LOWER BOUNDS TO RANDOMIZED ALGORITHMS FOR GRAPH PROPERTIES

Andrew Chi-Chih Yao

CS-TR-134-88

February 1988

Lower Bounds to Randomized Algorithms for Graph Properties[1]

Andrew Chi-Chih Yao

Department of Computer Science
Princeton University
Princeton, New Jersey 08544

Abstract

For any property P on n-vertex graphs, let $C(P)$ be the minimum number of edges needed to be examined by any decision tree algorithm for determining P. In 1975 Rivest and Vuillemin settled the Aanderra-Rosenberg Conjecture, proving that $C(P) = \Omega(n^2)$ for every nontrivial monotone graph property P. An intriguing open question is whether the theorem remains true when randomized algorithms are allowed. In this paper we show that $\Omega(n(\log n)^{1/12})$ edges need to be examined by any randomized algorithm for determining any nontrivial monotone graph property.

[1] This research was supported in part by the National Science Foundation under grant number DCR-8308109.

1 Introduction

Let $C(P)$ be the minimum number of entries that need to be examined in the worst case by any algorithm for computing an n-vertex graph property P, when the input graph is given as an adjacency matrix. In 1975 Rivest and Vuillemin [RV] settled the Aanderra-Rosenberg Conjecture [R], proving that $C(P) = \Omega(n^2)$ for every nontrivial monotone graph property P. An intriguing open problem (see [Y]) is whether their result remains true when randomized algorithms are allowed. In fact, Richard Karp conjectured (see [SW]) that $R(P) = \Omega(n^2)$, where $R(P)$ is the randomized complexity for deciding P. It was known that $R(P) = \Omega(n)$, which follows from a result of Blum (see [SW]) for general Boolean function evaluations (also follows from observations made in Kirkpatrick [Kir]) that for some inputs the shortest verification needs $\Omega(n)$ entries to be revealed. In this paper we will prove the following result which cannot be obtained by using lower bounds on nondeterministic verifications.

Theorem 1 $R(P) = \Omega(n(\log n)^{1/12})$ for any nontrivial monotone graph property P on n vertices.

We will also define and study a search problem, which seeks to identify all the edges in an input graph. The results obtained are used to prove Theorem 1, and are of interest by themselves.

It remains an intriguing question how much randomization helps in determining graph properties. It was observed in Saks and Wigderson [SW] and by Karp (private communication) that a factor of two can be saved in some case. For the general case of Boolean function evaluation, there exist examples by Snir [S], Boppana (see [SW]) and Saks and Wigderson [SW], where the randomized complexity is $O(n^\alpha), 0 < \alpha < 1$, while the deterministic complexity is $\Omega(n)$. For a general discussion of randomized complexity, see Yao [Y]. For a study of the randomized complexity of Boolean function evaluation, see Saks and Wigderson [SW]. Also see Manber and Tompa [MT], Meyer auf der Heide [M], and Snir [S] for discussions on other randomized decision tree problems.

2 Preliminaries

A *graph* G on n vertices is an $n \times n$ matrix (a_{ij}) such that $a_{ii} = 0$, $a_{ij} = a_{ji} \in \{0, 1\}$ for all $1 \le i$, $j \le n$; we sometimes write $G = (V, E_G)$, where $V = \{v_1, v_2, \ldots, v_n\}$ and E_G is the *edge set* $\{\{v_i, v_j\} | a_{ij} = 1\}$. Two graphs $G = (a_{ij})$, $G' = (a'_{ij})$ are *isomorphic* if there exists a permutation σ on $\{1, 2, \ldots, n\}$ such that $a'_{ij} = 1$ if and only if $a_{\sigma(i)\sigma(j)} = 1$. Let $\mathcal{G}_n$ denote the set of all G on n vertices. A *graph property* (on n-vertex graphs) is a function $P : \mathcal{G}_n \to \{0, 1\}$ such that $P(G) = P(G')$ if G, G' are isomorphic. We say P is *nontrivial* if P is not a constant.

Let $G = (a_{ij})$, $G' = (a'_{ij}) \in \mathcal{G}_n$. We write $G \le G'$ if $a_{ij} \le a'_{ij}$ for all i, j. A graph property P

on n-vertex graphs is *monotone* if $G \leq G'$ implies $P(G) \leq P(G')$. Let $\mathcal{P}_n$ denote the set of all nontrivial monotone graph properties on n vertices.

A *decision tree algorithm* A computes a graph property P for any input G by asking a series of queries $a_{i_1 j_1} = ?$, $a_{i_2 j_2} = ?$, ... , until $P(G)$ can be determined; the queries are adaptively chosen depending on the answers to previous queries (see e.g. [RV] for more formal descriptions). Without loss of generality, we will require that the same query will not be asked twice. Let *cost(A, G)* be the number of queries asked by A when G is the input. Let $\mathcal{A}_P$ denote the set of all decision tree algorithms for P. The *worst case complexity* $C(P)$ is $\min\{cost(A) | A \in \mathcal{A}_P\}$, where $cost(A)$ is defined as $\max\{cost(A, G) | G \in \mathcal{G}_n\}$.

A *randomized decision tree algorithm* is a probability distribution α over $\mathcal{A}_P$. The expected number of queries asked by α for input G is $\sum_{A \in \mathcal{A}_P} \alpha(A)\, cost(A, G)$, denoted by $h(\alpha, G)$. The *cost* of α is defined as $\max\{h(\alpha, G) | G \in \mathcal{G}_n\}$. The *randomized complexity* $R(P)$ is the minimum cost of any α. This cost is achieved by some α, as is guaranteed by the Minimax Theorem (see [Y]).

As an intermediate step for proving our theorem, we need to consider *bipartite graphs* G, which are $m \times n$ matrices (a_{ij}) where $a_{ij} \in \{0, 1\}$ for $1 \leq i \leq m$, $1 \leq j \leq n$. We sometimes write $G = (V \times W, E_G)$ where $V = \{v_1, v_2, \ldots, v_m\}$, $W = \{w_1, w_2, \ldots, w_n\}$ and E_G denotes the *edge set* $\{(v_i, w_j) | a_{ij} = 1\}$. Two graphs $G = (a_{ij})$ and $G' = (a'_{ij})$ are isomorphic if there exist permutations σ, ρ on $\{1, 2, \ldots, m\}$, $\{1, 2, \ldots, n\}$, respectively, such that $a'_{ij} = 1$ if and only if $a_{\sigma(i), \rho(j)} = 1$. Let $\mathcal{G}_{m,n}$ denote the set of all bipartite graphs on $V \times W$. A *bipartite graph* property is a function $P : \mathcal{G}_{m,n} \to \{0, 1\}$ such that $P(G) = P(G')$ if G and G' are isomorphic.

Let $\mathcal{P}_{m,n}$ denote the set of all nontrivial monotone bipartite graph properties on $V \times W$, where the concepts of "nontrivial" and "monotone" are straightforward analogues of the corresponding ones for graph properties. We can also develop the decision tree model and its randomized version for bipartite graph properties in a similar manner. Henceforth we will use the same notations, e.g. $cost(A, G)$ etc., as in graph properties.

Theorem 1 follows immediately from the next two propositions.

Proposition 1 For every $P \in \mathcal{P}_{n,n}$, $R(P) = \Omega(n(\log n)^{1/4})$.

Proposition 2 Let $\epsilon > 0$ be any fixed constant. If every $P \in \mathcal{P}_{n,n}$ satisfies $R(P) = \Omega(n(\log n)^{\epsilon})$, then every $P \in \mathcal{P}_n$ satisfies $R(P) = \Omega(n(\log n)^{\epsilon/3})$.

In Section 3, we present a proof of Proposition 1. We digress in Section 4 to define and study a family of search problems which seek to identify all the edges in input bipartite graphs. In Section 5, we used the results in Section 4 and an embedding technique from [RV] to prove Proposition 2.

3 Proof of Proposition 1

As defined earlier, let $\mathcal{G}_{m,n}$ be the set of all bipartite graphs on vertex set $V \times W$, where $V = \{v_1, v_2, \ldots, v_m\}$, $W = \{w_1, w_2, \ldots, w_n\}$.

Definition 1 Consider any bipartite graph $G \in \mathcal{G}_{m,n}$. Let d_i =degree(w_i) for $1 \leq i \leq n$, then the *degree sequence* $\tilde{d}(G)$ is the sequence $(d_{i_1}, d_{i_2}, \ldots, d_{i_n})$ such that $d_{i_1} \geq d_{i_2} \geq \ldots \geq d_{i_n}$ and $(i_1, i_2, \ldots, i_n)$ is a permutation of $(1, 2, \ldots, n)$. For any two $G_1, G_2 \in \mathcal{G}_{m,n}$, we write $G_1 < \cdot\, G_2$ if $\tilde{d}(G_1)$ is lexicographically strictly smaller than $\tilde{d}(G_2)$. Let $e(G)$ denote the number of edges in G.

Definition 2 Let $P \in \mathcal{P}_{m,n}$. A bipartite graph $G \in \mathcal{G}_{m,n}$ is a *minimal graph* for P if $P(G) = 1$ and every proper subgraph G' of G satisfies $P(G') = 0$. Let $\mathcal{M}_P$ denote the set of all minimal graphs for P. For any $P \in \mathcal{P}_{m,n}$, let G_P denote a lexicographically smallest minimal graph for P, i.e. $\tilde{d}(G_P) < \cdot\, \tilde{d}(G)$ or $\tilde{d}(G_P) = \tilde{d}(G)$ for all $G \in \mathcal{M}_P$. (There may be many possible choices of G_P; we choose any one once and for all.)

