JOURNAL OF COMPUTER AND SYSTEM SCIENCES **42**, 267–287 (1991)

Lower Bounds to Randomized Algorithms for Graph Properties*

ANDREW CHI-CHIH YAO

Department of Computer Science, Princeton University, Princeton, New Jersey 08544

Received February 19, 1988; revised November 24, 1988

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. 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 [6] settled the Aanderra–Rosenberg Conjecture [7], proving that $C(P) = \Omega(n^2)$ for every nontrivial monotone graph property P. An intriguing open problem (see [10]) is whether their result remains true when randomized algorithms are allowed. In fact, Richard Karp conjectured (see [8]) 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 [8]) for general Boolean function evaluations (also follows from observations made in Kirkpatrick [3]) that for some inputs the shortest verification needs $\Omega(n)$ entries to be revealed. In this paper we prove the following result which cannot be obtained by using lower bounds on nondeterministic verifications.

THEOREM 1. *$R(P) = \Omega(n(\log n)^{1/2})$ for any nontrivial monotone graph property P on n vertices.*

We also define and study a search problem, which seeks to identify all the edges

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

0022-0000/91 $3.00

571/42/3-2

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. At present no example is known for which randomization can save more than a factor of 2 over the deterministic case. For the general case of Boolean function evaluation, there exist examples by Snir [9], Boppana (see [8]), and Saks and Wigderson [8], 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 [10]. For a study of the randomized of Boolean function evaluation, see Saks and Wigderson [8]. Also see Manber and Tompa [4]. Meyer auf der Heide [5] and Snir [9] 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 $1\leqslant i, j\leqslant n$; we sometimes write $G=(V, E_G)$, where $V=\{v_1, v_2, ..., v_n\}$ and E_G is the *edge set* $\{\{v_i, v_j\}\mid a_{ij}=1\}$. Two graphs $G=(a_{ij})$, $G'=(a'_{ij})$ are *isomorphic* if there exists a permutation σ on $\{1, 2, ..., n\}$ such that $a'_{ij}=1$ if and only if $a_{\sigma(i)\sigma(j)}=1$. Let $\mathscr{G}_n$ denote the set of all G on n vertices. A *graph property* (on n-vertex graphs) is a function $P\colon \mathscr{G}_n\to\{0,1\}$ such that $P(G)=P(G')$ if G, G' are isomorphic. We say P is *nontrivial* if P is not a constant.

Let $G=(a_{ij})$, $G'=(a'_{ij})\in\mathscr{G}_n$. We write $G\leqslant G'$ if $a_{ij}\leqslant a'_{ij}$ for all i, j. A graph property P on n-vertex graphs is *monotone* if $G\leqslant G'$ implies $P(G)\leqslant P(G')$. Let $\mathscr{P}_n$ 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 $a_{i_1j_1}=?$, $a_{i_2j_2}=?$, ..., until $P(G)$ can be determined; the queries are adaptively chosen depending on the answers to previous queries (see, e.g. [6], for more formal descriptions). Without loss of generality, we require that the same query not be asked twice. Let cost(A, G) be the number of queries asked by A when G is the input. Let $\mathscr{A}_P$ denote the set of all decision tree algorithms for P. The *worst case complexity* $C(P)$ is $\min\{\text{cost}(A)\mid A\in\mathscr{A}_P\}$, where cost$(A)$ is defined as $\max\{\text{cost}(A, G)\mid G\in\mathscr{G}_n\}$.

A *randomized decision tree algorithm* is a probability distribution α over $\mathscr{A}_P$. The expected number of queries asked by α for input G is $\sum_{A\in\mathscr{A}_P}\alpha(A)\,\text{cost}(A, G)$, denoted by $h(\alpha, G)$. The cost of α is defined as $\max\{h(\alpha, G)\mid G\in\mathscr{G}_n\}$. 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 [10]).

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 $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$. We sometimes write $G=(V\times W, E_G)$ where $V=\{v_1, v_2, ..., v_m\}$, $W=\{w_1, w_2, ..., w_n\}$, and E_G denotes the *edge set* $\{(v_i, w_j)\mid a_{ij}=1\}$. Two graphs $G=\{a_{ij})$ and $G'=(a'_{ij})$ are *isomorphic* if there exist permutations σ, ρ on $\{1, 2, ..., m\}$, $\{1, 2, ..., n\}$, respectively, such that $a'_{ij}=1$ if and only if $a_{\sigma(i),\rho(j)}=1$. Let $\mathscr{G}_{m,n}$ denote the set of all bipartite graphs on $V\times W$. A *bipartite graph* property is a function $P\colon \mathscr{G}_{m,n}\to\{0,1\}$ such that $P(G)=P(G')$ if G and G' are isomorphic.

Let $\mathscr{P}_{m,n}$ denote the set of all nontrivial monotone bipartite graph properties on $V\times W$, where the concepts of "nontrivial" and "monotone" are straightforward analogs 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 use the same notations, e.g., $\mathrm{cost}(A, G)$ etc., as in graph properties.

Theorem 1 follows immediately from the next two propositions.

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

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

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 use the results in Section 4 and an embedding technique from [6] to prove Proposition 2.

