E(G)} \tanh(\theta_{uv})\right)} \leq \exp\left(2|\mathcal{V}_{S,S'}|^2 \theta^2\right). \tag{30}$$

Then combining Equations (19) and (30), we have that

$$\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0} \frac{d\mathbb{P}'_S}{d\mathbb{P}_0}(X)\right] \leq \exp\left(3|\mathcal{V}_{S,S'}|^2 \theta^2\right),$$

which completes the proof. □

By Lemma A.3, since $\exp(x) \leq 1 + 2x$ for $x \leq 1/2$ and $3|\mathcal{V}_{S,S'}|^2\theta^2 \leq 3s^2\theta^2 < 1/2$, we have

$$\mathbb{E}_0\left[\frac{d\mathbb{P}_S}{d\mathbb{P}_0} \frac{d\mathbb{P}'_S}{d\mathbb{P}_0}(X)\right] \leq \exp\left(3|\mathcal{V}_{S,S'}|^2 \theta^2\right) \leq 1 + 6|\mathcal{V}_{S,S'}|^2\theta^2.$$

Then by Lemma A.2, we have

$$\frac{2\log(T/\xi)}{3n} < \frac{1}{|\mathcal{C}^+(q)|^2} \sum_{S,S' \in \mathcal{C}^+(q)} 6|\mathcal{V}_{S,S'}|^2\theta^2 \leq \sup_{S \in \mathcal{E}} \frac{1}{|\mathcal{C}^+(q)|} \sum_{S' \in \mathcal{C}^+(q)} 6|\mathcal{V}_{S,S'}|^2\theta^2. \tag{31}$$

For $j = 0, \ldots, s$ and $S \in \mathcal{E}$, define $m_j = |\{S' \in \mathcal{E} : |\mathcal{V}(S,S')| = s - j\}|$. Then we have $\sum_{j=0}^{s} m_j = |\mathcal{E}| > |\mathcal{C}^+(q)|$. Then there exists integer $l^+(q) \geq 1$ s.t.

$$\sum_{j=0}^{l^+(q)} m_j > |\mathcal{C}^+(q)| \geq \sum_{j=0}^{l^+(q)-1} m_j. \tag{32}$$

For clarity, we define

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

Note that $h(j) := 6(s-j)^2\theta^2$ is a decreasing function of j, and that the term $\sum_{S' \in \mathcal{C}^+(q)} 6|\mathcal{V}_{S,S'}|^2\theta^2$ is the sum of $m_1 + \cdots + m_{l^+(q)-1} + \overline{m}$ terms, which m_j terms equal $h(j)$. Therefore from Equation (31),

$$\frac{2\log(T/\xi)}{3n} < \frac{\sum_{j=0}^{l^+(q)-1} h(j) \cdot m_j + h(l^+(q)) \cdot \overline{m}^+}{\sum_{j=0}^{l^+(q)-1} m_j + \overline{m}^+} \leq \frac{\sum_{j=0}^{l^+(q)-1} h(j) \cdot m_j}{\sum_{j=0}^{l^+(q)-1} m_j}.$$

By definition of the vertex overlap ratio ζ, for $i < j$ we have $m_i\zeta^j - m_j\zeta^i < 0$ and $h(i) - h(j) > 0$. Therefore

$$\sum_{1 \leq i < j \leq l^+(q)-1} (m_i\zeta^j - m_j\zeta^i)[h(i) - h(j)] \leq 0. \tag{33}$$

Hence we have

$$\frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot m_j}{\sum_{j=0}^{l^+(q)-1} m_j} \leq \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot \zeta^j}{\sum_{j=0}^{l^+(q)-1} \zeta^j} \leq \frac{\sum_{j=0}^{l^+(q)-1} h(j)\cdot \zeta^{-(s-j)}}{\sum_{j=0}^{l^+(q)-1} \zeta^{-(s-j)}}. \tag{34}$$

Note that $\zeta \geq c^{1/2}$ for d large enough and some constant $c < 1$. Therefore for $x = \zeta^{-1} \leq c^{-1/2}$, we have

$$\sum_{i=s-l+1}^{s} i^2 x^i \leq \sum_{i=1}^{\infty}(i+1)(i+2)x^i \leq 2\bar{c}^3(s-l+3)^2 x^{s-l+1}, \tag{35}$$

where $\bar{c} = \sqrt{c}/(\sqrt{c}-1)$. Combining Equations (33), (34), (35) we obtain

$$\frac{2\log(T/\xi)}{3n} \leq 12\bar{c}^3(s-l^+(q)+3)^2\theta^2.$$

Therefore for d large enough, we have

$$s - l^+(q) \geq \sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3. \tag{36}$$

On the other hand, by the definition of $\mathcal{C}^+(q)$ in Equation (32),

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^+(q)| \leq \sum_{j=0}^{l^+(q)} m_j \leq m_s \cdot \sum_{j=0}^{l^+(q)} \zeta^{j-s} \leq \frac{\zeta^{-[s-l^+(q)]}\cdot|\mathcal{E}|}{1-\zeta^{-1}} \leq 2\bar{c}\zeta^{-[s-l^+(q)]}\cdot|\mathcal{E}|. \tag{37}$$