Definition 3 Let $P \in \mathcal{P}_{m,n}$. The *dual* of P is the property $Q \in \mathcal{P}_{m,n}$ such that $Q(G) = 1$ if and only if $P(\bar{G}) = 0$, where $\bar{G}$ is the complement of G.

Definition 4 Let $P \in \mathcal{P}_{m,n}$. We say that P is *impartial* if $P(K_{\lceil m/4 \rceil, n}) = 0$.

Remarks. $K_{m,n}$ is the $m \times n$ complete bipartite graph, and K_n is the complete graph on n vertices. Later in Section 5, we will also use $K_{V \times W}$ to denote the complete bipartite graph on $V \times W$, and K_V to denote the complete graph on V.

Lemma 1 Let L and H be non-empty bipartite graphs on $V \times W$, and $\mathcal{H}$ be the family of all bipartite graphs isomorphic to H. Take a random H', uniformly chosen from $\mathcal{H}$, then

$$\Pr\{E_{H'} \cap E_L \neq \phi\} \leq \frac{|E_L| \cdot |E_H|}{mn}.$$

Proof. For each edge $e \in E_L$, $\Pr\{e \in E_{H'}\} = |E_H|/mn$. Therefore, $\Pr\{E_{H'} \cap E_L \neq \phi\} \leq \sum_{e \in E_L} \Pr\{e \in E_{H'}\} = |E_L| \cdot |E_H|/mn.\Box$

Lemma 2 Let $P \in \mathcal{P}_{m,n}$ and Q be the dual of P. Then the following statements are true:

(a) If $m \geq 4$ and P is not impartial, then Q is impartial;

(b) $R(P) = R(Q)$;

(c) $e(G) \cdot e(G') \geq m\,n$ for all $G \in \mathcal{M}_P$, $G' \in \mathcal{M}_Q$.

Proof. Statements (a) and (b) follow immediately from the definitions. To prove (c), observe that any H isomorphic to G must satisfy $E_H \cap E_{G'} \neq \phi$; we now apply Lemma 1 to show that, if (c) is not true, then a random H isomorphic to G has a nonzero probability of violating that constraint.□

Definition 5 Let $\lambda(n) = (\log_2 n)^{1/4}$, $\mu(n) = (\log_2 n)^{1/2}$.

Definition 6 Let $P \in \mathcal{P}_{m,n}$, and $A \in \mathcal{A}_P$. Let $\bar{C}_q(A)$ be the average value of $cost(A, G)$ when G is distributed according to probability distribution q on $\mathcal{G}_{m,n}$.

To prove Proposition 1, we will construct a q and prove that, for all $A \in \mathcal{A}_P$, $\bar{C}_q(A) = \Omega(n(\log_2 n)^{1/4})$. This will prove Proposition 1, as $R(P) \geq \bar{C}_q(A)$ by a general theorem in [Y]. For the rest of this section, we let $m = n \geq 4$. We assume that $P \in \mathcal{P}_{m,n}$ is impartial; this is done without loss of generality because of Lemma 2 (a)(b). We now prove Proposition 1 by a series of lemmas. Each lemma deals with a subclass of bipartite graph properties. The proof of Lemma 6 is perhaps the most interesting part of the proof of Proposition 1.

Lemma 3 If $e(G_P) \geq \lambda(n)n$, then $R(P) \geq \lambda(n)n$.

Proof: Let q be the probability distribution on $\mathcal{G}_{m,n}$ defined as follows: $q(G) = 1$ if $G = G_P$ and 0 otherwise. For any $A \in \mathcal{A}_P$, $\text{cost}(A, G_P) \geq e(G_P)$ as $G_P \in \mathcal{M}_P$. Hence $\bar{C}_q(A) = \text{cost}(A, G_P) \geq \lambda(n)n$. □

Lemma 4 If $e(G_P) \leq \frac{n}{\lambda(n)}$, then $R(P) \geq \lambda(n)n$.

Proof. Let Q be the dual of P. Then by Lemma 1(c), $e(G_Q) \geq mn/e(G_P) \geq \lambda(n)m$. By Lemma 2, $R(Q) \geq \lambda(n)m$. Thus, $R(P) = R(Q) \geq \lambda(n)n$ by Lemma 3. □

We can thus assume in what follows $n/\lambda(n) < e(G_P) < \lambda(n)n$. Let $d_{max} = \max\{d_1, d_2, \ldots, d_n\}$ where $d_i =$ degree (w_i) in G_P. (Recall that $\tilde{d}(G_P)$ is the sorted permutation of $(d_1, d_2, \ldots, d_n)$.) Let N_0 be any fixed integer large enough such that $\log_2 N_0 \geq 8^4$.

Lemma 5 Let $n \geq N_0$. If $d_{max} \leq \mu(n)$, then $R(P) \geq \frac{1}{4}\lambda(n)n$.

Proof. Let $s = \lceil m/4 \rceil$ and $m' = m - s$. Construct $P_1 \in \mathcal{P}_{m',n}$ from P as described below. For each $G_1 \in \mathcal{G}_{m',n}$ on vertex set $V \times W$, let $G \in \mathcal{G}_{m,n}$ be the graph obtained from G_1 by adding s new vertices to V and sn edges between these vertices and all the vertices in W; define $P_1(G_1) = P(G)$. Clearly, $R(P) \geq R(P_1)$; also P_1 is monotone. As P is impartial, $P_1(H) = 0$ for the $m' \times n$ empty bipartite graph H. Since $P_1(K_{m',n}) = P(K_{m,n}) = 1$, we have thus shown P_1 to be nontrivial and monotone. To prove Lemma 5, we only need to prove $R(P_1) \geq \frac{1}{4}\lambda(n)n$.

First we *claim* that there exists a minimal graph $G_0 \in \mathcal{M}_{P_1}$ such that $e(G_0) < \lambda(n)n$ and all vertices in G_0 have degree $\leq \mu(n)$. In G_P, let a_i =degree(v_i), and let $i_1, i_2, \ldots, i_s$ be the indices of the largest s a_i's. Obtain $G_1 \in \mathcal{G}_{m',n}$ from G_P by deleting $v_{i_1}, v_{i_2}, \ldots, v_{i_s}$ and all the incident edges. Then $P_1(G_1) = 1$ and $e(G_1) \leq e(G_P) < \lambda(n)n$. Now, $\min\{a_{i_1}, a_{i_2}, \ldots, a_{i_s}\} \leq 4\,\lambda(n)$, since otherwise $e(G_P) \geq \lambda(n)m$. Thus all vertices v_j in G_1 have degree $\leq 4\,\lambda(n) \leq \mu(n)$. By assumption, all the vertices w_i in G_1 also have degree $\leq d_{max} \leq \mu(n)$. Let G_0 be any subgraph of G_1 such that $G_0 \in \mathcal{M}_{P_1}$. This G_0 clearly satisfies all the constraints in the *claim* .

If $e(G_0) \leq n/\lambda(n)\,n$, then we can prove $R(P_1) \geq \lambda(n)m'$ exactly as done in Lemma 4. We can thus assume that

$$e(G_0) > \frac{1}{\lambda(n)}\,n. \tag{1}$$

Let $M = \{(v_{k_1}, w_{\ell_1}), (v_{k_2}, w_{\ell_2}), \ldots, (v_{k_t}, w_{\ell_t})\}$ be a maximum matching in G_0. Then all edges of G_0 must be incident to some v_{k_i} or w_{ℓ_j}. Thus

$$e(G_0) \leq 2\,\mu(n) \cdot t. \tag{2}$$

It follows from (1) and (2) that

$$|M| = t \geq \frac{n}{2(\lambda(n))^3}. \tag{3}$$

Relabeling the vertices if needed, we can assume that G_0 is a bipartite graph on $V \times W$, where $V = \{v_1, v_2, \ldots, v_{m'}\}$, $W = \{w_1, w_2, \ldots, w_n\}$ such that $\{(v_1, w_1), (v_2, w_2), \ldots, (v_{t_0}, w_{t_0})\}$ is a matching, where $t_0 = \lceil n/2(\lambda(n))^3 \rceil$. Let $\mathcal{D}(G_0)$ be the set of all bipartite graphs on $V \times W$ isomorphic to G_0. We will prove

$$|\mathcal{D}(G_0)| \geq \left(\frac{m}{2\mu(n)}\right)^{t_0}. \tag{4}$$

Inequality (4) implies $R(P_1) \geq \frac{1}{4}\,n\,\lambda(n)$ by the following argument: Consider the input distribution q defined by $q(G) = \frac{1}{|\mathcal{D}(G_0)|}$ if $G \in \mathcal{D}(G_0)$ and 0 otherwise. Then, for any $A \in \mathcal{A}_{P_1}$, all the inputs from $\mathcal{D}(G_0)$ lead to distinct leaves in A. The average distance of these leaves to the root is at least $\log_2 |\mathcal{D}(G_0)|$. Therefore, we have

$$\begin{aligned} \bar{C}_q(A) &\geq \log_2 |\mathcal{D}(G_0)| \\ &\geq t_0(\log_2 m - \frac{1}{2}\log_2\log_2 n - 1) \\ &\geq \frac{n}{4(\lambda(n))^3}\log_2 n \\ &= \frac{1}{4}\lambda(n)\,n. \end{aligned}$$

It remains to prove (4). Let Γ be the set of all permutations on V. For any $\sigma \in \Gamma$ and $G \in \mathcal{G}_{m',n}$, let σG denote the resulted graph when each $v_i \in V$ is relabeled $v_{\sigma(i)}$. Then the group

Γ acts transitively on the set $\{H \mid H = \sigma G_0 \text{ for some } \sigma \in \Gamma\}$. Let $\Gamma_0 \subseteq \Gamma$ be the the set of permutations σ such that $\sigma G_0 = G_0$. By elementary group theory,

$$\begin{aligned} |\mathcal{D}(G_0)| &= \frac{|\Gamma|}{|\Gamma_0|} \\ &= \frac{m'!}{|\Gamma_0|} \end{aligned} \tag{5}$$

As every $(v_i, w_i), 1 \leq i \leq t_0$, is still an edge in σG_0 for all $\sigma \in \Gamma_0$, we have

$$\begin{aligned} |\Gamma_0| &\leq b_1 b_2 \dots b_{t_0} \cdot (m' - t_0)! \\ &\leq (\mu(n))^{t_0} \cdot (m' - t_0)!, \end{aligned} \tag{6}$$

where b_i = degree (w_i) in G_0.