3. PROOF OF PROPOSITION 1

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

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

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

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

DEFINITION 4. Let $P\in\mathscr{P}_{m,n}$. 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 also use $K_{V \times W}$ to denoted 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 nonempty bipartite graphs on $V \times W$, and $\mathscr{H}$ be the family of all bipartite graphs isomorphic to H. Take a random H', uniformly chosen from $\mathscr{H}$, then*

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

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

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

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

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

(c) *$e(G) \cdot e(G') \geqslant mn$ for all $G \in \mathscr{M}_P$, $G' \in \mathscr{M}_Q$.*

Proof. Statements (a) and (b) follow immediately from the definitions. To prove (c), observe that any H isomorphic to G satisfy $E_H \cap E_{G'} \neq \varnothing$; 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 $P \in \mathscr{P}_{m,n}$, and $A \in \mathscr{A}_P$. Let $\bar{C}_q(A)$ be the average value of cost (A, G) when G is distributed according to probability distribution q on $\mathscr{G}_{m,n}$.

To prove Proposition 1, we construct a q and prove that, for all $A \in \mathscr{A}_P$, $\bar{C}_q(A) = \Omega((n \log_2 n)^{1/4})$. This proves Proposition 1, as $R(P) \geqslant \bar{C}_q(A)$ by a general theorem in [10]. For the rest of this section, we let $m = n \geqslant 4$. We assume that $P \in \mathscr{P}_{m,n}$ 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 prooperties. The proof of Lemma 6 is perhaps the most interesting part of the proof of Proposition 1.

LEMMA 3. *If $e(G_P) \geqslant \lambda(n)n$, then $R(P) \geqslant \lambda(n)n$.*

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

LEMMA 4. *If* $e(G_P) \leqslant n/\lambda(n)$, *then* $R(P) \geqslant \lambda(n)n$.

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

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

LEMMA 5. *Let* $n \geqslant N_0$. *If* $d_{\max} \leqslant \mu(n)$, *then* $R(P) \geqslant \frac{1}{4}\lambda(n)n$.

Proof. Let $s = \lceil m/4 \rceil$ and $m' = m - s$. Construct $P_1 \in \mathscr{P}_{m',n}$ from P as described below. For each $G_1 \in \mathscr{G}_{m',n}$ on vertex set $V \times W$, let $G \in \mathscr{G}_{m,n}$ 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, $R(P) \geqslant R(P_1)$; 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 need to prove $R(P_1) \geqslant \frac{1}{4}\lambda(n)n$.

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

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

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

Let $M = \{(v_{k_1}, w_{l_1}), (v_{k_2}, w_{l_2}), ..., (v_{k_t}, w_{l_t})\}$ 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

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

It follows from (1) and (2) that

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

Relabeling the vertices if needed, we can assume that G_0 is a bipartite graph on $V \times W$, where $V = \{v_1, v_2, ..., v_{m'}\}$, $W = \{w_1, w_2, ..., w_n\}$ 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 $\mathscr{D}(G_0)$ be the set of all bipartite graphs on $V \times W$ isomorphic to G_0. We prove

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

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

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

It remains to prove (4). Let Γ be the set of all permutations on V. For any $\sigma \in \Gamma$ and $G \in \mathscr{G}_{m',n}$, let σG denote the resulting graph when each $v_i \in V$ is relabeled $v_{\sigma(i)}$. Then the group Γ acts transitively on the set $\mathscr{H} \equiv \{H \mid H = \sigma G_0 \text{ for some } \sigma \in \Gamma\}$. Let $\Gamma_0 \subseteq \Gamma$ be the set of permutations σ such that $\sigma G_0 = G_0$. By elementary group theory, we have

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

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

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

where $b_i = \text{degree}(w_i)$ in G_0.

From (5) and (6) we obtain

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

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

LEMMA 6. *Let $n \geqslant N_0$. If $d_{\max} > \mu(n)$, then $R(P) \geqslant \frac{1}{80}\lambda(n)n$.*

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 $\geqslant 2\lambda(n)$. 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 $b_i \leqslant 2\lambda(n)$ for $2 \leqslant i \leqslant n'$, 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, $1 \leqslant i \leqslant n$. (Clearly $b_i = |S_i|$). We describe an input distribution of bipartite graphs. Let $T_1 = S_1 - S_{n'}$, $T_2 = S_1 - S_2$, and $T_i = S_1 - (S_{i-1} \cup S_i)$ $3 \leqslant i \leqslant n'$.

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 $v_j \in T_i \cup S_{i-1}$, $2 \leqslant i \leqslant n'$;

(c) Randomly pick a $T_i' \subseteq T_i$ with $\lceil 4\lambda(n) \rceil$ (all such T_i' are equally likely to be chosen), and delete all edges (v_j, w_i) for $v_j \in T_i'$, $2 \leqslant i \leqslant n'$;

(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 $G(\mathscr{B})$ of DIST is specified by the value of $\mathscr{B} = (T_1', T_2', ..., T_{n'}')$. (All other quantities are fixed by P.) We 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 $G(\mathscr{B})$ of DIST satisfies $P(G(\mathscr{B})) = 0$.