Combining Equations (36) and (37) we have

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^+(q)| \leq \bar{c}\cdot|\mathcal{E}|\cdot\exp\biggl[-\log(\zeta)\cdot\biggl(\sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3\biggr)\biggr].$$

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

$$\sup_{q\in\mathcal{Q}_{\mathscr{A}}} |\mathcal{C}^-(q)| \leq \bar{c}\cdot|\mathcal{E}|\cdot\exp\biggl[-\log(\zeta)\cdot\biggl(\sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3\biggr)\biggr].$$

Therefore

$$T\cdot\frac{\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|}{|\mathcal{E}|} \leq 2\bar{c}\cdot\exp\biggl[\log T - \biggl(\sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3\biggr)\cdot\log\zeta\biggr].$$

Then for polynomial computational budget with $T \leq d^\eta$ for some fixed $\eta > 0$, we have

$$T\cdot\frac{\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|}{|\mathcal{E}|} \leq \exp\biggl[\log(2\bar{c}) + \eta\log d - \biggl(\sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3\biggr)\cdot\log\zeta\biggr].$$

Let $\kappa = [(\eta+1)\vee 3]^{-1}(18\bar{c}^3)^{-1/2}$. Under the condition that

$$\theta \leq \kappa\frac{\log\zeta}{\log d + \log\zeta}\sqrt{\frac{\log(1/\xi)}{n}},$$

for d large enough, we have

$$\log(2\bar{c}) + \eta\log d - \biggl(\sqrt{\frac{\log(T/\xi)}{18\bar{c}^3\theta^2 n}} - 3\biggr)\cdot\log\zeta \leq -1,$$

indicating that $T\cdot\sup_{q\in\mathcal{Q}_{\mathscr{A}}}|\mathcal{C}(q)|/|\mathcal{E}| < 1$. Then by Lemma A, there exists an oracle r s.t. $\liminf_{n\to\infty}\mathcal{R}_n(\{\boldsymbol{\theta}_0\},\{\boldsymbol{\theta}_S\}_{S\in\mathcal{E}},\mathscr{A},\mathcal{O},T) \geq 1$, which completes the proof of the theorem.

B. Proof of Computational Upper Bounds

In this section we prove the computational upper bounds for different property testing problems provided in Section 3.2. They are all attained by the correlation query functions and test function in Equations (9) and (10).

B.1. Proof of Theorem 3.2: General Computational Upper Bound

In this section we prove the general computational upper bound provided in Theorem 3.2. The computational upper bound for perfect matching in Corollay 3.4 is just an application of it. We also use the Bernstein-type bound the deviation of the returned query functions $q_{jk} = \widehat{\mathbb{E}} X_j X_k$.

Since by FKG inequality in (Alon & Spencer, 2004) or Griffiths second inequality in (Griffiths, 1967), pruning edges reduces the correlation, for $\theta > 0$ and all pairs $(u, v) \in E(G)$ with $1 \le u < v \le d$, the correlation is larger than that of a single edge, i.e.

$$\mathbb{E}[X_u X_v] \ge \frac{e^\theta - e^{-\theta}}{e^\theta + e^{-\theta}} = \tanh(\theta),$$

and the variance of correlation for all pairs (u, v) with $1 \le u < v \le d$,

$$\text{Var}(X_u X_v) = 1 - (\mathbb{E}[X_u X_v])^2 \le 1.$$

Therefore by the concentration property of the oracle computational model, with probability at least $1 - 2\xi$,

$$\max_{1 \le u < v \le d} |q_{uv}(X) - \mathbb{E}[X_u X_v]| \le \max\left\{\frac{2}{3n}\log\left(\frac{d(d-1)}{2\xi}\right), \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}\right\}, \tag{38}$$

where the variance terms are substituted with an upper bound 1. Therefore under $\mathbf{H}_0$, since $\log(d)/n = o(1)$, with probability at least $1 - 2\xi$,

$$\max_{1 \le u < v \le d} q_{uv}(X) \le \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}.$$

Then according to the test given by Equation (10), we have

$$\sup_{\boldsymbol{\theta} \in \mathcal{C}_0} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 1] \le 2\xi.$$

On the other hand, under $\mathbf{H}_1$ with some $S \in \mathcal{C}_1$, we know that with probability at least $1 - 2\xi$, for $(j, k) \in E(S)$, we have

$$q_{jk}(X) \ge \mathbb{E}[X_j X_k] - \tau_q(s, \theta) \ge \tanh(\theta) - \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)} \ge \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)},$$

since for sufficiently small x, $\tanh(x) \ge x/2$. Therefore

$$\sup_{\boldsymbol{\theta} \in \mathcal{C}_1} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 0] \le 2\xi, \sup_{\boldsymbol{\theta} \in \mathcal{C}_0} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 1] + \sup_{\boldsymbol{\theta} \in \mathcal{C}_1} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 0] \le 4\xi,$$

which completes the proof.