From (5) and (6) we obtain

$$\begin{aligned} |\mathcal{D}(G_0)| &\geq \frac{1}{(\mu(n))^{t_0}} m'(m'-1)\dots(m'-t_0+1) \\ &\geq \left(\frac{m}{2\mu(n)}\right)^{t_0}. \end{aligned}$$

This proves (4), and completes the proof of Lemma 5. □

Lemma 6 Let $n \geq N_0$. If $d_{max} > \mu(n)$, then $R(P) \geq \frac{1}{320}\lambda(n)n$.

Proof. As $e(G_P) < \lambda(n)n$, there are at most $\lfloor n/2 \rfloor$ of vertices w_i in G_P with degree $\geq 2\lambda(n)$. Therefore, at least $n' = \lceil n/2 \rceil$ of the vertices w_i in G_P have degree $< 2\lambda(n)$. Without loss of generality, we can, by relabeling w_i's if needed, assume that $b_1 = b_{max} > \mu(n)$ and $b_i \leq 2\lambda(n)$ for $2 \leq i \leq n'$ where b_i is the degree of w_i.

Let S_i be the set of v_j such that (v_j, w_i) are edges in G_P, $1 \leq i \leq n$. (Clearly $b_i = |S_i|$). We will describe an input distribution of bipartite graphs. Let $T_1 = S_1 - S_{n'}$, $T_2 = S_1 - S_2$, and $T_i = S_1 - (S_{i-1} \cup S_i)$ $3 \leq i \leq n'$.

```
Algorithm DIST: [comment: generates a random bipartite graph $G$]

begin

    a) Initialize $G \leftarrow G_P$;
    b) Add to $G$ edges $(v_j, w_i)$ for all $v_j \in T_i \cup S_{i-1}$ , $2 \leq i \leq n'$;
    c) Randomly pick a $T_i' \subseteq T_i$ with $|T_i'| = \lceil 4\lambda(n) \rceil$ (all such $T_i'$ are equally likely to be chosen),
       and delete all edges $(v_j, w_i)$ for $v_j \in T_i'$, $2 \leq i \leq n'$;
    d) Add to $G$ edges $(v_j, w_1)$ for all $v_j \in S_{n'}$;
```

e) Randomly pick a $T_1' \subseteq T_1$ with $|T_1'| = \lceil 4\lambda(n) \rceil$ (all such T_1' are equally likely to be chosen), and delete all edges (v_j, w_1) for $v_j \in T_1'$;

end

An output graph $G(\mathcal{B})$ of DIST is specified by the value of $\mathcal{B} = (T_1', T_2', \ldots, T_{n'}')$. [All other quantities are fixed by P.] We will need two useful facts. The proof of Fact 1 utilizes the fact that G_P is a lexicographically smallest minimal graph for P.

Fact 1 Any output $G(\mathcal{B})$ of DIST satisfies $P(G(\mathcal{B})) = 0$.

Fact 2 Let $i \in [1, n']$ be any integer. In any output $G(\mathcal{B})$, if we add to it the set of edges (v_j, w_i) for all $j \in T_i'$, then the resulted graph $G_i(\mathcal{B})$ satisfies $P(G_i(\mathcal{B})) = 1$.

To prove Fact 1, we need ony show that $G(\mathcal{B}) < \cdot\, G_P$, as G_P is by definition a lexicographically smallest element in $\mathcal{M}_P$. Let b_i' be the degree of w_i in $G(\mathcal{B})$, $1 \leq i \leq n$. It suffices to prove that $\max\{b_1', b_2', \ldots, b_{n'}'\} < b_1$. This can be verified easily, as $b_i' \leq |T_i \cup S_{i-1}| + b_i - |T_i'| \leq |S_1| + |S_{i-1}| + |S_i| - 4\lambda(n) < |S_1| = b_1$ for $2 \leq i \leq n/2$, and $b_1' = |S_1 \cup S_{n'}| - |T_1'| \leq |S_1| + |S_{n'}| - 4\lambda(n) < |S_1| = b_1$. This establishes Fact 1.

To prove Fact 2, let $Y_{i,k}$ be the set of vertices v_j such that (v_j, w_k) are edges in $G_i(\mathcal{B})$, $1 \leq k \leq n$.

Case 1. If $i = 1$, then $Y_{i,k} = S_k$ for $n' + 1 \leq k \leq n$ and $Y_{i,k} \supseteq S_k$ for $1 \leq k \leq n'$. Therefore, G_P is a subgraph of $G_i(\mathcal{B})$. Hence $P(G_i(\mathcal{B})) \geq P(G_P) = 1$.

Case 2. If $2 \leq i \leq n'$, then $Y_{i,k} = S_k$ for $n' + 1 \leq k \leq n$, $Y_{i,k} \supseteq S_k$ for $2 \leq k < i$, and the following is true:

$$\begin{aligned} Y_{i,i} &\supseteq S_1, \\ Y_{i,k} &\supseteq S_{k-1} \text{ for } i < k \leq n', \\ Y_{i,1} &\supseteq S_{n'}. \end{aligned}$$

It follows that $G_i(\mathcal{B})$ contains a subgraph that is isomorphic to G_P. Thus $P(G_i(\mathcal{B})) \geq P(G_P) = 1$. This proves Fact 2.

We now complete the proof of Lemma 6. Let $A \in \mathcal{A}_P$. For any $G(\mathcal{B})$ as input graph to A, let $L_{\mathcal{B}}$ be the set of all entries of the incidence matrix of $G(\mathcal{B})$ that are examined by A. Facts 1 and 2 imply that, for each $1 \leq i \leq n'$, $\{(v_j, w_i) | v_j \in T_i'\} \cap L_{\mathcal{B}} \neq \emptyset$. In other words, A has to discover at least one of the missing edges in $\{(v_j, w_i) | v_j \in T_i'\}$ for every $1 \leq i \leq n'$.

Consider T_i' , $1 \leq i \leq n'$, as independent random variables. Each T_i' is a uniformly chosen random subset of T_i. Note that $|T_i| \geq |S_1| - 4\lambda(n) \geq \mu(n) - 4\lambda(n)$, and $|T_i'| \leq 4\lambda(n) + 1$. Let

$X_i = \{(v_j, w_i) | v_j \in T_i\} \cap L_{\mathcal{B}}$. A simple calculation shows that, for $\ell = \lceil |T_i|/(8|T_i'|) \rceil$,

$$\begin{aligned} \Pr\{|X_i| > \ell\} &= 1 - \sum_{1 \leq k \leq \ell} \Pr\{|X_i| = k \mid |X_i| > k-1\} \\ &\geq 1 - \sum_{1 \leq k \leq \ell} \frac{|T_i'|}{|T_i| - k + 1} \\ &\geq 1 - \ell \frac{5|T_i'|}{4|T_i|} \\ &\geq \frac{1}{2}. \end{aligned}$$

It follows that

$$\begin{aligned} E(|X_i|) &\geq \frac{1}{2}\ell \\ &\geq \frac{1}{16} \frac{\mu(n) - 4\lambda(n)}{4\lambda(n) + 1} \\ &\geq \frac{1}{160}\lambda(n). \end{aligned}$$

Thus,

$$\begin{aligned} E(|L_{\mathcal{B}}|) &\geq \sum_{1 \leq i \leq n'} E(|X_i|) \\ &\geq \frac{1}{160}\lambda(n)n'. \end{aligned}$$

This proves that for each $A \in \mathcal{A}_P$, $\bar{C}_q(A) \geq \frac{1}{320}\lambda(n)n$. This proves Lemma 6. □

We have completed the proof of Proposition 1.

4 Identification Problems for Graphs

In this section we derive two results for a special type of search problems. These results are of interest by themselves, and will be used in Section 5 to prove Proposition 2. Let $\mathcal{F} \in \mathcal{G}_{n,n}$ be a family of bipartite graphs. The *identification problem* for $\mathcal{F}$ is to locate and verify, for any given input $G = (a_{ij}) \in \mathcal{F}$, all the edges in G. In our model, an algorithm B is a binary decision tree with queries of the form "$a_{ij} =?$" at its internal nodes, such that any input $G = (a_{ij}) \in \mathcal{F}$ will follow in B a path along which all the nonzero a_{ij}'s will be queried. As in the case for algorithms in $\mathcal{A}_P$, we will use *cost*(B, G) and $\bar{C}_q(B)$ to denote the *cost* and the *average cost* with respect to distribution q.