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

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

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

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

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

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

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

Consider T_i', $1 \leqslant i \leqslant n'$, as independent random variables. Each T_i' is a uniformly chosen random subset of T_i. Note that $|T_i| \geqslant |S_1| - 4\lambda(n) \geqslant \mu(n) - 4\lambda(n)$, and $|T_i'| \leqslant 4\lambda(n) + 1$. Let $X_i = \{(v_j, w_i) \mid v_j \in T_i\} \cap L_{\mathscr{B}}$. Clearly, for $0 \leqslant l \leqslant |T_i| - |T_i'|$,

$$\begin{aligned} \Pr\{|X_i| > l\} &\geqslant \prod_{0 \leqslant j < l} \frac{|T_i| - |T_i'| - j}{|T_i| - j} \\ &= \binom{|T_i| - l}{|T_i'|} \Big/ \binom{|T_i|}{|T_i'|}. \end{aligned}$$

It follows that

$$\begin{aligned} E(|X_i|) &= \sum_{l \geqslant 0} \Pr\{|X_i| > l\} \\ &\geqslant \binom{|T_i|}{|T_i'|}^{-1} \sum_{0 \leqslant l \leqslant |T_i| - |T_i'|} \binom{|T_i| - l}{|T_i'|} \\ &= \binom{|T_i| + 1}{|T_i'| + 1} \Big/ \binom{|T_i|}{|T_i'|} \\ &= \frac{|T_i| + 1}{|T_i'| + 1} \\ &\geqslant \frac{\mu(n) - 4\lambda(n)}{4\lambda(n) + 2} \\ &\geqslant \frac{1}{40} \lambda(n). \end{aligned}$$

Thus,

$$E(L_{\mathscr{B}}|) \geqslant \sum_{1 \leqslant i \leqslant n'} E(|X_i|)$$
$$\geqslant \frac{1}{40} \lambda(n)\, n'.$$

This proves that for each $A \in \mathscr{A}_P$, $\bar{C}_q(A) \geqslant \frac{1}{80}\lambda(n)n$. This proves Lemma 6. ∎

We have completed the proof of Proposition 1.

4. Identification Problem for Graphs

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

We are interested in two particular classes of identification problems. We first introduce some notations. Let $V = \{v_i \mid 1 \leqslant i \leqslant ml\}$ and $W = \{w_j \mid 1 \leqslant j \leqslant ml\}$ be disjoint sets, where m, l are positive integers. Call the subsets $V_i = \{v_{(i-1)m+s} \mid 1 \leqslant s \leqslant m\}$, $W_j = \{w_{(j-1)m+s} \mid 1 \leqslant s \leqslant m\}$ the ith and the jth *blocks* of V, W. We 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 $1 \leqslant i, j \leqslant l$.

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 nonempty bipartite graph. Let $\mathscr{H}$ be the set of all m by m bipartite graphs isomorphic to H. Let $\mathscr{D}(m, l, H) \subseteq \mathscr{G}_{n,n}$, where $n = ml$, be the set $\{F_{i,j,H'} \mid 1 \leqslant i, j \leqslant l,\ H' \in \mathscr{H}\}$, 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 $p = |E_H|/m^2$, and q be the uniform probability distribution over $\mathscr{D}(m, l, H)$.

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

We first derive a lemma. Let $k > 0$, and B be any decision tree which, for every input $(x_1, x_2, ..., x_k) \in \{0, 1\}^k$, halts either upon finding an $x_i = 1$ or having found $x_i = 0$ for all i. Let q be a probability distribution on $\{0, 1\}^k$. For each $1 \leqslant i \leqslant k$, let q_i be the probability of $x_i = 1$, for a random $(x_1, x_2, ..., x_m)$ distributed according to q. Let $b > 0$.

LEMMA 7. *If $q_i \leqslant b$ for all i, then $\bar{C}_q(B) \geqslant \min\{1/2b, k/2\}$.*

Proof. To fix the notation, let $x_{j_1}, x_{j_2}, ..., x_{j_k}$ be the sequence of entries examined by B when the k-tuple $(0, 0, ..., 0)$ is the input.

Now, consider a random input $(x_1, x_2, ..., x_k)$ distributed according to q, and let Z be the random variable corresponding to the number of entries examined by B. Then $E(Z) = \sum_{i \geqslant 0} \alpha_i$, where $\alpha_i = \Pr\{Z > i\}$. Clearly,

$$\begin{aligned}\alpha_i &= 1 - \Pr\{\exists 1 \leqslant s \leqslant i \text{ such that } x_{j_s} = 1\} \\ &\geqslant 1 - \sum_{1 \leqslant s \leqslant i} \Pr\{x_{j_s} = 1\} \\ &\geqslant 1 - ib.\end{aligned}$$

Writing $t = \min\{\lfloor 1/b \rfloor, k\}$, we have

$$\begin{aligned}E(Z) &\geqslant \sum_{0 \leqslant i \leqslant t} (1 - ib) \\ &= (t+1) - bt(t+1)/2 \\ &\geqslant (t+1)/2.\end{aligned}$$

This proves Lemma 7. ∎

Theorem 2 is an immediate consequence of Lemma 7 with $k = m^2 l^2$ and $b = p/l^2$; $1/2b \leqslant k/2$ in this case.

Before discussing the second class of identification problems, we prove an auxiliary result. Let H be an $m \times m$ bipartite graph with $r > 0$ edges, and $\mathscr{H}$ 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 $H' \in \mathscr{H}$, 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 $\mathscr{H}$. Let ζ_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 8. $\zeta_A \leqslant 1/500$.