B.2. Proof of Theorem 3.3: Computational Upper Bound for Clique Detection

In this section we prove the computational upper bound for clique detection problem provided in Theorem 3.3. We first define some notations. In s-clique detection problem, each $S \in \mathcal{C}_1$ is a graph of s-clique, i.e. $V(S) \subset [d]$, $V(S) = s$, $|S| = s(s-1)/2$, which corresponds to parameter vector $\boldsymbol{\theta}_S = (\theta_e)$ where $\theta_e = \theta$ if $e \in S$ and $\theta_e = 0$ otherwise. Therefore the probability measure $\mathbb{P}_S$ is the same for all $S \in \mathcal{C}_1$ up to a permutation of vertices. We can define the expected correlation as

$$E_2(s, \theta) := \mathbb{P}_S[X_j X_k], \quad (j, k) \in S.$$

Therefore Var$(q_{ij}(X)) = 1 - E_2(s, \theta)^2$ if $(j,)$ is an edge in an s-clique. Our proof for Theorem 3.3 depend on the following lemmas.

Lemma B.1. *For $S \in \mathcal{C}_1$ an s-clique, we have*

$$E_2(s,\theta) = 1 - 4 \cdot \frac{\sum_{k=0}^{s} k(s-k) C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^{s} s(s-1) C_s^k e^{-2k(s-k)\theta}}. \tag{39}$$

Proof. For s-clique S, without loss of generality we assume $S = [s]$, then by symmetry

$$\begin{aligned} E_2(s,\theta) =& \mathbb{P}[X_j X_k = 1] - \mathbb{P}[X_j X_k = -1] \\ =& 1 - 2\mathbb{P}[X_j X_k = -1] = 1 - 4\mathbb{P}[X_j = 1, X_k = -1], \end{aligned}$$

where

$$\mathbb{P}[X_j = 1, X_k = -1] = \frac{\sum_{\mathbf{x}\in\{\pm 1\}^d, x_j = 1, x_k = -1} \exp\left(\theta \sum_{(u,v)\in S} x_u x_v\right)}{\sum_{\mathbf{x}\in\{\pm 1\}^d} \exp\left(\theta \sum_{(u,v)\in S} x_u x_v\right)}. \tag{40}$$

For the numerator in Equation (40), it consists of all terms such that $x_j = 1, x_k = -1$. We categorize them by the number of vertices $u \in [s] \backslash \{j,k\}$ that take value of 1. If there are m vertices other than j,k equals 1, the exponential term is

$$\exp\left\{\frac{\theta}{2}\Big(m(m-1) + (s-m-2)(s-m-3) - 2\Big)\right\}.$$

Therefore

$$\sum_{\substack{\mathbf{x}\in\{\pm 1\}^d,\\ x_j = 1, x_k = -1}} \exp\Big(\theta \sum_{(u,v)\in S} x_u x_v\Big) = \sum_{m=0}^{s-2} C_{s-2}^m \exp\left\{\frac{\theta}{2}\Big(m(m-1) + (s-m-2)(s-m-3) - 2\Big)\right\}.$$

Categorizing terms in the denominator in Equation (40), we have

$$\sum_{\mathbf{x}\in\{\pm 1\}^d} \exp\Big(\theta \sum_{(u,v)\in S} x_u x_v\Big) = \sum_{m=0}^{s} C_s^k \exp\left\{\frac{\theta}{2}\Big(m(m-1) + (s-m)(s-m-2) - 2m(s-m)\Big)\right\}.$$

Plugging them into Equation (40), we obtain the desired formula. □

Lemma B.2. *For $E_2(s,\theta)$ defined before with $\theta > 0$, we have $E_2(s,\theta) \geq \theta$.*

Proof. By FKG inequality, for simple zero-field ferromagnetic Ising model, deleting an edge reduces the correlation $\mathbb{E}_S[X_j X_k]$. Therefore the correlation under s-clique is larger than that of 2-clique for $s \geq 2$

$$E_2(s,\theta) \geq E_2(2,\theta) = 1 - 4 \cdot \frac{2e^{-2\theta}}{2(1 + 2e^{-2\theta} + 1)} = \frac{1 - e^{-2\theta}}{1 + e^{-2\theta}} \geq \theta.$$

□

Moreover, when the graph is an s-clique, due to the high density of edges, a better lower bound for correlation $E_2(s,\theta)$ is provided by the following lemma.

Lemma B.3. *For each $\delta \in (0, 1/2)$, there exists some constant $c = c(\delta) > 0$ such that for all $\theta \geq c/s$, we have $E_2(s,\theta) \geq 3\delta^2$.*

Proof. Consider the formula in Equation (39), we have

$$E_2(s,\theta) = 1 - 4 \cdot \frac{\sum_{k=0}^{s} k(s-k) C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^{s} s(s-1) C_s^k e^{-2k(s-k)\theta}} = 1 - 4 \cdot \frac{\sum_{k=0}^{s} \frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^{s} C_s^k e^{-2k(s-k)\theta}}.$$