We will be interested in two particular classes of identification problems. We first introduce some notations. Let $V = \{v_i \mid 1 \leq i \leq m\ell\}$ and $W = \{w_j \mid 1 \leq j \leq m\ell\}$ be disjoint sets, where

m, ℓ are positive integers. Call the subsets $V_i = \{v_{(i-1)m+s} \mid 1 \le s \le m\}$, $W_j = \{w_{(j-1)m+s} \mid 1 \le s \le m\}$ the i-th and the j-th *blocks* of V, W. We will consider bipartite graphs $G = (a_{ij})$ on the vertex set $V \times W$. Let Q_{ij} denote the set of all queries "$a_{st} =?$" with $v_s \in V_i$, $w_t \in W_j$, where $1 \le i, j \le \ell$.

The first class of problems is parametrized by a triplet (m, ℓ, H), where m, ℓ are positive integers and H is an m by m non-empty bipartite graph. Let $\mathcal{H}$ be the set of all m by m bipartite graphs isomorphic to H. Let $\mathcal{D}(m, \ell, H) \subseteq \mathcal{G}_{n,n}$, where $n = m\ell$, be the set $\{F_{i,j,H'} \mid 1 \le i, j \le \ell, H' \in \mathcal{H}\}$, where $F_{i,j,H'}$ denote the bipartite graph on the vertex set $V \times W$ such that (a) the induced subgraph between V_i and W_j is H', and (b) there are no other edges. Let $p = |H|/m^2$, and q be the uniform probability distribution over $\mathcal{D}(m, \ell, H)$.

Theorem 2 There exists a constant $\lambda > 0$ such that any algorithm B which solves the identification problem for $\mathcal{D}(m, \ell, H)$ must satisfy $\bar{C}_q(B) \ge \lambda \ell^2 / p$.

Proof. For any $H' \in \mathcal{H}$, let

$$S(H') = \frac{1}{\ell^2} \sum_{1 \le i,j \le \ell} \mathrm{cost}(B, F_{i,j,H'}). \tag{7}$$

Clearly, for a random $H' \in \mathcal{H}$, we have $E(S(H')) = \bar{C}_q(B)$. This implies that

$$\Pr\{S(H') \le 4\bar{C}_q(B)\} \ge \frac{3}{4}. \tag{8}$$

Suppose the graph $F_{i,j,H'}$ is input to B. Let $d(i,j,H')$-1 be the number of queries in Q_{ij} having been asked at the time just before the first nonzero entry is discovered. Now take a random $H' \in \mathcal{H}$, and for each i, j, let Z_{ij} be the event that $d(i,j,H') > \frac{1}{100p}$. Let $Z = \sum_{1 \le i,j \le \ell} Z_{ij}$.

Fact 3 $E(Z) \ge \frac{63}{80}\ell^2$.

If $p > 1/100$, then all events Z_{ij} always happen, and in this case $E(Z) = \ell^2$. We can thus assume that $p \le 1/100$. Let $k = \lfloor 1/(100p) \rfloor$, then $k \ge 1$. Let Λ be the path in B, when the empty bipartite graph is the input, and let $a_{(i-1)m+s_1,(j-1)m+t_1}, a_{(i-1)m+s_2,(j-1)m+t_2}, \ldots, a_{(i-1)m+s_r,(j-1)m+t_r}$ be the sequence of queries in Q_{ij} asked along Λ. Clearly $r \ge 1$. Let k' =min$\{k, r\}$, and define an $m \times m$ bipartite graph L on $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, m\}$ with edge set $\{(s_1, t_1), (s_2, t_2), \ldots, (s_{k'}, t_{k'})\}$.

To prove Fact 3, it suffices to show that $E(Z_{ij}) \ge 63/80$ for all i, j. Fix i, j and take a random $H' \in \mathcal{H}$. For input $F_{i,j,H'}$, the traversed path in B will follow Λ at least until an edge is discovered. For Z_{ij} not to happen, H' must contain at least one edge from $\{(v_{(i-1)m+s_1}, w_{(j-1)m+t_1}), (v_{(i-1)m+s_2}, w_{(j-1)m+t_2}), \ldots, (v_{(i-1)m+s_{k'}}, w_{(j-1)m+t_{k'}})\}$. That means that the probability for Z_{ij} not to happen is at most γ, which is defined as the probability for a random $H' \in \mathcal{H}$ to contain at least an edge from L. From Lemma 1, $\gamma \leq k'|H|/m^2 \leq 1/100$. This proves that the probability for Z_{ij} to happen is at least 99/100, which is greater than 63/80. This proves Fact 3.

It follows from Fact 3 that

$$\Pr\{Z \geq \frac{1}{10}\ell^2\} \geq \frac{3}{4}, \tag{9}$$

since otherwise $E(Z) < \frac{3}{4} \cdot \ell^2 + \frac{1}{4} \cdot \frac{1}{10}\ell^2 < \frac{63}{80}\ell^2$. Let D denote the set of all pairs of integers (i, j), where $1 \leq i, j \leq \ell$. We conclude from (8) and (9) that there exist $H' \in \mathcal{H}$ and $D' \subseteq D$ with $|D'| \geq \ell^2/10$ such that

$$\bar{C}_q(B) \geq \frac{1}{4}S(H'), \tag{10}$$

and for all $(i,j) \in D'$,

$$d(i,j,H') > \frac{1}{100p}. \tag{11}$$

Choose any such H' and D'.

For any internal node u of B, let us call the outgoing branch labeled by 0 the *left* branch, and the other one the *right* branch. Let $(i,j) \in D'$ and consider the path traced in B from the root down, when $F_{i,j,H'}$ is the input bipartite graph. Clearly, this path follows the leftmost branch in B until, at some node $u_{i,j}$, a query ”$a_{st} =?$” in $Q_{i,j}$ is asked with an $a_{st} = 1$ response. By (11), at least $\lceil \frac{1}{100p} \rceil$ queries in $Q_{i,j}$ have been asked (counting the one at $u_{i,j}$).

Arrange the set of nodes $u_{i,j}$ for all $(i,j) \in D'$ in increasing distance from the root of B, say, $u_{i_1,j_1}, u_{i_2,j_2}, \ldots, u_{i_r,j_r}$, where $r \geq \lceil \ell^2/10 \rceil$. Clearly, for each $k \geq \lceil \ell^2/20 \rceil$, the total number of queries asked from the root to (and including) u_{i_k,j_k} is at least $\frac{1}{20}\ell^2 \cdot \frac{1}{100p}$. That is,

$$\mathrm{cost}(B, F_{i_k,j_k,H'}) \geq \frac{\beta\ell^2}{p}, \tag{12}$$

where $\beta = 1/2000$. Now the number of such k's is at least $\lceil \frac{1}{10}\ell^2 \rceil - \lceil \frac{1}{20}\ell^2 \rceil + 1 \geq \frac{1}{20}\ell^2$. Thus, from (7) and (12), we have

$$S(H') \geq \frac{\beta\ell^2}{20p}. \tag{13}$$

It follows from (10) and (13) that

$$\bar{C}_q(B) \geq \frac{\beta\ell^2}{80p}.$$

This completes the proof of Theorem 2.□

Before discussing the second class of identification problems, we will prove an auxiliary result. Let H be an $m \times m$ bipartite graph with $r > 0$ edges, and $\mathcal{H}$ be the family of all bipartite graphs isomorphic to H. Let $t = \lfloor m^2/(1000r) \rfloor$. Let A be a decision-tree procedure that tries to locate at least one edge of any input $H' \in \mathcal{H}$, by asking an adaptive series of t queries "$a_{i_1 j_1}$ =?", "$a_{i_2 j_2}$ =?", ..., "$a_{i_t j_t}$ =?". Now, consider a random input H' uniformly chosen from $\mathcal{H}$. Let ξ_A be the probability that A succeeds in receiving at least one positive answer, i.e. some query receives an answer "$a_{i_s j_s}$ =1".

Lemma 7 $\xi_A \leq 1/500$.

Proof. If $r > m^2/1000$, then $t = 0$ and $\xi_A = 1$. We can thus assume that $0 < p \leq 1/1000$, where $p = r/m^2$. For $1 \leq k \leq t$, let X_k be the event that $a_{i_s j_s} = 0$ for all $1 \leq s \leq k$; let Y_k be the event that $a_{i_k j_k} = 1$. Let $\alpha_k = \Pr\{X_k\}$ and $\gamma_k = \Pr\{Y_k \mid X_{k-1}\}$ for $1 \leq k \leq t$, where we interpret γ_1 as $\Pr\{Y_1\}$. We will prove inductively that, for $1 \leq k \leq t$,

$$\alpha_k \geq 499/500, \text{ and } \gamma_k \leq 2p. \tag{14}$$

For $k = 1$, observe that the choice of the first query is uniquely determined. Using Lemma 1 with $|E_L| = 1$, we have $\gamma_1 = \Pr\{a_{i_1 j_1} = 1\} \leq r/m^2 \leq 2p$, and $\alpha_1 = 1 - \gamma_1 \geq 499/500$.