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

$$\alpha_k \geqslant 499/500 \qquad \text{and} \qquad \gamma_k \leqslant 2p. \tag{7}$$

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

Let $1 < k \leqslant t$, and assume that we have proved (7) for all values less than k. We prove (7) 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 $\alpha_{k-1} \geqslant 499/500$, we have

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

Also, we have

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

This completes the inductive proof of (7). Lemma 8 follows immediately from (7), since $\zeta_A = 1 - \alpha_t$. ∎

The second class of identification problems is parametrized by a triplet $(m, l, \tilde{H}^{(0)})$, where $m, l > 0$ are integers and $\tilde{H}^{(0)} = (H_1^{(0)}, H_2^{(0)}, \ldots, H_l^{(0)})$ is a sequence of m by m nonempty bipartite graphs. Let $\mathscr{H}_i$ be the set of all m by m bipartite graphs isomorphic to $H_i^{(0)}$, and let $\tilde{\mathscr{H}} = \mathscr{H}_1 \times \mathscr{H}_2 \times \cdots \times \mathscr{H}_l$. Let Γ be the set of all permutations on $(1, 2, \ldots, l)$. For each $\tilde{z} = (\sigma, \tilde{H})$, where $\sigma \in \Gamma$ and $\tilde{H} = (H_1, H_2, \ldots, H_l) \in \tilde{\mathscr{H}}$, 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 $\mathscr{E}(m, l, \tilde{H}^{(0)}) = \{F_{\tilde{z}} \mid \tilde{z} \in (\Gamma, \tilde{\mathscr{H}})\}$. Let $p = \max_i\{|E_{H_i^{(0)}}|/m^2\}$, and q be the uniform probability distribution over $\mathscr{E}(m, l, \tilde{H}^{(0)})$.

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

Proof. We first give the intuition behind the proof. For an input $F_{(\sigma, \tilde{H})}$, B must discover at least one edge between V_i and $W_{\sigma(i)}$ for each $1 \leqslant i \leqslant l$. By Lemma 8, B typically needs to examine $\Omega(1/p)$ entries in $V_i \times W_{\sigma(i)}$ for each i. Furthermore, since

σ is arbitrary, for a typical i, B must search about $\Omega(l)$ blocks of entries of the form $V_i \times W_j$ to have included the block $V_i \times W_{\sigma(i)}$ in the search. Thus, for a typical i, B needs to examine $\Omega(l/p)$ entries in $V_i \times W$. This implies the assertion in Theorem 3. To carry out the proof, consider the path in B followed by the input $F_{(\sigma, \tilde{H})}$. We call a query in Q_{ij} (or precisely, the node asking this query) *primary critical*, if so far B has examined $\Omega(1/p)$ entries in $V_i \times W_j$ without finding any edge. Our approach is to prove that a typical input $F_{(\sigma, \tilde{H})}$ encounters $\Omega(l^2)$ primary critical nodes along its traversed path in B. The argument is developed in two stages. First, we find in a specific way (Lemma 9) a "typical $\tilde{H}$" such that the expected running time (called $S(\tilde{H})$) for input $F_{(\sigma, \tilde{H})}$ for a random σ provides a good estimate of $\bar{C}_q(B)$. Then we derive a lower bound to $S(\tilde{H})$ (Lemmas 10 and 11) using the special property defining $\tilde{H}$.

For any internal node u of B, we say that u is of *type* (i, j), if the query at u is contained in Q_{ij}. Let $\tilde{H} = (H_1, H_2, ..., H_l)$ be any element in $\tilde{\mathscr{H}}$. For any internal node u of B, if its type is (i, j), let $L(u)$ be the set of queries in Q_{ij} 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 $1 \leqslant d$, $e \leqslant m$ 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 call u a *primary* node if $|L(u)| > 1/1000p$, and a *secondary* node otherwise. In the above definitions, a critical node u is also called a *σ-critical node* (with respect to $\tilde{H}$), for any $\sigma \in \Gamma$ satisfying $\sigma(i) = j$; similarly we use the terms *primary* and *secondary* σ-critical nodes. Note that a node may be σ-critical for many different σ's.

Consider the path $\Delta(\sigma, \tilde{H})$ in B traversed by 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 $\Delta(\sigma, \tilde{H})$.

For any $\tilde{H} \in \mathscr{H}$, let

$$S(\tilde{H}) = \frac{1}{|\Gamma|} \sum_{\sigma \in \Gamma} \mathrm{cost}(B, F_{(\sigma, \tilde{H})}). \tag{8}$$

LEMMA 9. *There exist $\tilde{H} \in \tilde{\mathscr{H}}$ and $\Gamma' \subseteq \Gamma$ with $|\Gamma'| \geqslant \frac{1}{10}|\Gamma|$ such that*

$$\bar{C}_q(B) \geqslant \tfrac{1}{4} S(\tilde{H}), \tag{9}$$

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

$$r_1(\sigma, \tilde{H}) > \tfrac{99}{100} l. \tag{10}$$

Choose any $\tilde{H}$ and Γ' satisfying the conditions in Lemma 9. Let $\Gamma'' = \{\sigma \mid \sigma \in \Gamma', N_1(\sigma, \tilde{H}) > l^2/5000\}$.

LEMMA 10. *For all $\sigma \in \Gamma''$,* $\mathrm{cost}(B, F_{(\sigma, \tilde{H})})$ *is at least* $N_1(\sigma, \tilde{H})/(1000p)$.

LEMMA 11. $|\Gamma''| \geqslant \frac{1}{2}|\Gamma'|$.