For $\delta \in (0, 1/2)$, when $|k/s - 1/2| \geq \delta$, we have

$$\frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta} \leq \frac{s}{s-1}\Big(\frac{1}{2} - \delta\Big)\Big(\frac{1}{2} + \delta\Big) C_s^k e^{-2k(s-k)\theta},$$

and when $|k/s - 1/2| < \delta$,

$$\sum_{|\frac{k}{s}-\frac{1}{2}|<\delta} \frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta} \leq 2\delta s \cdot \frac{s}{4(s-1)} C_s^{[s/2]} \exp\big(-2(\frac{1}{2}+\delta)(\frac{1}{2}-\delta)s^2\theta\big),$$

where

$$C_s^{[s/2]} = \frac{s!}{([\frac{s}{2}])! \cdot ([\frac{s}{2}])!}.$$

By Stirling's approximation, there exists constants c_1, c_2 s.t.

$$s! = \Omega\Big(\sqrt{2\pi s}(\frac{s}{e})^s\Big),$$

where $x = \Omega(y)$ means there exists some constants $c_1, c_2 > 0$ s.t. $c_1 y < x < c_2 y$. Therefore

$$C_s^{[s/2]} = \Omega\Big(\frac{\sqrt{2\pi s}\,\left(\frac{s}{e}\right)^s}{2\pi \cdot \frac{s}{2} \cdot \left(\frac{s}{2e}\right)^2}\Big) = \Omega\Big(\frac{2^s}{\sqrt{2\pi s}}\Big).$$

Therefore

$$2\delta s \cdot \frac{s}{4(s-1)} C_s^{[s/2]} \exp\big(-2(\frac{1}{2}+\delta)(\frac{1}{2}-\delta)s^2\theta\big) = \Omega\Big(\frac{\delta s}{\sqrt{2\pi s}} \exp\big(s\log 2 - 2(\frac{1}{4}-\delta^2)s^2\theta\big)\Big).$$

If $\theta \geq c/s$ for some sufficiently large constant $c > 0$, we have

$$\sum_{|\frac{k}{s}-\frac{1}{2}|<\delta} \frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta} \to 0, \quad (s \to \infty).$$

Therefore

$$\begin{aligned}\frac{\sum_{k=0}^s k(s-k) C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^s s(s-1) C_s^k e^{-2k(s-k)\theta}} =& \frac{\sum_{|\frac{k}{s}-\frac{1}{2}|<\delta} \frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^s C_s^k e^{-2k(s-k)\theta}} + \frac{\sum_{|\frac{k}{s}-\frac{1}{2}|\geq\delta} \frac{k(s-k)}{s(s-1)} C_s^k e^{-2k(s-k)\theta}}{\sum_{k=0}^s C_s^k e^{-2k(s-k)\theta}} \\ \leq& \frac{1}{4} - \delta^2 + o(1). \end{aligned} \tag{41}$$

Plugging Equation (41) into Equation (39) we have

$$E_2(s,\theta) \geq 4\delta^2 + o(1) \geq 3\delta^2 \tag{42}$$

for sufficiently large s.

□

With the above lemmas in hand, we turn to the proof of Theorem 3.3. Under the oracle computational model, the size of query space is $\eta(\mathcal{Q}_{\mathscr{A}}) = \log\binom{d}{2}$. Also the bound of query function can be taken to be $M = 1$. Therefore with probability at least $1 - 2\xi$, the realizations returned by the oracle satisfies

$$|q_{jk}(X) - \mathbb{E}[q_{jk}(\mathbf{X})]| = |q_{jk}(X) - \mathbb{E}_S[X_j X_k]| \leq \tau_q(s,\theta),$$

uniformly for all $1 \leq j < k \leq d$, where

$$\tau_q(s,\theta) = \max\left\{\frac{2}{3n}\log\Big(\frac{d(d-1)}{2\xi}\Big), \sqrt{\frac{2}{n}\log\Big(\frac{d(d-1)}{2\xi}\Big)}\right\}. \tag{43}$$

Here the variance terms are substituted with their common upper bound 1. Then under $\mathbf{H}_0$ where $G_0 = (V, \varnothing)$, we have $\mathbb{E}_0[X_j X_k] = 0$ for all $1 \leq j < k \leq d$. Therefore with probablity at least $1 - 2\xi$, it holds that

$$-\tau_q(s,0) \leq \min_{j\neq k} q_{jk}(X) \leq \max_{j\neq k} q_{jk}(X) \leq \tau_q(s,0).$$

In our setting where $\log(d)/n = o(1)$, this means that

$$\sup_{\boldsymbol{\theta}\in\mathcal{C}_0} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 1] \leq 2\xi.$$

On the other hand, under $\mathbf{H}_1$ with some $S \in \mathcal{C}_1$ and corresponding probability measure $\mathbb{P}_S$, we know for $(j,k) \notin S$, $\mathbb{E}[X_j X_k] = 0$ and for $(j,k) \in S$, $\mathbb{E}[X_j X_k] = E_2(s,\theta) > 0$. Therefore

$$\min_{j\neq k} q_{jk}(X) \leq \tau_q(s,\theta), \quad \max_{j\neq k} q_{jk}(X) \geq E_2(s,\theta) - \tau_q(s,\theta),$$

hence with probability at least $1-2\xi$, it holds that

$$\max_{j\neq k} q_{jk}(X) - \min_{j\neq k} q_{jk}(X) \geq E_2(s,\theta) - 2\tau_q(s,\theta).$$

Therefore as long as

$$E_2(s,\theta) - 2\tau_q(s,\theta) \geq 2\tau_q(s,0),$$

we would have $\sup_{\boldsymbol{\theta}\in\mathcal{C}_1} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 0] \leq 2\xi$. By Equation (43), we have

$$\tau_q(s,\theta) \leq \max\left\{\frac{2}{3n}\log\left(\frac{d(d-1)}{2\xi}\right), \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}\right\} = \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}$$

for sufficiently large (s,d,n) since $\log(d)/n = o(1)$. Therefore it suffices to prove that under the conditions in Theorem 3.3, we have $E_2(s,\theta) \geq 4\tau_q(s,0)$.