Let $1 < k \leq t$, and assume that we have proved (14) for all values less that k. We will prove (14) for the value k. When X_{k-1} occurs, the next query is uniquely determined, say, "$a_{jj'}$=?". Utilizing Lemma 1 and the inductive hypothesis $\alpha_{k-1} \geq 499/500$, we have

$$\begin{aligned}
\gamma_k &= \frac{\Pr\{Y_k \wedge X_{k-1}\}}{\Pr\{X_{k-1}\}} \\
&\leq \frac{\Pr\{a_{jj'} = 1\}}{\alpha_{k-1}} \\
&\leq \frac{r}{m^2 \alpha_{k-1}} \\
&\leq 2p.
\end{aligned}$$

Also, we have

$$\begin{aligned}
\alpha_k &= 1 - \Pr\{Y_1\} - \Pr\{X_1 \wedge Y_2\} - \Pr\{X_2 \wedge Y_3\} - \cdots - \Pr\{X_{k-1} \wedge Y_k\} \\
&= 1 - \Pr\{Y_1\} - \Pr\{X_1\}\Pr\{Y_2 \mid X_1\} - \Pr\{X_2\}\Pr\{Y_3 \mid X_2\} - \cdots - \Pr\{X_{k-1}\}\Pr\{Y_k \mid X_{k-1}\} \\
&\geq 1 - \Pr\{Y_1\} - \Pr\{Y_2 \mid X_1\} - \Pr\{Y_3 \mid X_2\} - \cdots - \Pr\{Y_k \mid X_{k-1}\} \\
&= 1 - (\gamma_1 + \gamma_2 + \cdots + \gamma_k) \\
&\geq 1 - 2pk \\
&\geq 499/500.
\end{aligned}$$

This completes the inductive proof of (14). Lemma 7 follows immediately from (14), since $\xi_A = 1 - \alpha_t$.□

The second class of identification problems is parametrized by a triplet $(m, \ell, \tilde{H})$, where $m, \ell > 0$ are integers and $\tilde{H} = (H_1, H_2, \ldots, H_\ell)$ is a sequence of m by m non-empty bipartite graphs. Let $\mathcal{H}_i$ be the set of all m by m bipartite graphs isomorphic to H_i, and let $\tilde{\mathcal{H}} = \mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_\ell$. Let Γ be the set of all permutations on $(1, 2, \ldots, \ell)$. For each $\tilde{z} = (\sigma, \tilde{H}')$, where $\sigma \in \Gamma$ and $\tilde{H}' = (H'_1, H'_2, \ldots, H'_\ell) \in \tilde{\mathcal{H}}$, let $F_{\tilde{z}}$ be the bipartite graph on $V \times W$ such that, for every i, the induced subgraph between V_i and $W_{\sigma(i)}$ is H'_i, and that there are no other edges in $F_{\tilde{z}}$. Let $\mathcal{E}(m, \ell, \tilde{H}) = \{F_{\tilde{z}} \mid \tilde{z} \in (\Gamma, \tilde{\mathcal{H}})\}$. Let $p = \max_i\{|H_i|/m^2\}$, and q be the uniform probability distribution over $\mathcal{E}(m, \ell, \tilde{H})$.

Theorem 3. There exists a constant $\lambda' > 0$ such that any algorithm B which solves the identification problem for $\mathcal{E}(m, \ell, \tilde{H})$ satisfies $\bar{C}_q(B) \geq \lambda' \ell^2 / p$.

Proof. The proof has the same general outline as that of Theorem 2. For any $\tilde{H}' \in \mathcal{H}$, let

$$S(\tilde{H}') = \frac{1}{|\Gamma|} \sum_{\sigma \in \Gamma} \mathrm{cost}(B, F_{(\sigma, \tilde{H}')}). \tag{15}$$

Clearly, for a random $\tilde{H}' \in \tilde{\mathcal{H}}$, we have $E(S(\tilde{H}')) = \bar{C}_q(B)$. This implies that

$$\Pr\{S(\tilde{H}') \leq 4\bar{C}_q(B)\} \geq \frac{3}{4}. \tag{16}$$

For any internal node u of B, we will say that u is of *type* (i, j), if the query at u is contained in Q_{ij}. Let $\tilde{H}' = (\tilde{H}'_1, \tilde{H}'_2, \ldots, \tilde{H}'_\ell)$ be any fixed element in $\tilde{\mathcal{H}}$. For any internal node u of B, if its type is (i, j), let $L(u)$ be the set of queries in $Q_{i,j}$ that are asked along the path from the root down to and including u; suppose that the query at u is ”$a_{\alpha,\beta}$=?”, then we call u a *critical node* (with respect to $\tilde{H}'$), if (a)$(H_i)_{d,e} = 1$ where $1 \leq d, e \leq m$ and $\alpha = im + d$, $\beta = jm + e$, and (b) $(H_i)_{s,t}$=0 for all queries ”$a_{im+s,jm+t}$=?” in $L(u)$ other than the query ”$a_{\alpha,\beta}$=?”. When u is critical, we will call u a *primary* node if $|L(u)| > \frac{1}{1000p}$, and a *secondary* node otherwise. In the above definitions, a critical node u will also be called a *σ-critical node* (with respect to $\tilde{H}'$), for any $\sigma \in \Gamma$ satisfying $\sigma(i) = j$; similarly we will use the terms *primary* and *secondary* σ-critical nodes. Note that a node may be σ-critical for several different σ's.

Now, consider the path $\Delta(\sigma, \tilde{H}')$ in B traversed for input $F_{(\sigma, \tilde{H}')}$.Let $N_1(\sigma, \tilde{H}')$, $N_2(\sigma, \tilde{H}')$ be the number of primary and secondary critical nodes (with respect to $\tilde{H}'$) on path $\Delta(\sigma, \tilde{H}')$. Let $r_1(\sigma, \tilde{H}')$, $r_2(\sigma, \tilde{H}')$ be the number of primary and secondary σ-critical nodes (with respect to $\tilde{H}'$) on path $\Delta(\sigma, \tilde{H}')$.

Fact 4 Along the path $\Delta(\sigma, \tilde{H}')$, no two critical nodes with respect to $\tilde{H}'$ are of the same type. Furthermore, there are exactly ℓ σ-critical nodes with respect to $\tilde{H}'$, one of type $(i, \sigma(i))$ for each $1 \leq i \leq \ell$.

Fact 5 *$N_1(\sigma, \tilde{H}') + N_2(\sigma, \tilde{H}') \leq \ell^2$, and $r_1(\sigma, \tilde{H}') + r_2(\sigma, \tilde{H}') = \ell$.*

Fact 4 is an elementary consequence of the definition of critical nodes. Fact 5 follows from Fact 4.

Now, take a random $\tilde{H}' \in \mathcal{H}$, and for each $\sigma \in \Gamma$, let Z_σ denote the event that $r_1(\sigma, \tilde{H}') > \frac{99}{100}\ell$. Let $Z = \sum_{\sigma \in \Gamma} Z_\sigma$.

Fact 6 $E(Z) \geq \frac{63}{80}|\Gamma|$.

To prove Fact 6, it suffices to show that $E(Z_\sigma) \geq \frac{63}{80}$ for all σ. It follows from Fact 4 that, for any input $F_{(\sigma,\tilde{H}')}$, the path $\Delta(\sigma, \tilde{H}')$ in B will contain exactly ℓ σ-critical nodes, one of type $(i, \sigma(i))$ for each $1 \leq i \leq n$, with respect to H'; let $u_i(\sigma, \tilde{H}')$ denote the σ-critical node of type $(i, \sigma(i))$, i.e. the node at which the first edge between V_i and $W_{\sigma(i)}$ is discovered. For any fixed σ, take a random $\tilde{H}'$, and let $Z_{\sigma,i}$ be the event that $u_i(\sigma, \tilde{H}')$ is primary. By Lemma 7, if we fix the values of all components H'_j of $\tilde{H}'$ with $j \neq i$ and pick a random H'_i, then the probability of discovering an edge between the i-th block of V and the $\sigma(i)$-th block of W in no more than $\lfloor \frac{1}{1000p} \rfloor$ queries in Q_{ij} is at most $1/500$. This shows that $\Pr\{\neg Z_{\sigma,i}\} \leq 1/500$. Thus, $\Pr\{Z_{\sigma,i}\} \geq 499/500$.

Let $T_\sigma = \sum_{1 \leq i \leq \ell} Z_{\sigma,i}$. Then $E(T_\sigma) \geq \frac{499}{500}\ell$. Observe that $E(Z_\sigma) = \Pr\{T_\sigma > \frac{99}{100}\ell\}$. We conclude that $E(Z_\sigma) \geq \frac{63}{80}$, since otherwise

$$\begin{aligned} E(T_\sigma) &\leq \Pr\{T_\sigma > \frac{99}{100}\ell\} \cdot \ell + \Pr\{T_\sigma \leq \frac{99}{100}\ell\} \cdot \frac{99}{100}\ell \\ &\leq \frac{63}{80} \cdot \ell + \frac{17}{80} \cdot \frac{99}{100}\ell \\ &< \frac{499}{500}\ell. \end{aligned}$$

This proves Fact 6.

In the same way that (9) follows from Fact 3, it follows from Fact 6 that

$$\Pr\{Z \geq \frac{1}{10}|\Gamma|\} \geq \frac{3}{4}. \tag{17}$$

From (16) and (17), we conclude that there exist $\tilde{H}' \in \tilde{\mathcal{H}}$ and $\Gamma' \subseteq \Gamma$ with $|\Gamma'| \geq \frac{1}{10}|\Gamma|$ such that

$$\bar{C}_q(B) \geq \frac{1}{4} S(\tilde{H}'), \tag{18}$$

and for all $\sigma \in \Gamma'$,

$$r_1(\sigma, \tilde{H}') > \frac{99}{100}\ell. \tag{19}$$

Choose any such $\tilde{H}'$ and Γ'.