Assume for the moment that Lemmas 9–11 have been proved. We show how to prove Theorem 3. From Lemma 10 and Lemma 11, we have, with $\beta' = 10^{-7}$,

$$\sum_{\sigma\varepsilon\Gamma''} \operatorname{cost}(B, F_{(\sigma,\tilde{H})}) \geq \frac{1}{2}|\Gamma'| \cdot \frac{1}{5000} l^2 \frac{1}{1000p},$$
$$= \frac{\beta' |\Gamma'| l^2}{p}.$$

As $|\Gamma'| \geq \frac{1}{10}|\Gamma|$, we obtain from (8),

$$S(\tilde{H}) \geq \frac{\beta' l^2}{10p}. \tag{11}$$

It follows from (9) and (11) that

$$\bar{C}_q(B) \geq \frac{\beta' l^2}{40p}.$$

Thus, to complete the proof of Theorem 3, we only need to establish Lemmas 9–11. We first state two elementary facts.

Fact 3. Let $\sigma \in \Gamma$ and $\tilde{H}' \in \tilde{\mathscr{H}}$. Then 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 $1 \leq i \leq l$.

Fact 4. Let $\sigma \in \Gamma$ and $\tilde{H}' \in \tilde{\mathscr{H}}$. Then $N_1(\sigma, \tilde{H}') + N_2(\sigma, \tilde{H}') \leq l^2$, and $r_1(\sigma, \tilde{H}') + r_2(\sigma, \tilde{H}') = l$.

Fact 3 is an elementary consequence of the definition of critical nodes. Fact 4 follows from Fact 3.

Proof of Lemma 9. Take a random $\tilde{H}' \in \mathscr{H}$, and for each $\sigma \in \Gamma$, let Z_σ denote the event that $r_1(\sigma, \tilde{H}') > \frac{99}{100} l$. Let $Z = \sum_{\sigma \in \Gamma} Z_\sigma$. We claim that

$$E(Z) \geq \frac{63}{80} |\Gamma|. \tag{12}$$

Let $\sigma \in \Gamma$. To prove (12), it suffices to show that $E(Z_\sigma) \geq \frac{63}{80}$. By Fact 3, for any input $F_{(\sigma,\tilde{H}')}$, the path $\Delta(\sigma, \tilde{H}')$ in B contains 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. Take a random $\tilde{H}'$, and let $Z_{\sigma,i}$ be the event that $u_i(\sigma, \tilde{H}')$ is a primary critical node with respect to $\tilde{H}'$. By Lemma 8, 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 ith block of V and the $\sigma(i)$th block of W in no more than $\lfloor 1/1000p \rfloor$ 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 $T_\sigma = \sum_{1 \leqslant i \leqslant l} Z_{\sigma,i}$. Then $E(T_\sigma) \geqslant \frac{499}{500} l$. Observe that $E(Z_\sigma) = \Pr\{T_\sigma > \frac{99}{100} l\}$. We conclude that $E(Z_\sigma) \geqslant \frac{63}{80}$, since otherwise

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

This proves (12).

It follows from (12) that

$$\Pr\left\{Z \geqslant \frac{1}{10} |\Gamma|\right\} \geqslant \frac{3}{4}. \tag{13}$$

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

$$\Pr\{S(\tilde{H}') \leqslant 4\bar{C}_q(B)\} \geqslant \frac{3}{4}. \quad \blacksquare \tag{14}$$

Lemma 9 follows from (13) and (14).

Proof of Lemma 10. 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 3 guarantees that there are $N_1(\sigma, \tilde{H})$ primary critical nodes of distinctly different types. This proves Lemma 10. ∎

Proof of Lemma 11. Keep in mind that $\tilde{H}$ has been chosen. 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 $(l+1)$-tuple $\xi(\sigma, \tilde{H}) = (k, i_1, i_2, ..., i_k, j_1, j_2, ..., j_{l-k})$ 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.

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

Fact 5. If σ and σ' are distinct elements in Γ', then $\xi(\sigma, \tilde{H}) \neq \xi(\sigma', \tilde{H})$.

Given the value of $\xi(\sigma, \tilde{H}) = (k, i_1, i_2, ..., i_k, j_1, j_2, ..., j_{l-k})$, 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 branch to take is clearly determined by the following rules: (a) if u is a critical node, $\xi(\sigma, \tilde{H}) = (k, i_1, i_2, ..., i_k,$

$j_1, j_2, ..., j_{l-k}$) 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 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 σ-critical node of type (i, j), in which case we should take the 0-branch, *or* we have already seen a σ-critical node of type (i, j), in which case we know that the induced subgraph of input between the ith block of V and the jth 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 5.

From Fact 5, we can find an upper bound to $|\Gamma' - \Gamma''|$ by counting the number of possible values of $\xi(\sigma, \tilde{H}) = (k, i_1, i_2, ..., i_k, j_1, j_2, ..., j_{l-k})$ for $\sigma \in \Gamma' - \Gamma''$. Let $a = \lceil 99l/100 \rceil$ and $b = \lfloor l^2/5000 \rfloor$. Inequality (10) says that $k \geqslant a$, Fact 4 says that $j_t \leqslant l^2$ for all t, and the constraint that $N_1(\sigma, \tilde{H}) \leqslant l^2/5000$ says that $i_s \leqslant b$ for all s. It follows that

$$\begin{aligned}
|\Gamma' - \Gamma''| &\leqslant \sum_{a \leqslant k \leqslant l} \binom{b}{k} \binom{l^2}{l-k} \\
&\leqslant \sum_{a \leqslant k \leqslant l} \frac{b^k \, l^{2(l-k)}}{k!\,(l-k)!} \\
&= \sum_{a \leqslant k \leqslant l} \binom{l}{k} \frac{b^k l^{2(l-k)}}{l!} \\
&\leqslant \sum_{a \leqslant k \leqslant l} \binom{l}{k} \frac{l^{2l}}{(5000)^k l!} \\
&\leqslant \sum_{a \leqslant k \leqslant l} \binom{l}{k} \frac{l^{2l}}{(5000)^a l!} \\
&\leqslant \sum_{a \leqslant k \leqslant l} \binom{l}{k} \frac{l^{2l}}{(2000)^l l!} \\
&\leqslant 2^l \frac{l^{2l}}{(2000)^l l!}.
\end{aligned}$$