On one hand, when

$$\theta \geq 4\sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}$$

for some constant $c > 0$, we have

$$E_2(s,\theta) \geq \theta \geq 4\sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)} = 4\tau_q(s,0). \tag{44}$$

On the other hand, we fix some $\delta > 0$ and suppose $\theta \geq c/s$ for $c = c(\delta) > 0$ as in Lemma B.3, we have

$$E_2(s,\theta) \geq 3\delta^2 \geq 4\tau_q(s,0), \tag{45}$$

for sufficiently large s, since $\tau_q(s,0) \to 0$ as $d \to \infty$ in our setting. Combining Equations (44) and (45), we complete the proof of Theorem 3.3.

B.3. Proof of Theorem 3.4: Computational Upper Bound for Nearest Neighbor Graph Detection

In this section we prove the computational upper bound for $s/4$-nearest neighbor graph detection in Theorem 3.4. It is attained by the query functions in Equation (9) and the test function in Equation (10).

By the Bernstein-type bound of deviation provided by oracle model, with probability at least $1-2\xi$,

$$|q_{jk}(X) - \mathbb{E}[q_{jk}(\mathbf{X})]| = |q_{jk}(X) - \mathbb{E}_S[X_j X_k]| \leq \tau_q$$

uniformly for all $1 \leq j < k \leq d$, where

$$\tau_q = \max\left\{\frac{2}{3n}\log\left(\frac{d(d-1)}{2\xi}\right), \sqrt{\frac{2}{n}\log\left(\frac{d(d-1)}{2\xi}\right)}\right\}, \tag{46}$$

where we substitute the variance of $q_{jk}(X)$, which may be different for pairs (j,k), with their common upper bound 1. Therefore by the same statements as in the proof of computational upper bound for s-clique detection, when $\log(d)/n = o(1)$ we have $\sup_{\boldsymbol{\theta}\in\mathcal{C}_0} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 1] \leq 2\xi$.

On the other hand, for simplicity we assume $s/4$ is integer. Then in a $s/4$-nearest neighbor graph, if two vertices are within $(s/4)$ distance along the circle, they are connected by an edge. Therefore there exists at least an $(s/4)$-clique. Since deleting edges reduces the correlation, for $(u,v) \in E(G)$, we have

$$\mathbb{E}_S[X_u X_v] \geq E_2(s/4, \theta),$$

where $E_2(s,\theta)$ is the correlation for an edge in an s-clique. Therefore by Lemma B.3, when $\theta \geq c/s$ for some sufficiently large constant c, we have

$$\max_{1\leq j<k\leq d} q_{jk}(X) \geq \widetilde{c} - \tau_q,$$

with constant $\widetilde{c}$ and τ_q defined in Equation (46). Therefore as $s \to \infty$, for sufficiently large s, we have

$$\sup_{\boldsymbol{\theta}\in\mathcal{C}_1} \mathbb{P}_{\boldsymbol{\theta}}[\psi = 0] \leq 2\xi,$$

thus completing the proof.

C. Proof of Theorem 3.5: Information Upper Bounds

In this section we prove the general information upper bound in Theorem 3.5 attained by the query functions and test in Equation (14) and Equation (15) for structures containing $\gamma \cdot s^2$ edges for some constant $\gamma > 0$. Before bounding key elements in our proof, we first introduce some quantities and notations based on s-clique case. Suppose G is an s-clique with $V(G) \subset [d]$, $V(G) = s$, $|E(G)| = s(s-1)/2$. Or equivalently we represent G as $G \subset [d]$ with $|G| = s$, $E(G) = \{(i,j) | i,j \in S, i \neq j\}$. The probability measure is the same for all subsets of $[d]$ with size s up to a permutation of vertices. We defined 4-correlation in an s-clique as

$$E_4(s,\theta) := \mathbb{P}_G[X_{i_1} X_{i_2} X_{i_3} X_{i_4}], \tag{47}$$

where $\{i_1, \ldots, i_4\} \subset G$, $\big|\{i_1, \ldots, i_4\}\big| = 4$. Recall $E_2(s,\theta)$ denotes the correlation for a pair of nodes in s-clique.