To complete the proof of Theorem 3, our strategy is to use (19) to show that there exists a large subset $\Gamma'' \subseteq \Gamma$ such that, for all $\sigma \in \Gamma''$, we have cost$(B,\ F_{(\sigma,\tilde{H}')})$=$\Omega(\ell^2/p)$; the theorem then follows from (15) and (18).

Consider the set of paths $\{\Delta(\sigma,\tilde{H}') \mid \sigma \in \Gamma'\}$. Clearly $\Delta(\sigma,\tilde{H}') \neq \Delta(\sigma',\tilde{H}')$ if $\sigma \neq \sigma'$. To each $\Delta(\sigma,\tilde{H}')$, we associate an $(\ell+1)$-tuple $\xi(\sigma,\tilde{H}') = (k, i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_{\ell-k})$ as described below. In what follows, "critical nodes" will mean critical nodes with respect to $\tilde{H}'$; the same is true for σ-critical nodes, primary critical nodes, etc.

Let $y_1, y_2, \ldots, y_{N_1(\sigma,\tilde{H}')}$ be the sequence of primary critical nodes along $\Delta(\sigma,\tilde{H}')$, and $z_1, z_2, \ldots, z_{N_2(\sigma,\tilde{H}')}$ be the sequence of secondary critical nodes along $\Delta(\sigma,\tilde{H}')$; let $y_{i_1}, y_{i_2}, \ldots, y_{i_k}$ be the subsequence consisting of all the primary σ-critical nodes, and $z_{j_1}, z_{j_2}, \ldots, z_{j_{\ell-k}}$ be the subsequence consisting of all the secondary σ-critical nodes. Define $\xi(\sigma,\tilde{H}') = (k, i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_{\ell-k})$. Note that $0 \leq k \leq \ell$, $1 \leq i_s \leq N_1(\sigma,\tilde{H}')$, and $1 \leq j_t \leq N_2(\sigma,\tilde{H}')$ for all s,t. Let $\Gamma'' = \{\sigma \mid \sigma \in \Gamma', N_1(\sigma,\tilde{H}') > \ell^2/5000\}$.

Fact 7 If σ and σ' are distinct, then $\xi(\sigma,\tilde{H}') \neq \xi(\sigma',\tilde{H}')$.

Given the value of $\xi(\sigma,\tilde{H}') = (k, i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_{\ell-k})$, we show that there is a unique path in B that gives rise to $\xi(\sigma,\tilde{H}')$. Starting from the root, whenever we encounter an internal node u, the only possible path giving rise to $\xi(\sigma,\tilde{H}')$ is clearly determined by the following rules: (a) if u is a critical node, $\xi(\sigma,\tilde{H}') = (k, i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_{\ell-k})$ tells us whether u is σ-critical, since we can count how many primary and secondary critical nodes have been seen along the path so far; we will take the branch labeled by 1 if and only if u is σ-critical; (b) if u is not critical, and suppose the query at u is in Q_{ij}, then *either* we have so far not seen a critical node of type (i,j), in which case we should take the 0-branch, *or* we have already seen a critical node of type (i,j), in which case we know that the induced subgraph of input between the i-th block of V and the j-th block of W is H_i, and we can decide from H_i which branch to take. This determines the path and thus the σ uniquely. This proves Fact 7.

Fact 8 $|\Gamma''| \geq \frac{1}{2}|\Gamma'|$.

From Fact 7, we can find an upper bound to $|\Gamma' - \Gamma''|$ by counting the number of possible values of $\xi(\sigma,\tilde{H}') = (k, i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_{\ell-k})$. Let $a = \lceil 99\ell/100 \rceil$ and $b = \lfloor \ell^2/5000 \rfloor$. Inequality (19) says that $k \geq a$, Fact 5 says that $j_t \leq \ell^2$ for all t, and the constraint that $N_1(\sigma,\tilde{H}') \leq \ell^2/5000$ for such σ's says that $i_s \leq b$ for all s. It follows that

$$\begin{aligned}|\Gamma' - \Gamma''| &\leq \sum_{a \leq k \leq \ell} \binom{b}{k} \binom{\ell^2}{\ell-k} \\ &\leq \sum_{a \leq k \leq \ell} \frac{b^k}{k!} \frac{\ell^{2(\ell-k)}}{(\ell-k)!}\end{aligned}$$

$$\begin{aligned} &= \sum_{a\le k\le \ell} \binom{\ell}{k} \frac{b^k \ell^{2(\ell-k)}}{\ell!} \\ &\le \sum_{a\le k\le \ell} \binom{\ell}{k} \frac{\ell^{2\ell}}{(5000)^k \ell!} \\ &\le \sum_{a\le k\le \ell} \binom{\ell}{k} \frac{\ell^{2\ell}}{(5000)^a \ell!} \\ &\le \sum_{a\le k\le \ell} \binom{\ell}{k} \frac{\ell^{2\ell}}{(2000)^\ell \ell!} \\ &\le 2^\ell \frac{\ell^{2\ell}}{(2000)^\ell \ell!}. \end{aligned}$$

Now, $(\ell!)^2 \ge (\ell/e)^{2\ell}$ for all $\ell \ge 1$. That means $\ell^{2\ell}/(\ell!) \le e^{2\ell}\ell!$. Noting that $|\Gamma'| \ge |\Gamma|/10$, we have

$$\begin{aligned} |\Gamma' - \Gamma''| &\le (\frac{2e^2}{2000})^\ell \ell! \\ &\le \frac{1}{20}|\Gamma| \\ &\le \frac{1}{2}|\Gamma'|. \end{aligned}$$

This proves Fact 8.

Now, preceding each primary critical node of type (i,j), there are at least $\lceil 1/1000p \rceil - 1$ nodes with queries in Q_{ij} along the path $\Delta(\sigma, \tilde{H}')$. Fact 4 guarantees that there are $N_1(\sigma, \tilde{H}')$ primary critical nodes of distinctly different types. This proves the next fact.

Fact 9 For all $\sigma \in \Gamma''$, $\mathrm{cost}(B,\, F_{(\sigma,\tilde{H}')})$ is at least $N_1(\sigma, \tilde{H}')/(1000p)$.

From Facts 8 and 9, we have, with $\beta' = 10^{-7}$,

$$\begin{aligned} \sum_{\sigma\in\Gamma'} \mathrm{cost}(B, F_{(\sigma,\tilde{H}')}) &\ge \frac{1}{2}|\Gamma'| \cdot \frac{1}{5000}\ell^2 \frac{1}{1000p}, \\ &= \frac{\beta' |\Gamma'| \ell^2}{p}. \end{aligned}$$

As $|\Gamma'| \ge \frac{1}{10}|\Gamma|$, we obtain from (15),

$$S(\tilde{H}') \ge \frac{\beta' \ell^2}{10p}. \tag{20}$$

It follows from (18) and (20) that

$$\bar{C}_q(B) \ge \frac{\beta' \ell^2}{40p}$$

This proves Theorem 3.□

5 Proof of Proposition 2

The proof uses results from the last section and a technique of finding embedded bipartite graph properties from graph properties used by Rivest and Vuillemin [RV]. As in [RV], we use the notation $A+B+C$ for the graph obtained from taking the disjoint union of graphs A, B, C (with disjoint vertex sets); for any integer j, jA means $A + A + \cdots + A$ j times. Let N_0' be any fixed integer that satisfies $\log_2 N_0' \geq 13 + \lceil 10^{3/\epsilon} \rceil$. Thus, $(\log_2 n)^{\epsilon/3} \geq 10$ for all $n \geq N_0'/8$.

We first prove $R(P) = \Omega(n(\log n)^{\epsilon/3})$ when $n = 2^k$ with integral k and $n \geq N_0'/8$. Let $L_i = 2^{k-i}K_{2^i}$ for $0 \leq i \leq k$. Since $P \in \mathcal{P}_n$, there exists $0 \leq i_0 < k$ such that $P(L_{i_0}) = 0$ and $P(L_{i_0+1}) = 1$. (Such a sequence was employed in [RV].) We consider two cases depending on the value of 2^{i_0}.

Suppose $2^{i_0} \geq n/((\log_2 n)^{2\epsilon/3})$. Let $H_j = jK_{2^{i_0+1}} + (2^{k-i_0} - 2j)K_{2^{i_0}}$ for $j = 0, 1, 2, \ldots, 2^{k-i_0-1}$. Thus $H_0 = L_{i_0}$, and $H_{2^{k-i_0-1}} = L_{i_0+1}$. Since $P \in \mathcal{P}_n$, there exists $0 \leq j_0 < 2^{k-i_0-1}$ such that $P(H_{j_0}) = 0$ and $P(H_{j_0+1}) = 1$. Write $H_{j_0} = J + I_1 + I_2$, $H_{j_0+1} = J + I_3$, where I_1, I_2 are complete graphs on disjoint vertex sets V_1, V_2 with $|V_1| = |V_2| = 2^{i_0}$, and I_3 is the complete graph on $V_1 \cup V_2$.

Let Q be the bipartite graph property on the vertex set $V_1 \times V_2$ obtained from P by setting all the edges as present or absent exactly as H_{j_0} *except* for the ones in $V_1 \times V_2$. Clearly, $R(P) \geq R(Q)$. As Q is nontrivial and monotone, we have by assumption $R(Q) = \Omega(2^{i_0}(\log 2^{i_0})^{\epsilon}) = \Omega(n(\log n)^{\epsilon/3})$.