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

$$\begin{aligned}
|\Gamma' - \Gamma''| &\leqslant \left(\frac{2e^2}{2000}\right)^l l! \\
&\leqslant \frac{1}{20} |\Gamma| \\
&\leqslant \frac{1}{2} |\Gamma'|.
\end{aligned}$$

This proves Lemma 11. ∎

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 [6]. As in [6], 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 $\log_2 N_0' \geqslant 20 + \lceil 10^{3/\varepsilon} \rceil$. Thus, $(\log_2 n)^{\varepsilon/3} \geqslant 10$ for all $n \geqslant N_0'/8$.

We first prove $R(P) = \Omega(n(\log n)^{\varepsilon/3})$ when $n = 2^k$ with integral k and $n \geqslant N_0'/8$. Let $L_i = 2^{k-i} K_{2^i}$ for $0 \leqslant i \leqslant k$. Since $P \in \mathscr{P}_n$, there exists $0 \leqslant i_0 < k$ such that $P(L_{i_0}) = 0$ and $P(L_{i_0+1}) = 1$. (Such a sequence was employed in [6]). We consider two cases depending on the value of 2^{i_0}.

Suppose $2^{i_0} \geqslant n/((\log_2 n)^{2\varepsilon/3})$. Let $H_j = jK_{2^{i_0+1}} + (2^{k-i_0} - 2j) K_{2^{i_0}}$ for $j = 0, 1, 2, ..., 2^{k-i_0-1}$. Thus $H_0 = L_{i_0}$, and $H_{2^{k-i_0-1}} = L_{i_0+1}$. Since $P \in \mathscr{P}_n$, there exists $0 \leqslant j_0 < 2^{k-i_0-1}$ 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, $R(P) \geqslant R(Q)$. As Q is nontrivial and monotone, we have by assumption $R(Q) = \Omega(2^{i_0}(\log 2^{i_0})^{\varepsilon}) = \Omega(n(\log n)^{\varepsilon/3})$.

We now consider the case

$$2^{i_0} < \frac{n}{(\log_2 n)^{2\varepsilon/3}}. \tag{15}$$

Let V denote the disjoint union of sets V_i, $1 \leqslant i \leqslant l \equiv 2^{k-i_0-1}$, where $|V_i| = 2^{i_0}$; similarly let $W = \bigcup_{1 \leqslant i \leqslant l} W_i$. Let $x_{ij,ab}$ be Boolean variables, where $1 \leqslant i, j \leqslant l$ and $1 \leqslant a, b \leqslant 2^{i_0}$. 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 $l_0 = l^2 2^{2i_0}$. For any truth assignment $\tilde{x} \in \{0, 1\}^{l_0}$ to $\langle x_{ij,ab} \rangle$, let $G_{\tilde{x}} \in \mathscr{G}_n$ 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 $1 \leqslant i \leqslant l$. If $x_{ij,ab} = 1$ then there is an edge between ath node in V_i and bth node in W_j.

We later construct a probability distribution q over $\mathscr{G}_n$, with $q(G) = 0$ unless $G = G_{\tilde{x}}$ for some $\tilde{x}$, and prove that $\bar{C}_q(A) = \Omega(n(\log_2 n)^{\varepsilon/3})$ for all $A \in \mathscr{A}_P$. To help describe 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 $X = \{\tilde{x} \mid \tilde{x} \in \{0, 1\}^{l_0}, \tilde{x} \leqslant \tilde{x}^{(1)}, P(G_{\tilde{x}}) = 1$, 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 6. If there is an $\tilde{x} \in X$ with $\#(\tilde{x}) \geqslant n(\log_2 n)^{\varepsilon/3}$, then $R(P) = \Omega(n(\log_2 n)^{\varepsilon/3})$.

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

$$\#(\tilde{x}) < n(\log_2 n)^{\varepsilon/3}. \tag{16}$$

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

$$\#(\tilde{y}) = \alpha_1 + \alpha_2 + \cdots + \alpha_{s(\tilde{y})}. \tag{17}$$

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

$$\mu = \frac{\#(\tilde{y})}{s(\tilde{y})}. \tag{18}$$

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

LEMMA 12. *If* $\mu \geqslant 4m(\log_2 n)^{\varepsilon/3}$, *then* $R(P) = \Omega(n(\log_2 n)^{\varepsilon/3})$.