We return to any subset $S \subset [d]$ with $|S| = s$ in a graph G where $|V(G)| = s$, $E(G) \geq \gamma \cdot s^2$. For query function $q_S(X) = \big(\frac{1}{s}\sum_{i\in S} x_i\big)^2$ with S, under $\mathbf{H}_1$ we have

$$\mathbb{E}_G[q_S(X)] = \mathbb{E}_G\big(\frac{1}{s}\sum_{i\in S} x_i\big)^2 = \frac{1}{s} + \frac{1}{s}\sum_{i,j\in S, i\neq j} \mathbb{E}_G[X_i X_j] \geq \frac{1}{s},$$

and

$$\mathrm{Var}_G[q_S(X)] = \mathbb{E}_G\Big[\big(\frac{1}{s}\sum_{i\in S} x_i\big)^4\Big] - \big(\mathbb{E}_G[q_S(X)]\big)^2 \leq \mathbb{E}_G\Big[\big(\frac{1}{s}\sum_{i\in S} x_i\big)^4\Big] - \big(\mathbb{E}_G[q_S(X)]\big)^2 - \frac{1}{s^2}.$$

Moreover, for $S \in \mathcal{C}_1$ exactly the subset with the desired structure,

$$\mathbb{E}_G[q_S(X)] = \mathbb{E}_G(\frac{1}{s}\sum_{i\in S} x_i)^2 = \frac{1}{s} + \frac{1}{s}\sum_{i,j\in S, i\neq j} \mathbb{E}_G[X_i X_j] \geq \frac{1}{s} + 2\gamma E_2(s,\theta).$$

We consider the term

$$\begin{aligned}
\mathbb{E}_G\Big[\big(\sum_{i\in S} x_i\big)^4\Big] =& \sum_{i_1,i_2,i_3,i_4=1}^{s} \mathbb{E}_G[X_{i_1} X_{i_2} X_{i_3} X_{i_4}] \\
=& s + 3s(s-1) + \sum_{\substack{i,j,k \\ \text{distinct}}} \mathbb{E}_G[X_i^2 X_j X_k] + 4\sum_{i\neq j} \mathbb{E}_G[X_i^3 X_j] + 24 \sum_{\substack{i,j,k,l \\ \text{distinct}}} \mathbb{E}_G[X_i X_j X_k X_l] \\
=& 3s^2 - 2s + s(s-1)(6s-8)E_2(s,\theta) + s(s-1)(s-2)(s-3)E_4(s,\theta),
\end{aligned}$$

where the first s represents those $i_1, \ldots, i_4$ are identical, and the $3s(s-1)$ represents those $i_1, \ldots, i_4$ that take two distinct values, with two each value. By Griffiths second inequality in (Griffiths, 1967), increasing any paramter θ_{uv} increases multiple-node correlation. Therefore $\mathbb{E}_G[X_jX_k] \le E_2(s,\theta)$ and $\mathbb{E}_G[X_iX_jX_kX_l] \le E_4(s,\theta)$ for 4-pairs (i,j,k,l) where i,j,k,l are distinct. Hence the variances for all $q_S(X)$ are bounded by

$$\text{Var}_G[q_S(X)] = \mathbb{E}_G\Big[\big(\frac{1}{s}\sum_{i\in S} x_i\big)^4\Big] - (\mathbb{E}_G[q_S(X)])^2 \le E_4(s,\theta) + \frac{6}{s}E_2(s,\theta) + \frac{2}{s^2}.$$

Then by the concentration property of oracle computational model, with probability at least $1-2\xi$,

$$\max_{S\subset[d],|S|=s} \big|q_S(X) - \mathbb{E}_G[q_S(X)]\big| \le \tau_q(s,\theta).$$

Here

$$\begin{aligned}\tau_q(s,\theta) =& \max\left\{\frac{2}{3n}\log\Big[\frac{1}{\xi}\binom{d}{s}\Big], 2\sqrt{\frac{2\max_S\{\text{Var}_S[q_S(X)]\}}{n}\log\Big[\frac{1}{\xi}\binom{d}{s}\Big]}\right\}\\ \le& c\cdot\max\left\{\frac{s}{n}\log\big(\frac{d}{s\xi}\big), \sqrt{\frac{s}{n}\cdot\big[E_4(s,\theta)+\frac{6}{s}E_2(s,\theta)+\frac{2}{s^2}\big]\cdot\log\big(\frac{d}{s\xi}\big)}\right\},\end{aligned}$$

for some constant $c>0$, where the variance terms in the Bernstein-type concentration of oracle computational model is substituted by their common upper bound.

Under $\mathbf{H}_0$, all vertices are independent and have expectation zero, hence $\text{Var}_S[q_S(X)] = 2(s-1)/s^3$ and $\mathbb{E}_S[q_S(X)] = 1/s$, we have

$$\tau_q(s,0) \le c\cdot\max\left\{\frac{s}{n}\log\big(\frac{d}{s\xi}\big), \sqrt{\frac{1}{ns}\cdot\log\big(\frac{d}{s\xi}\big)}\right\}.$$

Therefore our test satisfies

$$\sup_{\boldsymbol\theta\in\mathcal{C}_0}\mathbb{P}_{\boldsymbol\theta}[\psi=1]\le 2\xi.$$