We now consider the case

$$2^{i_0} < \frac{n}{(\log_2 n)^{2\epsilon/3}}. \tag{21}$$

Let V denote the disjoint union of sets V_i, $1 \leq i \leq \ell \equiv 2^{k-i_0-1}$, where $|V_i| = 2^{i_0}$; similarly let $W = \cup_{1 \leq i \leq \ell} W_i$. Let $x_{ij,ab}$ be Boolean variables, where $1 \leq i, j \leq \ell$ and $1 \leq a, b \leq 2^{i_0}$. Consider the sequence $\langle x_{ij,ab} \rangle$ of ℓ_0 variables $x_{ij,ab}$ arranged in increasing lexicographical order of their indices (i, j, a, b), where $\ell_0 = \ell^2 2^{2i_0}$. For any truth assignment $\tilde{x} \in \{0,1\}^{\ell_0}$ to $\langle x_{ij,ab} \rangle$, let $G_{\tilde{x}} \in \mathcal{G}_n$ denote the graph on the vertex set $V \cup W$ defined as follows: each V_i is a clique and each W_i is a clique for $1 \leq i \leq \ell$; if $x_{ij,ab} = 1$ then there is an edge (v_c, w_d) for $c = i\ell + a$ and $d = j\ell + b$; there are no other edges.

We will later construct a probabiliity distribution q over $\mathcal{G}_n$, with $q(G) = 0$ unless $G = G_{\tilde{x}}$ for some $\tilde{x}$, and prove that $\bar{C}_q(A) = \Omega(n(\log_2 n)^{\epsilon/3})$ for all $A \in \mathcal{A}_P$, To help describing q, we first construct a $G_{\tilde{y}}$ satisfying $P(G_{\tilde{y}}) = 1$ with a certain minimality property.

Let $\tilde{x}^{(0)}$ denote the truth assignment to $\langle x_{ij,ab} \rangle$ with all $x_{ij,ab} = 0$. Let $\tilde{x}^{(1)}$ be the truth assignment where $x_{ij,ab} = 1$ if $i = j$, and $x_{ij,ab} = 0$ otherwise. Then $G_{\tilde{x}^{(0)}} = L_{i_0}$ and $G_{\tilde{x}^{(1)}} = L_{i_0+1}$;

hence $P(G_{\tilde{x}^{(0)}}) = 0$ and $P(G_{\tilde{x}^{(1)}}) = 1$. Let $X = \{\tilde{x} \mid \tilde{x} \in \{0,1\}^{\ell_0}, \tilde{x} \le \tilde{x}^{(1)}, P(G_{\tilde{x}}) = 1$, and $P(G_{\tilde{z}}) = 0$ for all $\tilde{z} < \tilde{x}\}$. Each $G_{\tilde{x}}$, where $\tilde{x} \in X$, is called an *induced minimal graph* for P. Let $\#(\tilde{x})$ denote the number of 1's in $\tilde{x}$. The next statement is clearly true.

Fact 10 If there is an $\tilde{x} \in X$ with $\#(\tilde{x}) \ge n(\log_2 n)^{\epsilon/3}$, then $R(P) = \Omega(n(\log_2 n)^{\epsilon/3})$.

We can thus assume that, for all $\tilde{x} \in X$,

$$\#(\tilde{x}) < n(\log_2 n)^{\epsilon/3}. \tag{22}$$

For each $\tilde{x} = \langle x_{ij,ab} \rangle \in X$, let $J_i(\tilde{x}) = \{(a,b) \mid x_{ii,ab} = 1\}$ for $1 \le i \le \ell$. Let $\alpha(\tilde{x}) = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ denote the multi-set $\{|J_1(\tilde{x})|, |J_2(\tilde{x})|, \ldots, |J_\ell(\tilde{x})|\}$ sorted into decreasing order; say $\alpha_1 \ge \alpha_2 \ge \ldots \ge \alpha_{s(\tilde{x})} > 0$, and $\alpha_i = 0$ for $s(\tilde{x}) < i \le \ell$. Let $\tilde{y} = \langle y_{ij,ab} \rangle \in X$ be chosen such that $\alpha(\tilde{y}) \le \alpha(\tilde{x})$ lexicographically for all $\tilde{x} \in X$. We can choose $\tilde{y}$ so that we have $\alpha_i = |J_i(\tilde{y})|$ for $1 \le i \le \ell$ where $(\alpha_1, \alpha_2, \ldots, \alpha_\ell) = \alpha(\tilde{y})$. Clearly,

$$\#(\tilde{y}) = \alpha_1 + \alpha_2 + \ldots + \alpha_{s(\tilde{y})}. \tag{23}$$

Let $m = 2^{i_0}$, and

$$\mu = \frac{\#(\tilde{y})}{s(\tilde{y})}. \tag{24}$$

We will choose our distribution q in several different ways depending on the value of μ and m.

Lemma 8 If $\mu \ge 4m(\log_2 n)^{\epsilon/3}$, then $R(P) = \Omega(n(\log_2 n)^{\epsilon/3})$.

Proof. From (22) and (24),

$$s(\tilde{y}) < \frac{1}{2}\ell. \tag{25}$$

From (23) and (24),

$$\alpha_1 \ge 4m(\log_2 n)^{\epsilon/3}. \tag{26}$$

We now define a probability distribution q on $\mathcal{G}_n$ by generating a random $G \in \mathcal{G}_n$. Let $\tilde{z} = \langle z_{ij,ab} \rangle$ be defined as follows for all a, b: $z_{ii,ab} = y_{11,ab}$ for $i \in \{1, s(\tilde{y})+1, s(\tilde{y})+2, \ldots, \ell\}$, $z_{ii,ab} = y_{ii,ab}$ for $2 \le i \le s(\tilde{y})$, and $z_{ij,ab} = 0$ otherwise. Now pick a random sequence $\zeta = (a_1, b_1), (a_{s(\tilde{y})+1}, b_{s(\tilde{y})+1}), (a_{s(\tilde{y})+2}, b_{s(\tilde{y})+2}), \ldots, (a_\ell, b_\ell)$, where each (a_i, b_i) is uniformly and independently chosen from $J_1(\tilde{y})$. Let $\tilde{z}(\zeta)$ be obtained from $\tilde{z} = \langle z_{ij,ab} \rangle$ by setting $z_{ii,a_ib_i} = 0$ for $i \in \{1, s(\tilde{y})+1, s(\tilde{y})+2, \ldots, \ell\}$. Let the graph $G_{\tilde{z}(\zeta)}$ be the random $G \in \mathcal{G}_n$. This defines q.

Let $A \in \mathcal{A}_P$. Then at each leaf ρ of A, the sequence of queries asked along the path from the root to ρ must include "$z_{ii,a_ib_i} =?$" for every $i \in \{1, s(\tilde{y})+1, s(\tilde{y})+2, \ldots, \ell\}$. This is because

$P(G_{\tilde{z}(\zeta)}) = 0$ for all ζ (since $\tilde{y}$ is a lexicographically smallest element of X), while for any $\tilde{z}'$ that differs from $\tilde{z}(\zeta)$ only in some z_{ii,a_ib_i}, one has $P(G_{\tilde{z}'}) = 1$. Clearly, for a random G distributed according to q, we have $\bar{C}_q(A) \geq \sum_{s(\tilde{y})<i\leq \ell} E(D_i)$, where D_i is the random variable denoting the number of queries of the type "$z_{ii,ab}$ =?" that have been asked before the query "z_{ii,a_ib_i} =?" is asked. Clearly,

$$E(D_i) \geq \sum_{0\leq j<\alpha_1} \frac{\alpha_1 - j}{\alpha_1} = \frac{1}{2}(1+\alpha_1).$$

Thus, $\bar{C}_q(A) \geq (\ell - s(\tilde{y}))\frac{1}{2}(1+\alpha_1) = \Omega(n(\log_2 n)^{\epsilon/3})$ by (25) and (26). This proves Lemma 8.□

Lemma 9 *If* $\mu < 4m(\log_2 n)^{\epsilon/3}$, *then* $R(P) = \Omega(n(\log_2 n)^{\epsilon/3})$.

Proof. We will construct probability distributions q over $\mathcal{G}_n$, and show that any algorithms A for determining P must have $\bar{C}_q(A) = \Omega(n(\log_2 n)^{\epsilon/3})$. We distinguish two cases. First consider the case $s(\tilde{y}) < \ell/2$. Let $H = (h_{ab})$ be the m by m bipartite graph corresponding to the edge set $J_{s(\tilde{y})}(\tilde{y})$, i.e. $h_{ab} = y_{s(\tilde{y})s(\tilde{y}),ab}$ for $1 \leq a,b \leq m$. Let $\mathcal{H}$ be the set of all m by m bipartite graphs H' isomorphic to H. For each $\zeta = (s,t,H')$, where $s(\tilde{y}) \leq s,t \leq \ell$ and $H' = (h'_{ab}) \in \mathcal{H}$, define $\tilde{z}(\zeta) = (x_{ij,ab}) \in \{0,1\}^{\ell_0}$ as follows:

$$\begin{cases} x_{ii,ab} = y_{ii,ab} & \text{for} \quad 1 \leq i < s(\tilde{y}), \quad 1 \leq a,b \leq m \\ x_{st,ab} = h'_{ab} & \text{for} \quad 1 \leq a,b \leq m \\ x_{ij,ab} = 0 & \text{otherwise.} \end{cases}$$

The distribution q over $\mathcal{G}_n$ is generated by taking a random $\zeta = (s,t,H')$, where each of s,t,H' is uniformly and independently chosen from its domain, and let $G_{\tilde{z}(\zeta)}$ be the random G to be generated. If we restrict our attention to the variables $x_{ij,ab}$ with $s(\tilde{y}) \leq i,j \leq \ell$ and $1 \leq a,b \leq m$, the problem for determining P now becomes the identification problem for $\mathcal{D}(m,(\ell - s(\tilde{y})+1),H)$. In fact, any algorithm $A \in \mathcal{A}_P$ naturally induces an algorithm B for the identification problem $\mathcal{D}(m,(\ell - s(\tilde{y})+1),H)$ such that $\bar{C}_{q_0}(B) \leq \bar{C}_q(A)$, where q_0 is the uniform distribution for $\mathcal{D}$ discussed in Section 4. By Theorem 2, we have

$$\begin{aligned} C_{q_0}(B) &= \Omega((\ell - s(\tilde{y})+1)^2 m^2/|H|) \\ &= \Omega(\ell^2 m^2/\mu) \\ &= \Omega(n^2/(m(\log n)^{\epsilon/3})). \end{aligned}$$

Since $m = O(n/(\log n)^{2\epsilon/3})$, we have proved Lemma 9 for this case.