Proof. From (16) and (18),

$$s(\tilde{y}) < \tfrac{1}{2}l. \tag{19}$$

From (17) and (18),

$$\alpha_1 \geqslant 4m(\log_2 n)^{\varepsilon/3}. \tag{20}$$

We now define a probability distribution q on $\mathscr{G}_n$ by generating a random $G \in \mathscr{G}_n$. Let $\tilde{z} = \langle z_{ij,ab} \rangle$ be defined as follows for all a, b: $z_{ii,ab} = y_{11,ab}$ for $i \in \{1, s(\tilde{y}) + 1, s(\tilde{y}) + 2, ..., l\}$, $z_{ii,ab} = y_{ii,ab}$ for $2 \leqslant i \leqslant s(\tilde{y})$, and $z_{ij,ab} = 0$ otherwise. Now pick a random sequence $\zeta = (a_1, b_1), (a_{s(\tilde{y})+1}, b_{s(\tilde{y})+1}), (a_{s(\tilde{y})+2}, b_{s(\tilde{y})+2}), ..., (a_l, b_l)$, 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 $i \in \{1, s(\tilde{y}) + 1, s(\tilde{y}) + 2, ..., l\}$. Let the graph $G_{\tilde{z}(\zeta)}$ be the random $G \in \mathscr{G}_n$. This defines q.

Let $A \in \mathscr{A}_P$. 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 $i \in \{1, s(\tilde{y}) + 1, s(\tilde{y}) + 2, ..., l\}$. 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 $\bar{C}_q(A) \geqslant \sum_{s(\tilde{y}) < i \leqslant l} E(D_i)$, 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,

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

Thus, $\bar{C}_q(A) \geqslant (l - s(\tilde{y}))\, \frac{1}{2}(1 + \alpha_1) = \Omega(n(\log_2 n)^{\varepsilon/3})$ by (19) and (20). This proves Lemma 12. ▮

LEMMA 13. *If* $\mu < 4m(\log_2 n)^{\varepsilon/3}$, *then* $R(P) = \Omega(n(\log_2 n)^{\varepsilon/3})$.

Proof. We construct probability distributions q over $\mathscr{G}_n$, and show that any algorithms A for determining P must have $\bar{C}_q(A) = \Omega(n(\log_2 n)^{\varepsilon/3})$. We distinguish two cases. First consider the case $s(\tilde{y}) < l/2$. 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 $1 \leqslant a$, $b \leqslant m$. Let $\mathscr{H}$ be the set of all m by m bipartite graphs H' isomorphic to H. For each $\zeta = (s, t, H')$, where $s(\tilde{y}) \leqslant s$, $t \leqslant l$ and $H' = (h'_{ab}) \in \mathscr{H}$, define $\tilde{z}(\zeta) = (x_{ij,ab}) \in \{0, 1\}^{l_0}$ as

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

The distribution q over $\mathscr{G}_n$ 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 $s(\tilde{y}) \leqslant i$, $j \leqslant l$ and $1 \leqslant a$, $b \leqslant m$, the problem for determining P now becomes the identification problem for $\mathscr{D}(m, (l - s(\tilde{y}) + 1), H)$. In fact, any algorithm $A \in \mathscr{A}_P$ naturally induces an algorithm B for the identification problem $\mathscr{D}(m, (l - s(\tilde{y}) + 1), H)$ such that $\bar{C}_{q_0}(B) \leqslant \bar{C}_q(A)$, where q_0 is the uniform distribution for $\mathscr{D}$ discussed in Section 4. By Theorem 2, we have

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

Since $m = O(n/(\log n)^{2\varepsilon/3})$ by (15), we have proved Lemma 13 for this case.

Now consider the case $s(\tilde{y}) \geqslant l/2$. Let $s_0 = \lceil s(\tilde{y})/2 \rceil$. For each $s_0 \leqslant i \leqslant s(\tilde{y})$, let H_i denote the m by m bipartite graph corresponding to the edge set $J_i(\tilde{y})$; clearly, $|E_{H_i}| \leqslant 2\mu$. Let $\mathscr{H}_i$ be the set of all m by m bipartite graphs isomorphic to H_i. Let Γ be the set of all permutations of $(s_0, s_0 + 1, ..., s(\tilde{y}))$. For each

$\zeta=(\sigma, H'_{s_0}, H'_{s_0+1}, ..., H'_{s(\tilde{y})})$, where $\sigma\in\Gamma$ and $H'_i\in\mathscr{H}_i$, define $\tilde{z}(\zeta)=(x_{ij,ab})\in\{0,1\}^{l_0}$ as

$$x_{ii,ab}=y_{ii,ab} \quad \text{for} \quad 1\leqslant i<s_0, \quad 1\leqslant a,b\leqslant m$$

$$x_{i\sigma(i),ab}=(H'_i)_{ab} \quad \text{for} \quad s_0\leqslant i\leqslant s(\tilde{y}), \quad 1\leqslant a,b\leqslant m$$

$$x_{ij,ab}=0 \quad \text{otherwise.}$$

The distribution q over $\mathscr{G}_n$ 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 $s_0\leqslant i, j\leqslant s(\tilde{y})$ and $1\leqslant a, b\leqslant m$, the problem for determining P now becomes the identification problem for $\mathscr{E}(m, (s(\tilde{y})-s_0+1), (H_{s_0}, H_{s_0+1}, ..., H_{s(\tilde{y})}))$ with the uniform distribution discussed in Section 4. Let $p=\max_i\{|E_{H_i}|/m^2|\}$. Then $p\leqslant 2\mu/m^2$. It follows then from Theorem 3 that, for every algorithm $A\in\mathscr{A}_P$, we have

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

Since $m=O(n/\log n)^{2\varepsilon/3})$ by (15), we have proved Lemma 13 for this last case. This completes the proof of Lemma 13. ∎

We have proved that, when $n\geqslant N'_0/8$ is a power of 2, $R(P)=\Omega(n\log_2 n)^{\varepsilon/3})$. We now prove it for all integers $n\geqslant N'_0$. We divide the discussion into two cases.