On the other hand, under $\mathbf{H}_1$ with $\theta>0$, with probability at least $1-2\xi$, uniformly for all $S\subset[d]$, $|S|=s$, we have $q_S(X)\le\mathbb{E}_S[q_S(X)]+\tau_q(s,\theta)$, thus

$$\max_{S\subset[d],|S|=s} q_S(X) \ge \mathbb{E}_{S\in\mathcal{C}_1}[q_S(X)] - \tau_q(s,\theta).$$

Therefore to prove $\sup_{\boldsymbol\theta\in\mathcal{C}_1}\mathbb{P}_{\boldsymbol\theta}[\psi=0]\le 2\xi$, it suffices to prove

$$\mathbb{E}_G[q_S(X)] - \frac{1}{s} - \tau_q(s,\theta) \ge r(n,d,s,\xi)$$

for $S\in\mathcal{C}_1$, when θ satisfies the conditions in Theorem 3.5. Thus to show

$$\sup_{\boldsymbol\theta\in\mathcal{C}_1}\mathbb{P}_{\boldsymbol\theta}[\psi=0]\le 2\xi,$$

it suffices to show

$$\gamma E_2(s,\theta) \ge 2\tau_q(s,\theta) = 2c\cdot\max\left\{\frac{s}{n}\log\big(\frac{d}{s\xi}\big), \sqrt{\frac{s}{n}\cdot\big[E_4(s,\theta)+\frac{6}{s}E_2(s,\theta)+\frac{2}{s^2}\big]\cdot\log\big(\frac{d}{s\xi}\big)}\right\}, \tag{48}$$

and

$$E_2(s,\theta) \ge 2r(n,d,s,\xi) = 2c\cdot\max\left\{\frac{s}{n}\log\big(\frac{d}{s\xi}\big), 2\sqrt{\frac{1}{ns}\log\big(\frac{d}{s\xi}\big)}\right\}. \tag{49}$$

Since $E_2(s,\theta)\ge\theta$ by Lemma B.2, when θ satisfies the conditions in Theorem 3.5, Equation (49) and the first part of Equation (48) are satisfied. So it remains to verify

$$E_2(s,\theta) \ge c\cdot\sqrt{\frac{s}{n}\cdot\big[E_4(s,\theta)+\frac{6}{s}E_2(s,\theta)+\frac{2}{s^2}\big]\cdot\log\big(\frac{d}{s\xi}\big)},$$

for some constant c, i.e.

$$E_2(s,\theta)^2 \geq \frac{c \cdot s}{n} \log\big(\frac{d}{s\xi}\big) \cdot \big[E_4(s,\theta) + \frac{6}{s}E_2(s,\theta) + \frac{2}{s^2}\big].$$

Hence it suffices to show

$$E_2(s,\theta) \geq \frac{c}{n} \log\big(\frac{d}{s\xi}\big), \tag{50}$$

$$E_2(s,\theta) \geq c\sqrt{\frac{s}{n} \log\big(\frac{d}{s\xi}\big) E_4(s,\theta)}, \tag{51}$$

$$E_2(s,\theta) \geq c\sqrt{\frac{1}{sn} \log\big(\frac{d}{s\xi}\big)}, \tag{52}$$

for some sufficiently large constant $c > 0$. Here Equations (50) and (52) are naturally satisfied by the conditions since $E_2(s,\theta) \geq \theta$. For Equation (51), which is equivalent to

$$\frac{E_2(s,\theta)^2}{E_4(s,\theta)} \geq \frac{c \cdot s}{n} \log\big(\frac{d}{s\xi}\big), \tag{53}$$

for some constant $c > 0$. To bound the term in 53, we introduce some lemmas regarding $E_4(s,\theta)$.

Lemma C.1. *For the aforementioned $E_4(s,\theta)$ and $s \geq 4$, we have*

$$E_4(s,\theta) = 1 - 8 \cdot \frac{\sum_{k=0}^{s-4} C_{s-4}^k \Big[e^{(2k^2-2ks+12k+18-6s)\theta}\Big]}{\sum_{k=0}^{s} C_s^k \exp\big(-2k(s-k)\theta\big)} - 8 \cdot \frac{\sum_{k=0}^{s-4} C_{s-4}^k \Big[e^{(2k^2-2ks-5k+2-2s)\theta}\Big]}{\sum_{k=0}^{s} C_s^k \exp\big(-2k(s-k)\theta\big)}. \tag{54}$$

Proof of Lemma C.1. By definition, we have

$$E_4(s,\theta) = \mathbb{P}_S[X_1X_2X_3X_4 = 1] - \mathbb{P}_S[X_1X_2X_3X_4 = -1] = 1 - 2\mathbb{P}_S[X_1X_2X_3X_4 = -1].$$