Now consider the case $s(\tilde{y}) \geq \ell/2$. Let $s_0 = \lceil s(\tilde{y})/2 \rceil$. For each $s_0 \leq i \leq s(\tilde{y})$, let H_i denote the m by m bipartite graph corresponding to the edge set $J_i(\tilde{y})$; clearly, $|H_i| \leq \mu$. Let $\mathcal{H}_i$ be the set of all m by m bipartite graphs isomorphic to H_i. Let Γ be the set of all permutations of $(s_0, s_0+1, \ldots, s(\tilde{y}))$. For each $\zeta = (\sigma, H'_{s_0}, H'_{s_0+1}, \ldots, H'_{s(\tilde{y})})$, where $\sigma \in \Gamma$ and $H'_i \in \mathcal{H}_i$, define

$\tilde{z}(\zeta) = (x_{ij,ab}) \in \{0,1\}^{\ell_0}$ as follows:

$$\begin{cases} x_{ii,ab} = y_{ii,ab} & \text{for} \quad 1 \leq i < s_0, \quad 1 \leq a,b \leq m \\ x_{i\sigma(i),ab} = (H_i')_{ab} & \text{for} \quad s_0 \leq i \leq s(\tilde{y}), \quad 1 \leq a,b \leq m \\ x_{ij,ab} = 0 & \text{otherwise.} \end{cases}$$

The distribution q over $\mathcal{G}_n$ is generated by taking a random ζ, where each component of ζ is uniformly and independently chosen from its domain, and let $G_{\tilde{z}(\zeta)}$ be the random G to be generated. If we restrict our attention to the variables $x_{ij,ab}$ with $s_0 \leq i,j \leq s(\tilde{y})$ and $1 \leq a,b \leq m$, the problem for determining P now becomes the identification problem for $\mathcal{E}(m,(s(\tilde{y})-s_0+1), H'_{s_0}, H'_{s_0+1}, \ldots, H'_{s(\tilde{y})})$ with the uniform distribution discussed in Section 4. Let $p = \max_i\{|H_i|/m^2|\}$. Then $p \leq \mu/m^2$. It follows then from Theorem 3 that, for every algorithm $A \in \mathcal{A}_P$, we have

$$\begin{aligned} C_q(A) &= \Omega((s(\tilde{y}) - s_0 + 1)^2/p) \\ &= \Omega(\ell^2 m^2/\mu) \\ &= \Omega(n^2/(m(\log n)^{\epsilon/3})). \end{aligned}$$

Since $m = O(n/(\log n)^{2\epsilon/3})$, we have proved Lemma 9 for this last case. This completes the proof of Lemma 9.□

We have proved that, when $n \geq N_0'/8$ is a power of 2, $R(P) = \Omega(n(\log_2 n)^{\epsilon/3})$. We now prove it for all integers $n \geq N_0'$. We divide the discussion into two cases.

First, suppose $n = 2^k + 2^\ell + t$ where $0 \leq t < 2^\ell$ and $\ell \leq k-2$. Let V be the disjoint union of V_1, V_2, V_3 with $|V_1| = |V_2| = 2^{k-1}$, $|V_3| = 2^\ell + t$. Let P be a nontrivial monotone graph property on the vertex set V. Consider the following sequence of graphs on vertex set V: G_0 is the empty graph, $G_1 = K_{V_3}$, $G_2 = K_{V_2} \cup G_1$, $G_3 = K_{V_1} \cup G_2$, $G_4 = K_{V_3 \times V_2} \cup G_3$, $G_5 = K_{V_3 \times V_1} \cup G_4$, $G_6 = K_V$. (Here union and equality on graphs only refer to their edge sets.) Let i be the minimum i such that $P(G_i) = 1$.

If $i = 1$, then by monotonicity $P(G_1') = 1$ where $G_1' = \{K_{V_2}\}$. Let Q be the property induced on the vertex set V_2 defined by $Q((V_2, E)) = P((V, E))$. Then Q is nontrivial and monotone on $|V_2| = 2^{k-1} \geq N_0'/8$ vertices. Thus, $R(P) \geq R(Q) = \Omega(2^{k-1}(\log 2^{k-1})^{\epsilon/3}) = \Omega(n(\log n)^{\epsilon/3})$. The same argument applies when $i = 2$ or 3.

If $i = 4$, then the property Q induced on the bipartite graph $V_2 \times V_1$, defined by $Q((V_2 \times V_1, E)) = P((V, E'))$ where E' is the union of E and all edges in G_3, is nontrivial and monotone. Thus by Theorem 1, $R(P) = R(Q) = \Omega(2^{k-1}(\log 2^{k-1})^\epsilon) = \Omega(n(\log n)^\epsilon)$. A similar argument works for $i = 5$ and $i = 6$.

The only other case is $n = 2^k + 2^{k-1} + t$ where $0 \leq t < 2^{k-1}$. Let V be the disjoint union of V_1, V_2, V_3 with $|V_1| = |V_2| = 2^{k-1}$+t, $|V_3| = 2^{k-1} - t$. Consider the sequence of graphs: G_0 is the empty graph, $G_1 = K_{V_1}$, $G_2 = K_{V_2 \cup V_3} \cup G_1$, $G_3 = K_{V_3 \times V_1} \cup G_2$, $G_4 = K_V$. Let i be the minimum i such that $P(G_i) = 1$. An analysis similar to that for the previous case $n = 2^k + 2^\ell + t$ then leads to $R(P) = \Omega(n(\log n)^{\epsilon/3})$. This completes the proof of Proposition 2.

6 Remarks

We feel that the determination of randomized complexity for Booean properties is a major topic in complexity theory with many interesting unresolved questions. We will mention just a few that have a direct bearing on the present discussion.

1. It remains a tantalizing question whether the randomoized complexity of every nontrivial monotone graph property is of order $\Omega(n^2)$. Recently, King [Kin] has improved our bound from $\Omega(n(\log n)^{1/12})$ to $\Omega(n^{5/4})$. Perhaps the next step is to prove an $\Omega(n^2)$ lower bound to the randomized complexity for monotone bipartite graph properties.

2. By how much can the randomized complexity $r = R(f)$ be smaller than the deterministic omplexity $m = D(f)$ for any Boolean function f? Saks and Wigderson [SW] conjectured that $r = \Omega(m^{.753\cdots})$. Could one prove at least a nonlinear bound, i.e. $r = \Omega(\sqrt{m}h(m))$ with $h(m) \to \infty$? Such a result would be very exciting even just for monotone functions.

3. How much can randomization help in the determination of any (monotone and non-monotone) graph property? As mentioned in the introduction, we know that $r = \Omega(\sqrt{m})$, in the notation of the last paragraph, and that there are examples in which $r \leq (1/2 - \epsilon)m$. Can one prove that $r = \Omega(\sqrt{m}h(m))$ with $h(m) \to \infty$?

References

[Kin] V. King, "An $\Omega(n^{5/4})$ lower bound on the randomized complexity of graph properties," *Proc. 20th Annual ACM Symposium on Theory of Computing*, 1988, to appear.

[Kir] D. Kirkpatrick, "Determining graph properties from matrix representations," *Proc. 6th Annual ACM Symposium on Theory of Computing*, 1974, pp. 84–90.

[MT] U. Manber and M. Tompa, "The complexity of problems on probabilistic, nondeterministic and alternating decision trees," *Journal of ACM* **32** (1985), pp. 720–732.

[M] F. Meyer auf der Heide, "Nondeterministic versus probabilistic linear algorithms," *Proc. 26th Annual IEEE Symposium on Foundations of Computer Science*, 1985, pp. 65–73.

[RV] R. Rivest and S. Vuillemin, "On recognizing graph properites from adjacency matrices," *Theoretical Computer Science*, **3**, 1978, pp. 371–384.

[R] A.L. Rosenberg, "On the time required to recognize properties of graphs: a problem," *SIGACT News* **5**, No. 4, (1973), pp. 15–16.

[SW] M. Saks and A. Wigderson, "Probabilistic Boolean decision trees and the complexity of evaluating game trees," *Proc. 27th Annual IEEE Symposium on Foundations of Computer Science*, 1986, pp. 29–38.

[S] M. Snir, "Lower bounds for probabilistic linear decision trees," *Theoretical Computer Science* **38**, (1985), pp. 69–82.

[Y] A.C. Yao, "Probabilistic computations: towards a unified measure of complexity," *Proc. 18th Annual IEEE Symposium on Foundations of Computer Science*, 1977, pp. 222–227.