First, suppose $n=2^k+2^l+t$, where $0\leqslant t<2^l$ and $l\leqslant k-2$. Let V be the disjoint union of V_1, V_2, V_3 with $|V_1|=|V_2|=2^{k-1}$, $|V_3|=2^l+t$. 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, $G_1=K_{V_2\cup V_3}$, $G_2=K_{V_1}\cup G_1$, $G_3=K_{V_1\times V_3}\cup G_2$, $G_4=K_V=K_{V_1\times V_2}\cup G_3$. (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 $P(K_{V_1\cup V_2})=1$. Let Q_1 be the property induced on the vertex set $V_1\cup V_2$ defined by $Q((V_1\cup V_2, E))=P((V,E))$. Then Q_1 is a nontrivial and monotone property on 2^k-vertex graphs. Thus, $R(P)\geqslant R(Q_1)=\Omega(2^k(\log 2^k)^{\varepsilon/3})=\Omega(n(\log n)^{\varepsilon/3})$.

If $i=2$, let Q_2 be the property induced on the vertex set V_1 defined by $Q((V_1,E))=P((V,E'))$, where E' is the union of E and all the edges in G_1. Then Q_2 is a nontrivial and monotone property on 2^{k-1}-vertex graphs. Thus, $R(P)\geqslant R(Q_1)=\Omega(2^{k-1}(\log 2^{k-1})^{\varepsilon/3})=\Omega(n(\log n)^{\varepsilon/3})$.

If $i\in\{3,4\}$, let Q_i be the bipartite graph property on vertex set $V_1\times V_2$, defined by $Q_i((V_1\times V_2, E))=P((V,E'_i))$ where E'_i is the union of E and all the edges in G_{i-1}. Then Q_i is nontrivial and monotone. Thus by Proposition 1, $R(P)=R(Q)=\Omega(2^{k-1}(\log 2^{k-1})^{\varepsilon})=\Omega(n\log n)^{\varepsilon})$.

The only other case is $n = 2^k + 2^{k-1} + t$, where $0 \leqslant t < 2^{k-1}$. Let V be the disjoint union of V_1, V_2, V_3 with $|V_1| = |V_2| = 2^{k-1} + t$, $|V_3| = 2^{k-1} - t$. Note that $|V_2 \cup V_3| = 2^k$. 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 $n = 2^k + 2^l + t$ then leads to $R(P) = \Omega(n(\log n)^{\varepsilon/3})$. This completes the proof of Proposition 2.

6. Remarks

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

1. It remains a tantalizing question whether the randomized complexity of every nontrivial monotone graph property is of order $\Omega(n^2)$. Valerie King [2] has improved our bound from $\Omega(n(\log n)^{1/12})$ to $\Omega(n^{5/4})$, and recently, Péter Hajnal [1] has improved it further to $\Omega(n^{4/3})$. 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 smaller can the randomized complexity $r = R(f)$ be than the deterministic complexity $m = D(f)$ for any Boolean function f? Saks and Wigderson [8] conjectured that $r = \Omega(m^{.753\cdots})$. Could one prove at least a bound which is nonlinear in $\sqrt{m}$, 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 nonmonotone) graph property? As mentioned in the introduction, we know that $r = \Omega(\sqrt{m})$, in the notation of the last paragraph. Can one prove that $r = \Omega(mh(m))$ with $h(m) \to \infty$?

Acknowledgments

The author thanks the referees for many helpful comments. He is especially grateful to one referee for simplifying the proof of Theorem 2 in Section 4.

References

1. P. Hajnal, "An $\Omega(n^{4/3})$ Lower Bound on the Randomized Complexity of Graph Properties," Technical Report 88-004, University of Chicago, 1988.
2. V. King, Lower bounds on the complexity of graph properties, *in* "Proc. 20th Annual ACM Symposium on Theory of Computing," pp. 468–476, 1988.
3. D. Kirkpatrick, Determining graph properties from matrix representations, *in* "Proc. 6th Annual ACM Symposium on Theory of Computing," pp. 84–90, 1974.
4. U. Manber and M. Tompa, The complexity of problems on probabilistic, nondeterministic and alternating decision trees, *J. Assoc. Comput. Mach.* **32** (1985), 720–732.

5. F. MEYER AUF DER HEIDE, Nondeterministic versus probabilistic linear algorithms, *in* "Proc. 26th Annual IEEE Symposium on Foundations of Computer Science," pp. 65–73, 1985.
6. R. RIVEST AND S. VUILLEMIN, On recognizing graph properties from adjacency matrices, *Theoret. Comput. Sci.* **3** (1978), 371–384.
7. A. L. ROSENBERG, On the time required to recognize properties of graphs: A problem, *SIGACT News* **5**, No. 4 (1973), 15–16.
8. M. SAKS AND A. WIGDERSON, Probabilistic Boolean decision trees and the complexity of evaluating game trees, *in* "Proc. 27th Annual IEEE Symposium on Foundations of Computer Science," pp. 29–38, 1986.
9. M. SNIR, Lower bounds for probabilistic linear decision trees, *Theoret. Comput. Sci.* **38** (1985), 69–82.
10. A. C. YAO, Probabilistic computations: Towards a unified measure of complexity, *in* "Proc. 18th Annual IEEE Symposium on Foundations of Computer Science," pp. 222–227, 1977.