Note that when $X_1X_2X_3X_4 = -1$, there are 3 vertices taking value 1 and one vertex -1, or 3 vertices taking value -1 and one 1. Therefore

$$\sum_{x_1x_2x_3x_4=-1} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right) = 4 \sum_{\substack{x_1=x_2=x_3=1,\\ x_4=-1}} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right) + 4 \sum_{\substack{x_1=x_2=x_3=-1,\\ x_4=1}} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right),$$

where

$$\begin{aligned}\sum_{\substack{x_1=x_2=x_3=1,\\ x_4=-1}} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right) &= \sum_{k=0}^{s-4} \sum_{\substack{x_1=x_2=x_3=1, x_4=-1,\\ k \text{ remaining vertices take value 1}}} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right) \\ &= \sum_{k=0}^{s-4} C_{s-4}^k \exp\big((2k^2 + s^2/2 - 2ks + 12k + 18 - 13s/2)\theta\big),\end{aligned} \tag{55}$$

and similarly we get

$$\sum_{\substack{x_1=x_2=x_3=-1,\\ x_4=1}} \exp\left(\sum_{(u,v)\in S} \theta x_u x_v\right) = \sum_{k=0}^{s-4} C_{s-4}^k \cdot \exp\big((2k^2 + s^2/2 - 2ks - 5k + 2 - 5s/2)\theta\big). \tag{56}$$

Plugging in Equations (55) and (56), we get the desired formula. ☐

With this formula in hand, we provide an upper bound for $E_4(s,\theta)$ specified by the following lemma.

Lemma C.2. *For $s \geq 4$ and $\theta > 0$, it always holds that $E_4(s,\theta) \leq 7s\theta$.*

Proof of Lemma C.2. Since $e^x \geq 1 + x$, we have

$$\frac{\sum_{k=0}^{s-4} C_{s-4}^k \Big[\exp\big((2k^2 - 2ks + 12k + 18 - 6s)\theta\big)\Big]}{\sum_{k=0}^{s} C_s^k \exp\big(-2k(s-k)\theta\big)} + \frac{\sum_{k=0}^{s-4} C_{s-4}^k \Big[\exp\big((2k^2 - 2ks - 5k + 2 - 2s)\theta\big)\Big]}{\sum_{k=0}^{s} C_s^k \exp\big(-2k(s-k)\theta\big)}$$
$$\geq \frac{1}{\sum_{k=0}^{s} C_s^k} \sum_{k=0}^{s-4} C_{s-4}^k [1 + (2k^2 - 2ks + 12k + 18 - 6s)\theta + 1 + (2k^2 - 2ks - 5k + 2 - 2s)\theta]$$
$$= 2^{-s}\left[2^{s-3} + (60 - 21s) \cdot 2^{s-5} \cdot \theta\right].$$

Therefore

$$E_4(s,\theta) \leq 1 - 8 \cdot 2^{-s}\left[2^{s-3} + (60-21s) \cdot 2^{s-5} \cdot \theta\right] \leq \frac{1}{4}(25s - 60)\theta \leq 7s\theta,$$

which completes the proof. □

We return to our proof of Theorem 3.5. By Lemma C.2 as well as $E_2(s,\theta) \geq \theta$, we have

$$\frac{E_2(s,\theta)^2}{E_4(s,\theta)} \geq \frac{\theta^2}{7s\theta} = \frac{\theta}{7s} \geq \frac{c \cdot s}{n} \log\big(\frac{d}{s\xi}\big),$$

since $\theta \geq \frac{c \cdot s^2}{n} \log(\frac{d}{s\xi})$ by the assumptions. This completes the proof of Theorem 3.5.

D. Proof of Theorem 3.6: Information Lower Bound for Perfect Matching

To provide an information lower bound for perfect matching, we introduce a sharper upper bound on the total variation of testing empty graph against perfect matching graphs with s vertices. We borrow some statements in Section 8.3.2 from (Daskalakis et al., 2016).

Lemma D.1. *Assume s is even. For perfect matching problem, we define $\mathcal{C}_0 = \{(V, \varnothing)\}$ with corresponding probability measure $\mathbb{P}_0$, and $\mathcal{C}_1 = \{G = (V,E) : |V| = s, |E| = s/2, G \text{ is a perfect matching }\}$. Denote $\mathbb{P}_0^{\otimes n}$ to be the probability measure that draws n samples from $\mathbb{P}_0$, and $\overline{\mathbb{P}}_1^{\otimes n}$ the probability measure corresponding to selecting some q from $\mathcal{C}_1$ uniformly at random and then drawing n samples from q. Then we have*

$$2d_{TV}^2(\mathbb{P}_0^{\otimes n}, \overline{\mathbb{P}}_1^{\otimes n}) \leq n \log \mathbb{E}_{\overline{\mathbb{P}}_1^{\otimes n}}\Big[\frac{\mathbb{P}_0^{\otimes n}}{\overline{\mathbb{P}}_1^{\otimes n}}\Big].$$

Furthermore we have

$$2d_{TV}^2(\mathbb{P}_0^{\otimes n}, \overline{\mathbb{P}}_1^{\otimes n}) \leq \frac{9sn\theta^4}{4} + \log\Big(\frac{3/2}{1 - \exp\big(3n\theta^2 - \log(3/2)\big)}\Big).$$

Proof of Lemma D.1. See Section 8.3.2 in (Daskalakis et al., 2016). □

Then if

$$\theta \leq \frac{c}{\sqrt{n}} \wedge \frac{c}{s} \tag{57}$$

for some sufficiently small constant c, then the total variance is upper bounded by a sufficiently small constant, therefore no algorithm can distinguish between the two hypotheses with probability larger than some small constant.